The ONE!

One Schedule to Rule them All!

Welcome to the "One Schedule to Rule them All!". Thank you for your interest by using this. This is an attempt to make things easier for you, the DEF CON attendee, to figure out the when/what/where during the chaos of DEF CON 29.

It started out simple. I had a Kindle and wanted an ebook of the schedule so I didn't have to wear out the paper pamphlet by pulling it out after every talk to figure out where to go next. Back then there was only the main DEF CON tracks, not really any Villages, and production of the ebooks were easy. Over time the Village system developed with a resulting multiplication in complexity, both for attendees and for my production. The offerings no longer include epub and mobi formats and instead now include html, csv, PDF, ical, public Google calendar, and mysql dump format files. Hopefully you'll find something of use.

The intent is still to be a resource to answer the question at the end of an hour of "What's next?"

As a general rule I do not include:

- Off-site events
- Blatent vender pitch events
- Nonspecific timed events. Unfortunately this means the contests aren't on the regular schedule.
- DEF CON events are emphasized, so BSides Las Vegas and BlackHat tend to not show up

Be sure to check out the Links section at the bottom of this. Most all of the events listed here were derived from these links and a Infoboot data feed. There is much more going on at DEF CON than what is listed here.

Check out the Guides/Tips/FAQs links if you're new to Las Vegas.
Notable suggestions are:

- Bring comfortable shoes, you'll be doing a lot more walking than you expect
- Bring a water bottle to keep hydrated
- Beware of going out doors, there's nothing like LV sun and heat
- Everything in Las Vegas is a longer walk than you think
- Relax, don't try to see everything, you'll never be able to!
- Have FUN!

And finally, this is only as good as the ideas and information used to generate it. I welcome your constructive suggestions and comments. Please send them to qumqats@outel.org

Have a good time at DEF CON 29!

Index of DEF CON 29 Activities

Maps and detailed Village Info

Hour by Hour list of happenings, start at the top, or go to a specific day.
Schedule
- Thursday - Friday - Saturday - Sunday

Sorted list of all the Speakers Names linked to their talk's description.
Speaker List

Sorted list of all the Talk's titles linked to the talk description.
Talk Title List

Talk lists for each Village, start at the alphabetic top, or go to a specific Village.
Village Talk List
AIV - APV - ASV - AVV - BCV - BHV - BICV - BTV - CAHV - CCV - CHV - CLV - CON - CPV - DC - DDV - DL - HHV - HRV - HTSV - ICSV - IOTV - LBV - LPV - MUS - PHV - PYV - RCV - RFV - RGV - SEV - SOC - VMV - WS

Descriptions and Info for all the talks.
Talk Descriptions

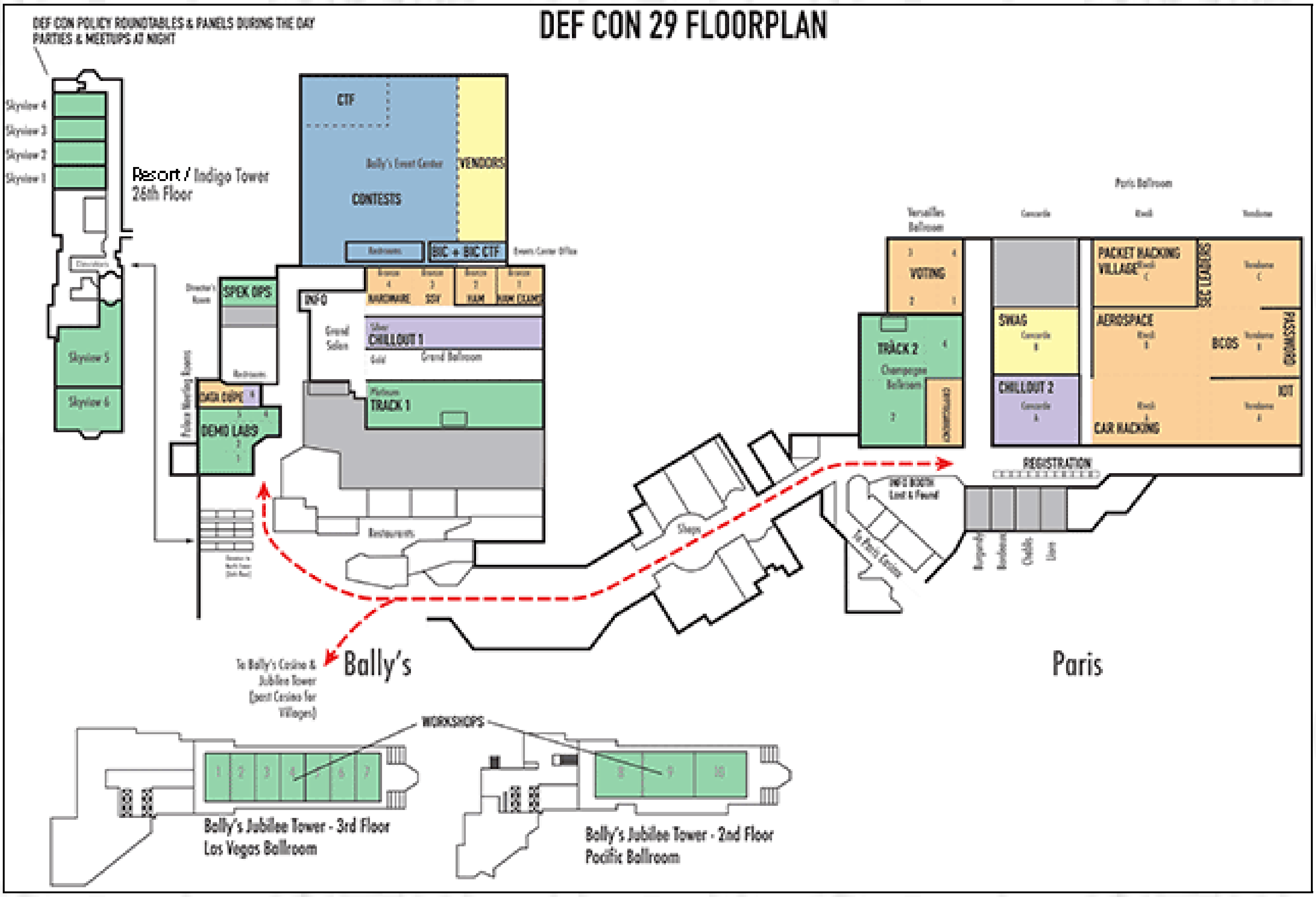
The latest news from defcon.org
DEF CON News

The answer to your questsions about DEF CON overall and for this year.
DEF CON FAQ
DEF CON 29 FAQ

Links to DEF CON 29 related pages

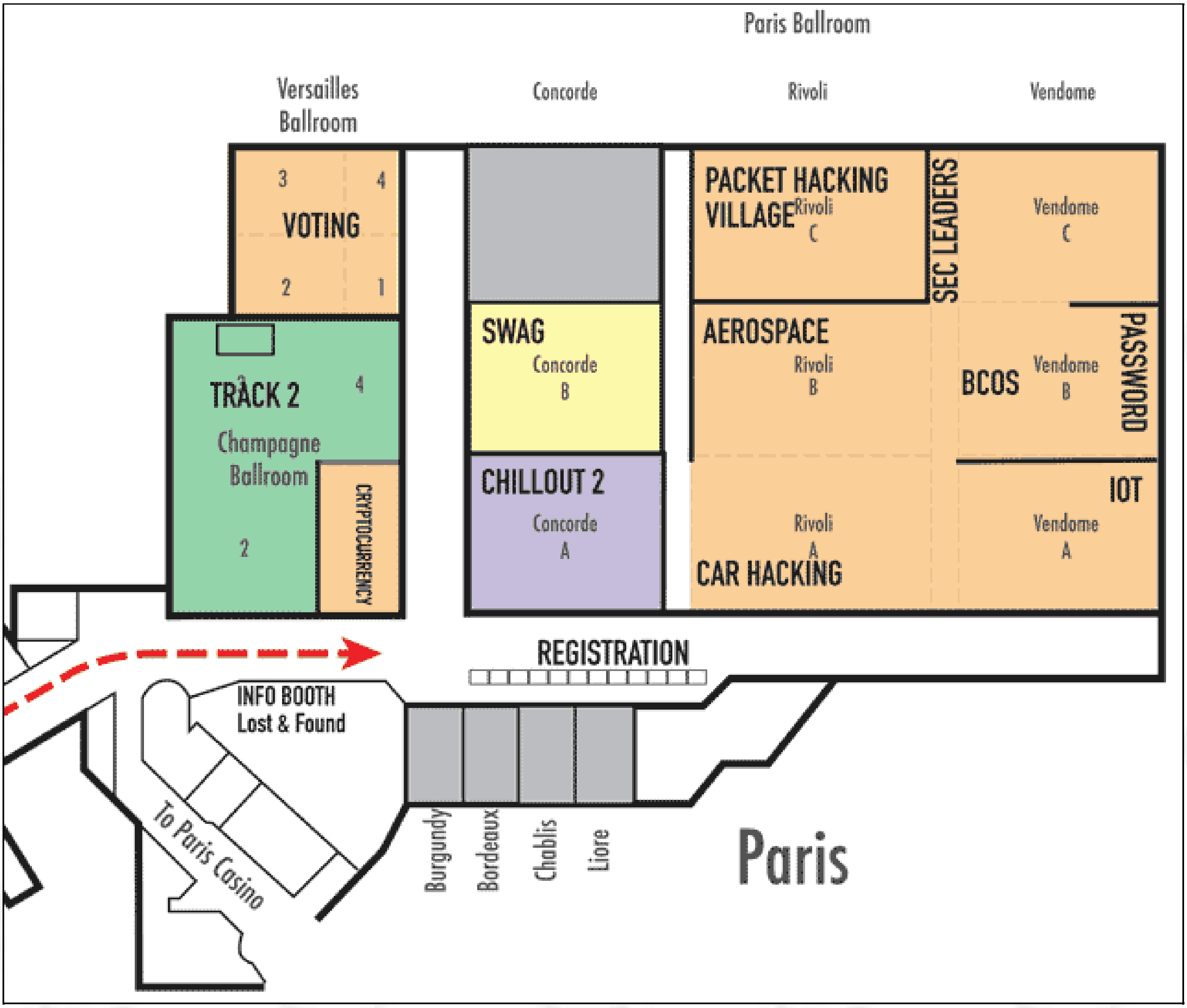
Maps and detailed Village Info

Full map of both Ballys's and Paris



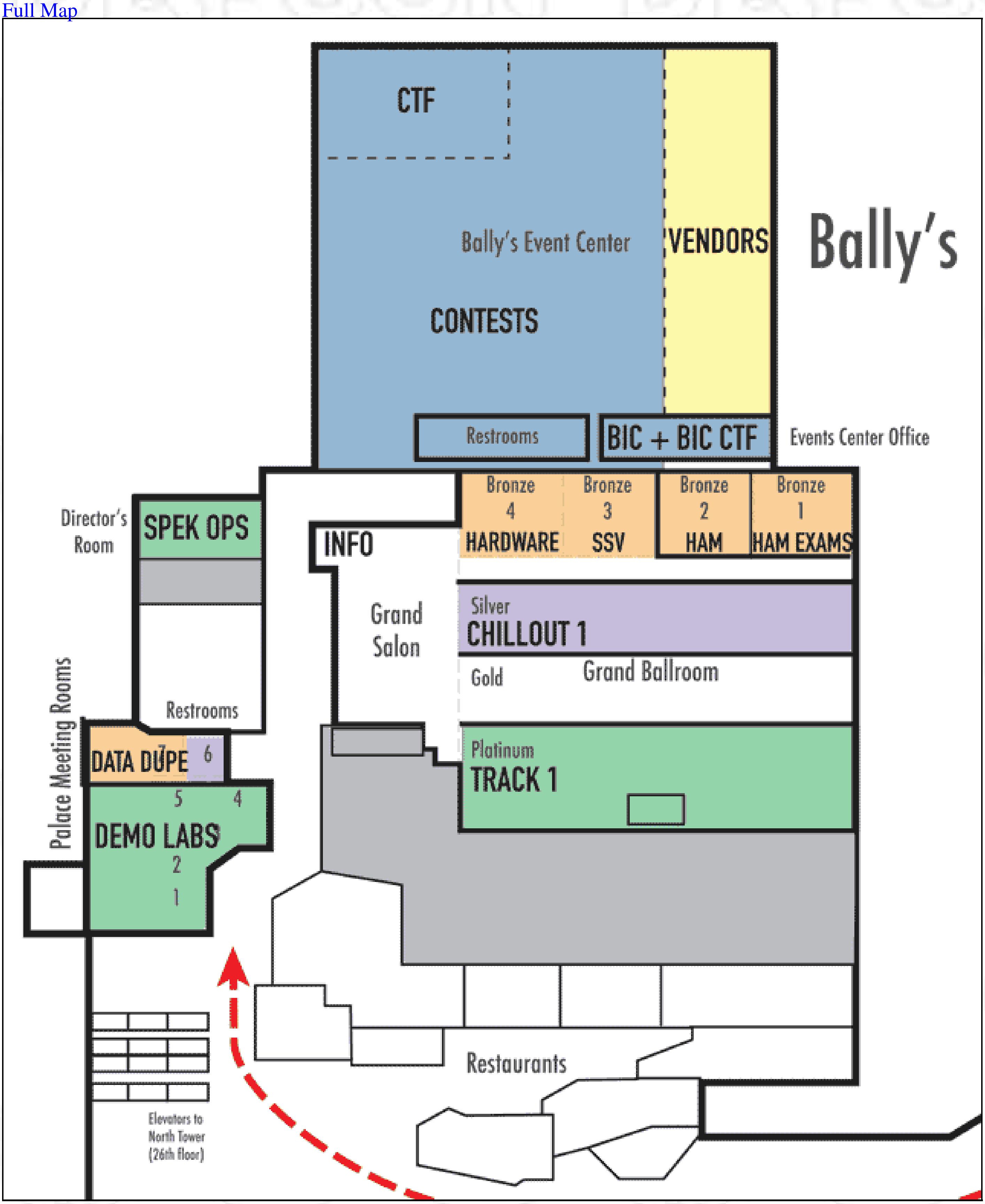
Closeup view of activities at Paris

Full Map



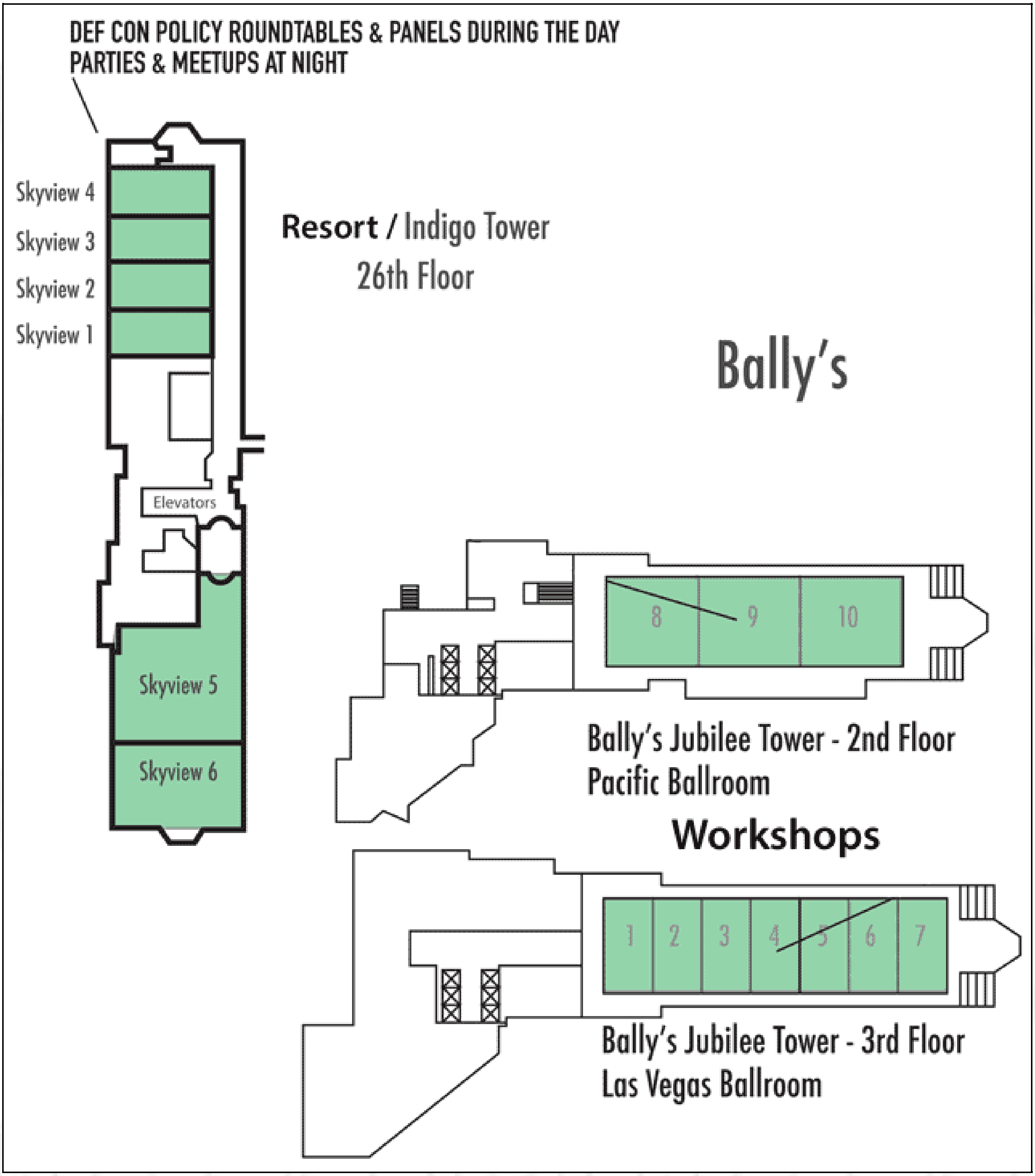
Closeup view of activities at Bally's

Full Map



Closeup of Ballys' Resort/Indigo Tower 26'th floor and Jubilee Tower 2/3 floors

Full Map



AVV - Adversary Village

AVV VillageTalk List:
Home Page: https://adversaryvillage.org/index.html
Sched Page: https://adversaryvillage.org/adversary-events/DEFCON-29/
DC Forums Page: https://forum.defcon.org/node/236914
DC Discord Chan: https://discord.com/channels/708208267699945503/865456992101466192
Hours: Fri: 11:00 - 21:00 - Sat: 10:00 - 21:00 - Sun: 10:00 - 17:00
Social Media Links:
TW @AdversaryVillag
IG @AdversaryVillage
LI @adversaryvillage
FB @AdversaryVillage
TI @AdversaryVillage
DC https://discord.gg/GDB3rC7KYz
YT link

The "Adversary Village" is a community torqued combat readiness platform purely focused on Adversary simulation, emulation tactics, Simulation CTFs, Supply chain security attack tactics, Adversary Tactics and urban survival skills.

This is different from any of what has been covered in the existing villages because our focus is on simulation of the actions of a threat actor or an adversary and this being simulated here.

As this domain matures, we anticipate active participation from enterprises as such simulations would help immensely towards internal capacity building from having a "live fire" training opportunity. An increasing number of researchers too are focusing on building tools and techniques for simulation of various adversarial actions against an organization or Supply chain, instead of actual real-world exploitation.The goal of the Adversary Village would be to build an open Security community for the researchers and organizations, who are putting together new means and methodologies towards the simulation/emulation of adversary tactics.

Return to Index

ASV - Aerospace Village

ASV VillageTalk List:
Home Page: https://aerospacevillage.org/
Sched Page: https://aerospacevillage.org/events/upcoming-events/def-con-29/def-con-29-schedule/
DC Forums Page: https://forum.defcon.org/node/236573
DC Discord Chan: https://discord.com/channels/708208267699945503/732393044363444264
Hours: Fri: 10:00 - 16:00 - Sat: 10:00 - 16:00
Social Media Links:
TW @secureaerospace
LI @aerospace-village
TW @hack_a_sat

The Aerospace Village at DEF CON will encompass all aspects of the aerospace sector ranging from airports, air traffic management, aircraft and space.

The aviation and space industries, security researchers, and the public share a common goal: safe, reliable, and trustworthy aviation and space operations. For too long, negative perceptions and fractured trust on all sides have held back collaboration between the aviation, space, and security researcher communities that has advanced safety, reliability, and security of other industries. As the traditional domains of aviation safety and cybersecurity increasingly overlap, more effective collaboration between stakeholders ensures we will be safer, sooner, together.

Through the Aerospace Village, the security research community invites industry leaders, researchers and academia interested in aviation and space security, safety, and resilience to attend, understand, collaborate together to achieve our common goals. Empathy and understanding build common ground, while acts and words likely to increase division between these two communities undermine these efforts. The Aerospace Village welcomes those who seek to improve aviation and space security, safety, and resilience through positive, productive collaboration among all ecosystem stakeholders.

Our Goal
The Aerospace Village is a volunteer team of hackers, pilots, and policy advisors who come from the public and private sectors. We believe the flying public deserves safe, reliable, and trustworthy air travel which is highly dependent on secure aviation and space operations.

Our Mission
Create, sustain, and grow an inclusive community focused on aerospace cybersecurity;

Inspire the next generation of aerospace cybersecurity leaders; Promote and develop aerospace cybersecurity expertise and knowledge.

The Aviation Village will do this by:
- Building connections, trust, and understanding among all Village participants. - Developing aerospace security skills among DEF CON attendees through workshops and hands-on activities. - Promoting constructive dialog through talks and interaction.?

Return to Index

AIV - AI Village

AIV VillageTalk List:
Home Page: https://aivillage.org/
Sched Page: https://aivillage.org/events/2020/8/4/ai-village-def-con-28-safe-mode-w6wsl
DC Forums Page: https://forum.defcon.org/node/236533
DC Discord Chan: https://discord.com/channels/708208267699945503/732733090568339536
Hours: Fri: 09:00 - 17:00 - Sat: 09:00 - 17:00 - Sun: 09:00 - 14:00
Social Media Links:
TW @aivillage_dc
TI @aivillage
YT link
DC https://aivillage.org/discord-guide

Artificial Learning techniques are becoming more prevalent in core security technologies like malware detection and network traffic analysis. Its use has opened up new vectors for attacks against non-traditional targets, such as deep learning based image recognition systems used in self driving cars. There are unique challenges in defending and attacking these machine learning systems that the security community needs to be made aware of. This AI Village will introduce DEF CON attendees to these systems and the state of the art in defending and attacking them. We will provide a setting to educate DEF CON at large through workshops and a platform for researchers in this area to share the latest research.

Our main focus is on expanding the hands-on activities that attendees can participate in. This year, attendees will create a realistic face using StyleGAN, learn how to generate text, and attack a discriminatory resume screening program. We'll also have talks via CFP, and workshops: both introductory ML for beginners and intermediate/advanced on Facial Recognition/Adversarial ML. We are planning three contests inside the village: one as a standard CTF, another on evading a malware classifier (Ember), and a final realtime panel of Deepfaked DarkTangent's answering personal questions and giving opinions on life, the universe, and everything!

Return to Index

APV - AppSec Village

APV VillageTalk List:
Home Page: https://www.appsecvillage.com/
Sched Page: https://www.appsecvillage.com/events/dc-2021
DC Forums Page: https://forum.defcon.org/node/236574
DC Discord Chan: https://discord.com/channels/708208267699945503/790973922949726228
Social Media Links:
TW @AppSec_Village
LI @appsecvillage
YT https://www.youtube.com/c/AppSecVillage

The first two AppSec Villages were a resounding success. We learned that whether in person or online, our AppSec community is fantastic. We are pumped to be back bigger and better.

Come immerse yourself in everything the world of application security has to offer. Whether you are a red, blue, or purple teamer, come learn from the best of the best to exploit software vulnerabilities and secure software. Software is everywhere, and Application Security vulnerabilities are lurking around every corner, making the software attack surface attractive for abuse. If you are just an AppSec n00b or launch deserialization attacks for fun and profit, you will find something to tickle your interest at the AppSec Village.

Software runs the world. Everything from IoT, medical devices, the power grid, smart cars, voting apps - all of it has software behind it. Such a variety of topics will be reflected in our cadre of guest speakers representing all backgrounds and walks of life.

AppSec Village welcomes all travelers to choose from talks by expert community members, an all AppSec-focused CTF, contests that challenge your mind and your skillz, and more. Bring your thirst for knowledge and passion for breaking things, and your visit to AppSec Village will be a thrill!

Like in the previous villages (but better this time), we will focus our efforts on hands-on activities and practical learning activities. We are planning workshops, interactive demos, step-by-step guided walkthroughs, CTF for AppSec beginners, and a reversed CTF for level builders.

Return to Index

BCV - Blockchain Village

BCV VillageTalk List:
Home Page: https://www.blockchainvillage.net/
Sched Page: https://www.blockchainvillage.net/schedule-2021/
DC Forums Page: https://forum.defcon.org/node/236915
DC Discord Chan: https://discord.com/channels/708208267699945503/732733136408019084
Hours: Fri: 10:00 - 17:30 - Sat: 10:00 - 18:00 - Sun: 10:00 - 13:30
Social Media Links:
TW @BCOSvillage

Blockchain Village is a 'Not for Profit' event organized as a part of Information Security conferences like DEF CON. Primary focus of Blockchain village is to promote, research, development & knowledge sharing around security of blockchain technology and applications of blockchain in the field of information security.

The village organizes hands-on workshops, contests, discussions and talks by & for the community members. The event, its members and supporters form across the world love to share the best research & latest content with our awesome community.

This year at Blockchain Village we bring back Capture-The-Coin contest running in parallel with more hands on workshops (Mathematical and Practical) along with cutting edge Talks-n-Tools, noteworthy Demos-n-Discussions, all focused on security of Blockchains and Distributed Applications.

Join us at DEF CON 29 as we celebrate the power + potential of Distributed applications, enabled by Blockchain technology.

Return to Index

BICV - Blacks in Cybersecurity

BICV VillageTalk List:
Home Page: https://www.blacksincyberconf.com/
Sched Page: https://www.blacksincyberconf.com/bic-village
DC Forums Page: https://forum.defcon.org/node/236923
Hours: Fri: 10:00 - 17:00 - Sat: 10:00 - 17:00
Social Media Links:
TW @BlackInCyberCo1
IG @blackincyberconf
TI @blacksincybersecurity
YT https://youtu.be/YsUw9z_gZzY
LI @blackincyberconference
PT @blacksincybersecurity
FB @blackincyberconf

The Blacks In Cybersecurity (BIC) Village seeks to bring culturally diverse perspectives to the holistic Cybersecurity community; by way of a series of talks and a capture the flag event.

In providing these activities, we believe that we can normalize the discussion of deficiency and prejudices in Cybersecurity literacy, education and development that ultimately impact the progress and development of the field.

Our village programming is also designed to highlight Black experiences, innovations in the field, Black culture and Black history which is designed to encourage more diverse hobbyists and professionals to engage and contribute to this conference and the greater Cybersecurity and Hacker/Maker communities.

Return to Index

BHV - Bio Hacking Village

BHV VillageTalk List:
Home Page: https://www.villageb.io/
DC Forums Page: https://forum.defcon.org/node/236534
DC Discord Chan: https://discord.com/channels/708208267699945503/735273390528528415
Social Media Links:
TW @dc_bhv
LI @biohacking-village
YT http://youtube.com/biohackingvillage
TI @biohackingvillage
DC https://discord.gg/Q8ubDb5
SP link

Growing from seeds of demand, the Biohacking Village emerged at DEF CON to deliver action-oriented reinvention of the safety and security of health care. THE BIOHACKING VILLAGE, a 501(c)3 organization, is uniquely poised to inform global conversations in health care cybersecurity research. Representing voices who see code as genetics, subroutines as organic processes, and programs as life itself the BHV has grown to become an expansive and inclusive, hands-on playground for the entire biomedical ecosystem - patients, clinicians, hackers, manufacturers, regulators, hospital administrators, and others seeking healthier futures through meaningful technology. This nimble community delivers hands-on, strident learning labs to influence in health care, industry, and manufacturing.

We bring the biomedical ecosystem to DEF CON in four ways:

Device Lab
A high-collaboration, hands-on learning environment builds trust and trustworthiness across multidisciplinary voices in healthcare, connecting security researchers, manufacturers, hospitals, and regulators in an experiential learning laboratory that encourages cross-pollination and real-world skills development. Device Lab research benefits patients and manufacturers by providing valuable, high-fidelity feedback on established, new, and developing devices.

Speaker Lab
Connection starts with shared experiences. Speakers at BHV have walked the walk - from their adventures in garage science to the emerging threats they uncover to next generation solutions and next level care. Full Stack Biotechnologists, security researchers, regulators, clinicians, citizen scientists, patients, and engineers enlighten and inspire BHV attendees through creative and collaborative discussions around emerging technologies and threats, novel work in biologics, security architectures, and the opportunities inside the interdisciplinary nature of healthcare.

Catalyst Lab
The worlds largest, meatiest problems cross through the BHV and the Catalyst Lab works to convene thought leaders, hacktivists, and manufacturers working in the biomedical industry to investigate the solutions of best fit and provide a series of tabletops for training, hands-on workshops, and solutions design that covers the entirety of the biomedical device and security ecosystem.

Capture The Flag
Hackers work to defend a hospital under siege, racing against the clock. The immersive, learn by doing environment challenges hackers to use their skills to anticipate, defend, and recover, as their adversary escalates their attacks throughout the game.

Return to Index

BTV - Blue Team Village

BTV VillageTalk List:
Home Page: https://blueteamvillage.org/
Sched Page: https://dc29.blueteamvillage.org/call-for-content-2021/schedule/
DC Forums Page: https://forum.defcon.org/node/236535
DC Discord Chan: https://discord.com/channels/708208267699945503/732454317658734613
Social Media Links:
TW @BlueTeamVillage
TI @blueteamvillage
YT https://www.youtube.com/c/blueteamvillage
DC https://discord.com/invite/blueteamvillage

We're still standing for our fourth DEF CON! Coming through the looking glass to showcase the defensive side of hacking, Blue Team Village is where you can find out all the multifarious facets of what it means to be a defender. You'll be able to teach and learn about the various ways to keep people safe - and how to subvert attacker expectations to turn their methods back on them.

You'll also be able to find community and mentor-ship within the defensive hacking paradigm, allowing you to find your path within this specialization to learning new skills and refining your old ones.

If you're looking for a community of like-minded hackers with a tendency towards forensics, threat hunting, and other blue-aligned topics, come celebrate the art of defensive hacking with us!

Return to Index

CHV - Car Hacking Village

CHV VillageTalk List:
Home Page: https://www.carhackingvillage.com/
DC Forums Page: https://forum.defcon.org/node/236536
DC Discord Chan: https://discord.com/channels/708208267699945503/732722838942777474
Hours: Fri: 10:00 - 16:30 - Sat: 10:00 - 16:30
Social Media Links:
TW @CarHackVillage
DC https://discord.gg/JWCcTAM

Learn, hack, play. The Car Hacking Village is an open, collaborative space to hack actual vehicles that you don't have to worry about breaking! Don't have tools? We'll loan you some. Never connected to a car? We'll show you how. Don't know where the controllers are? We'll show you how to take it apart.

Hybrid event this year: We'll be in-person in Las Vegas and Virtual. Check out CarHackingVillage or @CarHackVillage for up-to-date information.

Want to learn more about automotive hacking and cyber security? Check out our talks.

Want to hack mobility scooters? Yes! We'll do that to.

Also, check out the CHV CTF.

Return to Index

CAHV - Career Hacking Village

CAHV VillageTalk List:
Home Page: https://www.youtube.com/CareerHackingVillage
DC Forums Page: https://forum.defcon.org/node/236537
DC Discord Chan: https://discord.com/channels/708208267699945503/732732774347309077
Social Media Links:
TW @HackingCareer
YT https://www.youtube.com/CareerHackingVillage

This isnt just getting the next job, it is building, shifting, and presenting skills and capabilities to keep reaching the next level of where you want to go.

In 2020, studies showed that in the hacking community over 45% did not know how to find a job. Post pandemic with unemployment rising, this number has increased to 55%. These studies also show that many hackers do not know the next step in their career. From other studies, hackers have stated that they dont know the top ways to find a job and worse, how to plan the next step in their career. While we talk about the talent shortages, we are not equipping our community with the knowledge, skills, and expertise to sustain their career search and development.

Career Hacking village provides opportunities to build out your career plan and get through the next steps. We have workshops on plan development, resume refinement, identifying mentors, and practice interviews. We will complement this with one-on-one meetings with recruiters for resume review and career mentors for frank conversations about career search and development. New this year will be adding in Mock Interviews to finetune the virtual interviewing process.

The CAHV brings the opportunity to work with the one aspect of tech careers that wont run in the cloud - getting past recruiters and building a career that lets people match their passions with opportunities. No two paths are exactly the same.

From presentations that focus on key aspects of career search and career development to discussions with community career advisors these activities will help community members re-examine their overall career goals and tactics.

Return to Index

CLV - Cloud Village

CLV VillageTalk List:
Home Page: https://cloud-village.org/
Sched Page: https://cloud-village.org/#talks
DC Forums Page: https://forum.defcon.org/node/236916
DC Discord Chan: https://discord.com/channels/708208267699945503/732733373172285520
Hours: Fri: 10:00 - 17:00 - Sat: 10:00 - 17:00 - Sun: 10:00 - 13:20
Social Media Links:
TW @cloudvillage_dc
YT https://www.youtube.com/cloudvillage_dc

With the industry shifting towards cloud infrastructure at a rapid speed, the presence of an open platform to discuss and showcase cloud research becomes a necessity.

Cloud village is an open platform for researchers interested in the area of cloud security. We plan to organize talks, tool demos, CTF and workshops around Cloud Security and advancements. We will open Call for Papers/Workshops/Tools as soon as we get an approval from DEF CON.

Our CTF will be a jeopardy style 2.5 days contest where participants will have to solve challenges around Cloud infrastructure, security, recon, etc. These challenges will cover different cloud platforms including AWS, GCP, Azure, Digital Ocean, etc. We will also reward our top 3 teams with awards.

Return to Index

CCV - Cryptocurrency Village

CCV VillageTalk List:
Home Page: https://cryptocurrencyvillage.net/
Sched Page: https://cryptocurrencyvillage.net/#schedule
DC Forums Page: https://forum.defcon.org/node/236522
DC Discord Chan: https://discord.com/channels/708208267699945503/732733510288408676
Social Media Links:
TW @DEFCONCCVillage
YT https://www.youtube.com/c/MoneroSpaceWorkgroup

Cryptocurrency is a digital form of peer-to-peer money that is exchanged on decentralized networks independent of any central authority and is cryptographically secured. Networks operate under a set of programmatic rules, which maintains the immutability of a public ledger and ensures against double-spending. Although Bitcoin, Ethereum, and Dogecoin are the most well-known cryptocurrencies, other projects like Monero seek to address scalability, privacy, and censorship resistance in innovative ways.

The Cryptocurrency Village brings together leading experts in the area to explore substantive issues regarding the current state of blockchain technologies, regulatory landscape, and the general cryptocurrency ecosystem. The village hosts keynote talks, panels, workshops, networking events, and parties.

Return to Index

CPV - Crypto Privacy Village

CPV VillageTalk List:
Home Page: https://cryptovillage.org/
DC Forums Page: https://forum.defcon.org/node/236538
DC Discord Chan: https://discord.com/channels/708208267699945503/732734002011832320
Social Media Links:
TW @cryptovillage
SL https://cryptovillage.slack.com/
YT link
TI @cryptovillage
YT link

At the Crypto & Privacy Village (CPV) you can learn how to secure your own systems while also picking up some tips and tricks on how to break classical and modern encryption. The CPV features workshops and talks on a wide range of cryptography and privacy topics from experts. We'll also have an intro to crypto talk for beginners, crypto-related games, the infamous CPV puzzle, a key-signing party, privacy-related art installations, and other great events.

The forum for the Gold Bug Crypto Privacy Contest is located here: https://forum.defcon.org/node/236491

The CPV discusses the interesting intersection of privacy and technology as well as building privacy enhancing technologies. We are able to dig into the nitty gritty details of cryptography and give high level crypo intros for those who might feel intimidated by it. We also discuss and hack on major topics and issues: facial recognition technology, license plate readers, privacy enhancing clothing, crypto backdoor laws.

Return to Index

DDV - Data Duplication Village

DDV VillageTalk List:
Home Page: https://dcddv.org/
Sched Page: https://dcddv.org/dc29-schedule
DC Forums Page: https://forum.defcon.org/node/236520
DC Discord Chan: https://discord.com/channels/708208267699945503/732732641694056478
Hours: Thur: 16:00 - 19:00 - Fri: 10:00 - 17:00 - Sat: 10:00 - 17:00 - Sun: 10:00 - 11:00
Social Media Links:
TW @DDV_DC

It's true, the Data Duplication Village is back for DC 29! We have all the bits and bytes available from infocon.org packed up into nice, neat packages. If you're looking for something to fill up all your unused storage, may I recommend a nice hash table or two with a side of all of the DefCon talks? This is a "free-to-you" service where we're providing you direct access to terabytes of useful data to help build those skills.

HOW IT WORKS
DEF CON will provide a core set of drive duplicators as well as data content options. We accept 6, 8, and 10TB drives on a first come, first served basis and duplicate 'till we can no longer see straight. Bring in your blank SATA3 drives - check them in early - to get the data you want. Come back in about 24 hours to pick up your data-packed drive. Space allowing, we'll accept drives all the way through until Saturday morning - but remember, it's FIFO! It will be a first come, first served to duplicate 'till we drop. Bring labeled 6TB SATA blank drives, and submit them in the queue for the data you want. Come back in 14-24 hours to pick up your data-packed drive. Space allowing, the last drop-offs will be no later than Saturday afternoon and the last drives will run overnight with the final pickup time at 11:30am.

WHAT IS AVAILABLE - Three drives:
6TB drive 1-3: Updated archive of infocon.org plus other "direct from DT" content, built on last years collection and always adding more for your data consuming appetite. 6TB drive 2-3: freerainbowtables.com GSM A51 and MD5 hash tables (Tables 1-2) with about 404 gigs free 6TB drive 3-3: more rainbowtables, lanman, mysqlsha1, ntlm, and some word lists (Tables 2-2) with about 136 gigs free

The DC 29 content will be posted at dcddv.org once finalized

WHAT YOU NEED

- 6TB SATA3 512e format 7200rpm drive - one for each source you want

If you want a full copy of everything you will need three drives. You can bring back last year's drive(s) to be wiped / updated (you should remove any 2018 stickers).

WHEN TO BE THERE
Data Duplication Village Hours:

- Thursday, August 5 16:00 - 19:00 (drop off only)
- Friday, August 6 10:00 - 17:00
- Saturday, August 7 10:00 - 17:00
- Sunday, August 8 10:00 - 11:00 (last chance pickup only)
- Space permitting, last drop off is Saturday at 3:00pm.
- Last chance pickup is Sunday from 10:00 to 11:00.

We're working on a method to post completed ticket ranges to https://dcddv.org and https://twitter.com/DDV_DC

SIDE NOTES
Be aware that we cleared all the Vegas area stores of every single 6TB drive last year we did this so plan ahead and get them now! Duplicating a 6TB (About 5.46 usable) drive at an average of 120 Megabytes a second comes out to just under 14 hours per drive. With all about 16 duplicators going, we can duplicate about 95 drives concurrently. We're expect to push about 11GB per second out to the drives for 72 hours straight. We did 335 drives for DC24 and we're hoping to do even more at DC25! We are expecting more total duplicator capacity than last year!

THAT'S ALL?
But wait - there's more! At DC27, we made our our stretch goal a reality to provide a pick-and-pull datastore in the DDV. We expect to do it bigger and better this year!

Return to Index

HTSV - Hack the Sea Village

HTSV VillageTalk List:
Home Page: https://hackthesea.org/
DC Forums Page: https://forum.defcon.org/node/236575

DC Discord Chan: https://discord.com/channels/708208267699945503/732733427823935589
Social Media Links:
TW @hack_the_sea

Hack The Sea Village 3.0, Deep Dive, will be an opportunity for DEF CON attendees to explore the world of underwater robotics, seasteading communities, and hacking with maritime industrial control systems (ICS) and operational technology (OT) through hands-on CTFs, show-and-tells with gear and tools, talks, and hackathon style contests.

With this year's focus on undersea technology, especially robotics and UUV/ROVs we will provide attendees an opportunity to explore the "last frontier" on Earth.

Return to Index

HRV - Ham Radio Village

HRV VillageTalk List:
Home Page: https://hamvillage.org/
Sched Page: https://hamvillage.org/dc29.html
DC Forums Page: https://forum.defcon.org/node/236540
DC Discord Chan: https://discord.com/channels/708208267699945503/732733631667372103
Hours: Sat: 11:00 - 16:45 - Sun: 11:00 - 16:45
Social Media Links:
TW @HamRadioVillage
TI @HamRadioVillage
DC https://discord.gg/hrv

Ham radio isnt just what your grandpa does in the shed out back. Radios are an important piece of technology we use everyday, and amateur (ham) radio has been at the forefront of its development since day one -- we are some of the original hardware hackers! DIY, exploration, and sharing has always been a vital part of our community and the goal of Ham Radio Village is to nurture this growth into the next generation with all of the amazing people at DEF CON.

Our village will have demos, talks, presentations, contests, and of course, license exams!

So come visit Ham Radio Village to learn more about the hobby, including how antennas work (and how to build your own), how to actually use that software defined radio sitting on the shelf, how to trackdown a rogue transmitter with a handheld radio, and how you can legally transmit 1,500 Watts into the airwaves after taking a simple multiple-choice test!

One of the unique things about ham radio is that it goes deep into the theory and science of radio. This knowledge unlocks a whole new level of understanding about why and how radios work and radio waves propagate. With just about everything containing some sort of radio these days, this information can help us better research, attack, and defend all things that emit RF. For example: Just about anyone can build an antenna with simple hardware; having an understanding of the fundamentals allows you to troubleshoot and tune the performance of that antenna to pick up the exact signals you want while filtering out the rest.

Return to Index

HHV - Hardware Hacking and Soldering Skills Village

HHV VillageTalk List:
Home Page: https://dchhv.org/
Sched Page: https://dchhv.org/schedule/schedule.html
DC Forums Page: https://forum.defcon.org/node/236523

DC Discord Chan: https://discord.com/channels/708208267699945503/732728536149786665
Hours: Fri: 09:30 - 18:00 - Sat: 08:30 - 16:30 - Sun: 09:00 - 15:30
Social Media Links:
TW @DC_HHV

Every day our lives become more connected to consumer hardware. Every day the approved uses of that hardware are reduced, while the real capabilities expand.

Come discover hardware hacking tricks and tips regain some of that capacity, and make your own use for things! We have interactive demos to help you learn new skills. We have challenges to compete against fellow attendees. We have some tools to help with your fever dream modifications. Come share what you know and learn something new.

We are two villages in one. We run a large number of tables for soldering when in person, and to allow people to understand that hardware is more than soldering we run the Hardware Hacking Village as embedded / reversing / hardware things other than soldering.

Return to Index

ICSV - IndustrialControlSystems Village

ICSV VillageTalk List:
Home Page: https://www.icsvillage.com/
DC Forums Page: https://forum.defcon.org/node/236564
DC Discord Chan: https://discord.com/channels/708208267699945503/735938018514567178
Social Media Links:
TW @ICS_Village
LI @icsvillage
YT link
TI @ics_village

Mission.
ICS Village is a non-profit organization with the purpose of providing education and awareness of Industrial Control System security. Connecting public, industry, media, policymakers, and others directly with ICS systems and experts. Providing educational tools and materials to increase understanding among media, policymakers, and the general population. Providing access to ICS for security researchers to learn and test. Hands on instruction for industry to defend ICS systems.

Why.
High profile Industrial Controls Systems security issues have grabbed headlines and sparked changes throughout the global supply chain. The ICS Village allows defenders of any experience level to understand these systems and how to better prepare and respond to the changing threat landscape.

Exhibits.
Interactive simulated ICS environments, such as Hack the Plan(e)t and Howdy Neighbor, provide safe yet realistic examples to preserve safe, secure, and reliable operations. We bring real components such as Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), Remote Telemetry Units (RTU), actuators, to simulate a realistic environment throughout different industrial sectors. Visitors can connect their laptops to assess these ICS devices with common security scanners, network sniffers to sniff the industrial traffic, and more!

The Village provides workshops, talks, and training classes.

Return to Index

IOTV - InternetOfThings Village

IOTV VillageTalk List:
Home Page: https://www.iotvillage.org/
Sched Page: https://www.iotvillage.org/defcon.html
DC Forums Page: https://forum.defcon.org/node/236542
DC Discord Chan: https://discord.com/channels/708208267699945503/732734565604655114
Hours: Fri: 10:00 - 21:15 - Sat: 10:00 - 21:00
Social Media Links:
TW @iotvillage
TW @ISEsecurity
TW @Villageidiotlab
LI @iotvillage
TI @iotvillage
YT https://www.youtube.com/c/IoTVillage/videos
DC https://discord.gg/tmZASSpNnP

IoT Village advocates for advancing security in the Internet of Things (IoT) industry through bringing researchers and industry together. IoT Village hosts talks by expert security researchers, interactive hacking labs, live bug hunting in the latest IoT tech, and competitive IoT hacking contests. Over the years IoT Village has served as a platform to showcase and uncover hundreds of new vulnerabilities, giving attendees the opportunity to learn about the most innovative techniques to both hack and secure IoT. IoT Village is organized by security consulting and research firm, Independent Security Evaluators (ISE), and the non-profit organization, Village Idiot Labs (VIL).

The IoT RED ALERT Contest forum is located here: https://forum.defcon.org/node/236432

Check out the official IoT Village Store for all your IoT Village swag!

Watch IoT Village In Action to get an idea of our content and our attendees.

Return to Index

LBV - Lock Bypass Village

LBV VillageTalk List:
Home Page: https://bypassvillage.org/
Sched Page: https://www.bypassvillage.org/#schedule
DC Forums Page: https://forum.defcon.org/node/236524
DC Discord Chan: https://discord.com/channels/708208267699945503/732732893830447175
Hours: Fri: 09:00 - 19:00 - Sat: 09:00 - 19:00 - Sun: 09:00 - 17:00
Social Media Links:
TW @bypassvillage
TI @bypassvillage

The Lock Bypass Village explores the world of hardware bypasses and techniques generally outside of the realm of cyber security and lockpicking. Come learn some of these bypasses, how to fix them, and have the opportunity to try them out for yourself.

Well be covering the basics, like the under-the-door-tool and latch slipping attacks, as well as an in depth look at more complicated bypasses. Learn about elevator hacking, attacking alarm systems at the sensor and communication line, and cut-away and display models of common hardware to show how it works on the inside.

Looking for a challenge? Show us you can use lock bypass to escape from a pair of standard handcuffs in under 30 seconds and receive a prize!

The lock bypass village is almost 100% hands on and is one of the only villages that has content about physical security. We strive to develop new content on a yearly basis to retain the interest of new and existing participants. This year we will be rebuilding all of our door displays to improve the production value, we will also have new displays that capture elevator security, double doors (with a deadbolt), forceable entry, some content on Access controls/Wiegand/RFID cloning, and other subjects.

Return to Index

LPV - Lock Pick Village

LPV VillageTalk List:
Home Page: https://toool.us/
Sched Page: https://bit.ly/LPVSchedule2021
DC Forums Page: https://forum.defcon.org/node/236917
DC Discord Chan: https://discord.com/channels/708208267699945503/732734164780056708
Social Media Links:
TW @toool
TI @toool_us
YT https://youtube.com/c/TOOOL-US

Want to tinker with locks and tools the likes of which you've only seen in movies featuring secret agents, daring heists, or covert entry teams?

Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficultly to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

Return to Index

PHV - Packet Hacking Village

PHV VillageTalk List:
Home Page: https://www.wallofsheep.com/
Sched Page: https://www.wallofsheep.com/pages/dc29#talksschedule
DC Forums Page: https://forum.defcon.org/node/236521
DC Discord Chan: https://discord.com/channels/708208267699945503/708242376883306526
Hours: Fri: 14:00 - 18:00 - Sat: 14:00 - 18:00
Social Media Links:
TW @wallofsheep
FB @wallofsheep
YT https://youtube.com/wallofsheep

TI @wallofsheep
PS https://www.periscope.tv/wallofsheep

The Packet Hacking Village is where youll find network shenanigans and a whole lot more. Theres exciting events, live music, competitions with awesome prizes, and tons of giveaways. PHV welcomes all DEF CON attendees and there is something for every level of security enthusiast from beginners to those seeking a black badge. Wall of Sheep gives attendees a friendly reminder to practice safe computing through strong end-to-end encryption. PHV Speakers, Workshops, and Walkthrough Workshops delivers high quality content for all skill levels. Packet Detective and Packet Inspector offers hands-on exercises to help anyone develop or improve their Packet-Fu. WoSDJCo has some of the hottest DJs at con spinning live for your enjoyment. Finally... Capture The Packet, the ultimate cyber defense competition that has been honored by DEF CON as a black badge event for seven of the eight years of its run.

Return to Index

PWV - Password Village

PWV VillageTalk List:
Home Page: https://passwordvillage.org/
Sched Page: https://passwordvillage.org/schedule.html
DC Forums Page: https://forum.defcon.org/node/236918
DC Discord Chan: https://discord.com/channels/708208267699945503/732733760742621214
Hours: Fri: 10:00 - 19:00 - Sat: 10:00 - 15:00 - Sun: 12:00 - 13:00
Social Media Links:
TW @PasswordVillage
TI @passwordvillage
YT link

Have you ever been curious about password cracking, but were too embarrassed to admit you don't know anything about it? Have you seen the news about major password data breaches, but failed to see what all the fuss is about? Have you always wanted to implement password auditing at your organization, but you didn't know where to begin? Or do you feel like password cracking could not ever possibly relate to your job function? Does the prospect of discovering a unique intersection between human psychology, mathematics, information security, and high-performance computing arouse you? If you answered 'yes' to any of these questions, or if you just really fucking love password cracking, then the first-ever Password Village at DEF CON is right for you!

The Password Village provides training, discussion, and hands-on access to hardware and techniques utilized in modern password cracking, with an emphasis on how password cracking relates to your job function and the real world . No laptop? No problem! Feel free to use one of our terminals to access a pre-configured GPU environment to run password attacks against simulated real-world passwords. Village staff and expert volunteers will be standing by to assist you with on-the-spot training and introductions to Hashcat, as well as other FOSS cracking applications.

Already a password cracking aficionado? Feel free to give a lightning talk, show off your skills, help a n00b learn the basics, or engage in riveting conversation with other password crackers. Regardless of whether you're just a little hash-curious, a veteran cracker still relying on rainbow tables, a novice desiring to learn more, or an expert eager to share, we guarantee there will be something for everyone at the Password Village!

Return to Index

PYV - Payment Village

PYV VillageTalk List:
Home Page: https://www.paymentvillage.org/

Sched Page: https://www.paymentvillage.org/schedule
DC Forums Page: https://forum.defcon.org/node/236919
DC Discord Chan: https://discord.com/channels/708208267699945503/732733473558626314
Social Media Links:
TW @paymentvillage
TI @paymentvillage
YT link

Payment technologies are an integral part of our lives, yet few of us know much about them. Have you ever wanted to learn how payments work? Do you know how criminals bypass security mechanisms on Point of Sales terminals, ATMs and digital wallets? Come to the Payment Village and learn about the history of payments. Well teach you how hackers gain access to banking endpoints, bypass fraud detection mechanisms, and ultimately, grab the money!

We're covering top notch topics of payment security, which is the intersection of RE, hardware, appsec domains related to money flows. This year we will be glad to provide more hands-on and tasks for participants, and we already have a few requests for talks and interest for our Village.

Return to Index

RCV - Recon Village

RCV VillageTalk List:
Home Page: https://www.reconvillage.org/
Sched Page: https://www.reconvillage.org/recon-village-defcon-29-talks
DC Forums Page: https://forum.defcon.org/node/236921
DC Discord Chan: https://discord.com/channels/708208267699945503/732733566051418193
Hours: Fri: 10:00 - 16:45 - Sat: 10:00 - 16:05
Social Media Links:
TW @ReconVillage
FB @reconvillage

Recon Village is an Open Space with Talks, Live Demos, Workshops, Discussions, CTFs, etc. with a common focus on Reconnaissance. The core objective of this village is to spread awareness about the importance of reconnaissance, open-source intelligence (OSINT), and demonstrating how even small information about a target can cause catastrophic damage to individuals and organizations.

Recon Village appeared at DEF CON 25, 26, 27, 28 as well as DEF CON China Beta and 1.0 and we received an overwhelming response from speakers, CTF/HackAThon participants, and attendees.

We strive to make Recon Village even better this time and are expecting more active participation from the attendees. It will be really great if we can get at least the same size space (or bigger) as we got in DEFCON 27.

We will be opening 'Call For Papers and Workshops' on 22nd March 2021.

We will have our Jeopardy Style OSINT CTF Contest throughout the Village timings. Based on the feedback from last year, we plan to make the CTF more challenging this year. The challenges will be around harvesting information about target organizations, their employee's social media profiles, their public svn/gits, password breach dumps, darknet, paste(s), etc. followed by active exploitation, bug hunting, investigation, and pentest scenarios of virtual targets. All the target organizations, employees, servers, etc. will be created by our team and hence will not attract any legal issues.

Similar to the last year, there will be Awesome rewards for CTF winners, along with free t-shirts, stickers, village coins, and other schwag which attendees can grab and show off.

Guess what! our Badge will also be more interesting this time and as usual, it will be free. P.S. We will not be selling our badges.

Return to Index

RFV - RF Village

RFV VillageTalk List:
Home Page: https://rfhackers.com/
Sched Page: https://rfhackers.com/calendar
DC Forums Page: https://forum.defcon.org/node/236546
DC Discord Chan: https://discord.com/channels/708208267699945503/732732595493666826
Social Media Links:
TW @rfhackers
TW @rf_ctf
link
DC https://discordapp.com/invite/JjPQhKy

After 14 years of evolution, from the WiFi Village, to the Wireless Village, RF Hackers Sanctuary presents: The Radio Frequency Village at DEF CON.

The Radio Frequency Village is an environment where people come to learn about the security of radio frequency (RF) transmissions, which includes wireless technology, applications of software defined radio (SDR), Bluetooth (BT), Zigbee, WiFi, Z-wave, RFID, IR and other protocols within the usable RF spectrum. As a security community we have grown beyond WiFi, and even beyond Bluetooth and Zigbee.

The RF Village includes talks on all manner of radio frequency command and control as well as communication systems. While everyone knows about the WiFi and Bluetooth attack surfaces, most of us rely on many additional technologies every day.

RF Hackers Sanctuary is supported by a group of experts in the area of information security as it relates to RF technologies. RF Hackers Sanctuarys common purpose is to provide an environment in which participants may explore these technologies with a focus on improving their skills through offense and defense. These learning environments are provided in the form of guest speakers, panels, and Radio Frequency Capture the Flag games, to promote learning on cutting edge topics as it relates to radio communications. We promise to still provide free WiFi. https://rfhackers.com/the-crew

Speaker and contest schedule can be found on our website: https://rfhackers.com/calendar

Co-located with the RF Village is the RF Capture the Flag. Come for the talks, stay for the practice and the competition.

Return to Index

RGV - Rogues Village

RGV VillageTalk List:
Home Page: https://foursuits.co/roguesvillage
DC Forums Page: https://forum.defcon.org/node/236525
DC Discord Chan: https://discord.com/channels/708208267699945503/732732701144121434
Hours: Fri: 10:00 - 18:00 - Sat: 10:00 - 18:00 - Sun: 10:00 - 14:00
Social Media Links:
TW @RoguesVillage
TI @roguesvillage

TW @foursuits_co
YT https://www.youtube.com/c/foursuits
IG @foursuits_co

Rogues Village is a place to explore alternative approaches and uses for security concepts, tools, and techniques by looking to non-traditional areas of knowledge. Incorporating expertise from the worlds of magic, sleight of hand, con games, and advantage play, this village has a special emphasis on the overlap between Social Engineering, Physical Security, and Playful Mischief.

Because we specialize in non-traditional approaches, Rogues Village can be an excellent entry point for people with a less established background in the security space. By introducing and engaging with existing topics in innovative, relatable, and frequently hands-on ways, they can become easier for people to approach and pick up for the first time.

Additionally, we are one of the few villages with a view that explicitly extends beyond the security space, meaning our perspective will necessarily include influences, ideas, and inspirations that are unique to Rogues Village.

Return to Index

SLV - Security Leaders Village

SLV VillageTalk List:
Home Page: https://securityleadersvillage.org/
DC Forums Page: https://forum.defcon.org/node/236924
Social Media Links:
TW @securityleader2
DC https://discord.gg/wn58YfQEND

Security Leaders Village

Many of us who started out learning how technology worked through the security community now have leadership roles. There are many of us who don't wear the title of suit well, however we're in these positions. There are also quite a few of us who aspire to these roles and responsibilities, and don't know where to go. The goals of this village are to provide better support to security leaders who did not take the traditional career path, and to assist those currently on their path to achieve more.

We have not paid attention to how the hacker community has developed a significant amount of leaders. They are responsible for the safety and security of much of our critical infrastructure, including finance, healthcare, energy, and transportation. This village recognizes and realizes that, and gives these leaders the tools they need to further succeed. It's also there to develop a new generation.

Return to Index

SEV - Social Engineering Village

SEV VillageTalk List:
Home Page: https://www.social-engineer.org/
DC Forums Page: https://forum.defcon.org/node/236549
DC Discord Chan: https://discord.com/channels/708208267699945503/732733952867172382
Social Media Links:
FB @socialengineerinc
TW @humanhacker
LI @social-engineer

YT https://www.youtube.com/user/SocialEngineerOrg

Virtual SEV will be the one stop shop for all your SE needs during DEF CON. We will have a Social Engineering Capture for the Flag for Teens, we are planning another SECTF4Kids and we are working on a brand new competition for virtual SEV for all the rest of us. We plan on having a few speeches and Q&A sessions all about social engineering. Come and hang out with us, virtually of course.

Return to Index

VMV - Voting Machine Village

VMV VillageTalk List:
Sched Page: https://docs.google.com/document/d/123a7PYCkxzR6U2eW0C_YjYNRXIXqSHBKebb4b830J1I/edit
DC Forums Page: https://forum.defcon.org/node/236925
DC Discord Chan: https://discord.com/channels/708208267699945503/732733881148506164
Social Media Links:
TW @votingvillagedc
YT link

Looking forward to #DEFCON29 Aug. 5-8, 2021! Voting Village explores voting machines, systems, and databases and works to promote a more secure democracy.

Return to Index

SOC - Social Activities: Parties/Meetups

SOC VillageTalk List:

Return to Index

MUS - Music

MUS VillageTalk List:
Home Page: https://defconmusic.org
Sched Page: https://defconmusic.org/sched.txt
Social Media Links:
TW @defcon_music
YT link
TI @defcon_music
TI @defcon_chill

Music Link All the Things:

https://www.twitch.tv/defcon_music
https://www.twitch.tv/defcon_chill
http://www.defconmusic.org/

Return to Index

WS - DEF CON Workshops

WS VillageTalk List:
Home Page: https://defcon.org/html/defcon-29/dc-29-workshops.html

Return to Index

DL - DEF CON DemoLabs

DL VillageTalk List:
Home Page: https://forum.defcon.org/node/236373

Return to Index

DC - DEF CON Talks

DC VillageTalk List:
Home Page: https://defcon.org/html/defcon-29/dc-29-index.html
Sched Page: https://defcon.org/html/defcon-29/dc-29-schedule.html
Social Media Links:
TW @defcon
FB @defcon
YT https://www.youtube.com/user/DEFCONConference
http://www.reddit.com/r/defcon
IG @wearedefcon
DC https://discord.gg/defcon

Return to Index

CON - Contests

CON VillageTalk List:

Return to Index

QCV - Queercon

QCV VillageTalk List:
Home Page: https://www.queercon.org/
Social Media Links:
TW @Queercon
FB @126504813280
DC https://discord.com/invite/jeG6Bh5

Return to Index

MISC - Misc

MISC VillageTalk List:

Return to Index

Talk/Event Schedule

Thursday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Thursday - 07:00 PDT

Return to Index - Locations Legend

BHV - Table Top Exercise - Deus Ex Machina (Pre-registration Required) -
DC - DEF CON Human Registration (Badge Pickup) Open -

Thursday - 08:00 PDT

Return to Index - Locations Legend

DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -

Thursday - 09:00 PDT

Return to Index - Locations Legend

DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC

Thursday - 10:00 PDT

Return to Index - Locations Legend

BHV - Biohacking Village CTF: Hospital Under Siege (Pre-Qual) (Pre-registration required) -
CON - Tin Foil Hat Contest -
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
PYV - Welcome to the Payment Village

Thursday - 11:00 PDT

Return to Index - Locations Legend

BHV - cont...(10:00-13:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-Qual) (Pre-registration required) -
CON - cont...(10:00-16:59 PDT) - Tin Foil Hat Contest -
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC

Thursday - 12:00 PDT

Return to Index - Locations Legend

BHV - cont...(10:00-13:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-Qual) (Pre-registration required) -
CON - cont...(10:00-16:59 PDT) - Tin Foil Hat Contest -
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
RFV - Frag, You’re it - Hacking Laser Tag - Eric Escobar
RFV - ESP8266, do you know what's inside your IoT? - JoshInGeneral
RFV - Using UAV in Military Zone Areas by GPS Spoofing with RF Devices - Mehmet Onder Key
RFV - Assless Chaps: a novel combination of prior work to crack MSCHAPv2, fast (or why MSCHAPv2 is so broken, it’s showing it’s whole ass) - singe,cablethief
RFV - RF Propagation and Visualization with DragonOS - cemaxecuter
SOC - Friends of Bill W. -

Thursday - 13:00 PDT

Return to Index - Locations Legend

BHV - cont...(10:00-13:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-Qual) (Pre-registration required) -
CON - cont...(10:00-16:59 PDT) - Tin Foil Hat Contest -
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
SOC - A&E Pool Party! -

Thursday - 14:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-16:59 PDT) - Tin Foil Hat Contest -
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Thursday - 15:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-16:59 PDT) - Tin Foil Hat Contest -
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
DDV - Data Duplication Village - Open for dropoff only -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Thursday - 16:00 PDT

Return to Index - Locations Legend

CON - cont...(10:00-16:59 PDT) - Tin Foil Hat Contest -
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
DDV - cont...(15:00-18:59 PDT) - Data Duplication Village - Open for dropoff only -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - Toxic BBQ -
SOC - QueerCon Party -

Thursday - 17:00 PDT

Return to Index - Locations Legend

BCV - COSTA (Coinbase Secure Trait Analyzer) - Peter Kacherginsky
BCV - DeFi Must Change or Hacks Will Accelerate - Kadan Stadelmann
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
DDV - cont...(15:00-18:59 PDT) - Data Duplication Village - Open for dropoff only -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(16:00-21:59 PDT) - Toxic BBQ -
SOC - cont...(16:00-17:59 PDT) - QueerCon Party -
SOC - Friends of Bill W. -

Thursday - 18:00 PDT

Return to Index - Locations Legend

CON - AutoDriving CTF -
DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
DDV - cont...(15:00-18:59 PDT) - Data Duplication Village - Open for dropoff only -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(16:00-21:59 PDT) - Toxic BBQ -
SOC - QueerCon Virtual Mixer

Thursday - 19:00 PDT

Return to Index - Locations Legend

DC - cont...(07:00-19:59 PDT) - DEF CON Human Registration (Badge Pickup) Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(16:00-21:59 PDT) - Toxic BBQ -

Thursday - 20:00 PDT

Return to Index - Locations Legend

DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(16:00-21:59 PDT) - Toxic BBQ -

Thursday - 21:00 PDT

Return to Index - Locations Legend

BCV - Flash Loans Demystified - Anto Joseph
BCV - Blockchain as a Threat Modeling Thinking Tool - Shinchul Park, Graduate Student
BCV - Subtle and Not So Subtle Ways to Lose Your Cryptocurrency - Josh McIntyre
BCV - Will Secure Element Really Help Strengthen the Security of Cryptocurrency Wallets? - Byeongcheol Yoo
BCV - Scaling Blockchains: A Novel Approach - Colin Cantrell
BCV - Towards Understanding the Unlimited Approval in Ethereum - Dabao Wang
BCV - Preventing Sandwich Attacks on DeFi Protocols using Recurrent and Recursive Zero Knowledge Proofs - Gokul Alex
MUS - Music - CTRL/RSM - CTRL/rsm
MUS - Music - Deep Therapy - Deep Therapy
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(16:00-21:59 PDT) - Toxic BBQ -

Thursday - 22:00 PDT

Return to Index - Locations Legend

MUS - Music - Abstrct - Abstrct
MUS - Music - Tense Future - Tense Future
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Thursday - 23:00 PDT

Return to Index - Locations Legend

MUS - Music - Dr. McGrew - Dr. McGrew
MUS - Music - FuzzyNop - FuzzyNop
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Friday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Friday - 00:00 PDT

Return to Index - Locations Legend

CON - Coindroids -
MUS - Music - DJ St3rling - DJ St3rling

Return to Index - Locations Legend

CON - cont...(00:00-23:59 PDT) - Coindroids -
MUS - Music - Acid T - Acid T

CON - cont...(00:00-23:59 PDT) - Coindroids -

Friday - 03:00 PDT

Return to Index - Locations Legend

CON - cont...(00:00-23:59 PDT) - Coindroids -

Friday - 04:00 PDT

Return to Index - Locations Legend

CON - cont...(00:00-23:59 PDT) - Coindroids -

Return to Index - Locations Legend

CON - cont...(00:00-23:59 PDT) - Coindroids -

Return to Index - Locations Legend

CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - DEF CON Bike Ride -

Friday - 07:00 PDT

Return to Index - Locations Legend

CLV - Cloud Village CTF - Registration -
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(06:00-11:59 PDT) - DEF CON Bike Ride -
ICSV - Tabletop Exercise - GRIMM

Return to Index - Locations Legend

CLV - cont...(07:00-12:15 PDT) - Cloud Village CTF - Registration -
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(06:00-11:59 PDT) - DEF CON Bike Ride -
DC - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -

Friday - 09:00 PDT

Return to Index - Locations Legend

AIV - Welcome. A Short Tour of Good and Bad AI in 2021 - AI Village Organizers
AIV - (09:30-10:59 PDT) - Intro to ML Workshop - Gavin Klondike
APV - AppSec Village Welcome and Introductions
APV - Colorful AppSec - Luis Gomes,Erez Yalon,Pedro Umbelino,Tanya Janca
ASV - Retired but not forgotten – A look at IFEs - Alex Lomas,Phil Eveleigh
ASV - A-ISAC CTF -- Pre-registration Required -
ASV - (09:30-10:20 PDT) - The Antenny Board Design and Fabrication Saga: Sweat and Tears Along the Supply Chain - Ang Cui
BTV - (09:30-10:30 PDT) - Yeet the leet with Osquery (Effective Threathunting Without Breaking Bank) - Sebastiaan Provost
BTV - (09:30-10:59 PDT) - Attack and Detect with Prelude Operator and Security Onion - Wes Lambert
CLV - cont...(07:00-12:15 PDT) - Cloud Village CTF - Registration -
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(06:00-11:59 PDT) - DEF CON Bike Ride -
CON - Darknet-NG -
DC - cont...(08:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - Welcome to Discord - Dark Tangent
DC - Making the DEF CON 29 Badge - Katie Whiteley,Michael Whiteley
HHV - (09:30-09:59 PDT) - Meetup: Some HHV challenges - rehr
HRV - Ham Radio Exams -
LBV - (09:30-10:30 PDT) - Bypass 101
PHV - Web App Penetration Testing Workshop - Sunny Wear
PHV - The War for Control of DNS Encryption - Paul Vixie

Friday - 10:00 PDT

Return to Index - Locations Legend

AIV - cont...(09:30-10:59 PDT) - Intro to ML Workshop - Gavin Klondike
APV - Summer of Fuzz: MacOS - Jeremy Brown
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(09:30-10:20 PDT) - The Antenny Board Design and Fabrication Saga: Sweat and Tears Along the Supply Chain - Ang Cui
ASV - AIAA CubeSat Hacking Workshop - World Premier of the videos -
ASV - ARINC 429 Lab -
ASV - Deep Space Networking -
ASV - Hack-A-Sat2 Satellite Platform -
ASV - Antenny -
ASV - HACMS Live Demo -
ASV - Lego Spike Hub -
ASV - ADSB Demo and Paper Airplanes -
ASV - (10:30-11:20 PDT) - Hack-A-Sat 2: The Good, The Bad and the Cyber-Secure - Bryce Kerley,Capt Aaron Bolen,Frank Pound,Steve Wood
BCV - Welcome Note
BCV - (10:15-11:30 PDT) - Key Note
BHV - Biohacking Village Welcome Keynote - Nina Alli
BHV - Biohacking Village CTF: Hospital Under Siege (Pre-registration required)
BICV - (10:30-10:30 PDT) - Why don’t we have IoT, daddy? - Jessica Hoffman
BTV - cont...(09:30-10:30 PDT) - Yeet the leet with Osquery (Effective Threathunting Without Breaking Bank) - Sebastiaan Provost
BTV - cont...(09:30-10:59 PDT) - Attack and Detect with Prelude Operator and Security Onion - Wes Lambert
BTV - (10:45-11:45 PDT) - Velociraptor - Dig Deeper - Mike Cohen
BTV - (10:45-12:15 PDT) - Windows Forensics 101 (Beginner) - Surya Teja Masanam
CHV - Ready, fire aim: Hacking State and Federal Law Enforcement Vehicles - Alissa Knight
CLV - cont...(07:00-12:15 PDT) - Cloud Village CTF - Registration -
CLV - Cloud Village Opening Keynote
CLV - (10:15-10:59 PDT) - Detection Challenges in Cloud Connected Credential Abuse Attacks - Rod Soto
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(06:00-11:59 PDT) - DEF CON Bike Ride -
CON - cont...(09:00-15:59 PDT) - Darknet-NG -
CON - DEF CON 29 CTF by OOO -
CON - OpenSOC Blue Team CTF -
CON - Secure Coding Tournament CTF -
CON - Red Team Village CTF - Qualifiers Part 1 -
CON - Red Alert ICS CTF -
CON - Beverage Cooling Contraption Contest -
CON - Car Hacking CTF -
CON - CMD+CTRL -
CON - Hack3r Runw@y -
CPV - New Face, Who Dis? Protecting Privacy in an Era of Surveillance - Mike Kiser
DC - cont...(08:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - Welcome To DEF CON - Dark Tangent & Making the DEF CON 29 Badge - Dark Tangent,Katie Whiteley,Michael Whiteley
DC - Gone Apple Pickin': Red Teaming macOS Environments in 2021 - Cedric Owens
DC - HTTP/2: The Sequel is Always Worse - James Kettle
DC - DEF CON Vendor Area Open
DC - Community Roundtable - (De)Criminalizing Hacking Around the Globe -

DDV - Data Duplication Village - Open -
DL - AIS Tools - Gary Kessler
DL - Mooltipass - Mathieu Stephan
DL - WiFi Kraken Lite - Mike Spicer,Henry Hill
HHV - Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables - Federico Lucifredi
HRV - cont...(09:00-15:59 PDT) - Ham Radio Exams -
HRV - Ham Radio Village Opening Remarks
HTSV - AIS Tools Demo (DEF CON) - Gary Kessler
ICSV - Keynote - PW Singer - PW Singer
ICSV - (10:30-11:30 PDT) - Tabletop Exercise - GRIMM
IOTV - Pentesting 101 -
IOTV - When Penetration Testing Isn’t Penetration Testing At All - Ted Harrington
IOTV - UART to UBOOT to ROOT -
IOTV - IoT Village Capture the Flag (CTF) -
IOTV - IoT Village Labs -
IOTV - Black Box Challenges -
IOTV - (10:45-11:30 PDT) - Representation Matters - Camille Eddy,Chloe Messdaghi
LBV - cont...(09:30-10:30 PDT) - Bypass 101
LBV - (10:30-11:30 PDT) - Tools 101
LPV - Intro To Lockpicking - TOOOL
PHV - cont...(09:00-10:59 PDT) - Web App Penetration Testing Workshop - Sunny Wear
PHV - Internet Protocol (IP) - Roy Feng
PYV - ATM Transaction Reversal Frauds (And how to fight them) - Hector Cuevas Cruz
RCV - Recon Village Keynote - Ben S
RCV - (10:55-11:25 PDT) - Using Passive DNS for gathering Business Intelligence - Andy Dennis
RGV - Top 10 BOGUS Biometrics! - Vic Harkness
SEV - SECTF4Kids (Pre-Registration Required) - Ryan M,Colin H
VMV - Voting Village Logistical Information Broadcast (Discord, Youtube, Twitch) -
VMV - (10:30-10:59 PDT) - Hacking to Save Democracy: What Technologists Need to Know About Election Administration - Eddie Perez
WS - The Joy of Reverse Engineering: Learning With Ghidra and WinDbg - Wesley McGrew
WS - Inspecting Signals from Satellites to Shock Collars - Eric Escobar,Trenton Ivey
WS - Analysis 101 and 102 for the Incident Responder - Kristy Westphal
WS - House of Heap Exploitation - James Dolan,Maxwell Dulin,Nathan Kirkland,Zachary Minneker

Friday - 11:00 PDT

Return to Index - Locations Legend

AIV - The Coming AI Hackers - Bruce Schneier
APV - Vulnerability Inheritance - Attacking companies and scoring bounties through 3rd party integrations - Gal Nagli
APV - AppSec Village Capture the Flag Starts -
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(10:00-11:30 PDT) - AIAA CubeSat Hacking Workshop - World Premier of the videos -
ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -
ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -
ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -
ASV - cont...(10:00-15:59 PDT) - Antenny -
ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -
ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -
ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -
ASV - cont...(10:30-11:20 PDT) - Hack-A-Sat 2: The Good, The Bad and the Cyber-Secure - Bryce Kerley,Capt Aaron Bolen,Frank Pound,Steve Wood
ASV - (11:30-11:55 PDT) - Steal This Drone: High-Assurance Cyber Military Systems - Darren Cofer
ASV - (11:30-12:59 PDT) - AIAA CubeSat Hacking Workshop - Virtual Lab #1 -
BCV - cont...(10:15-11:30 PDT) - Key Note
BCV - (11:30-11:59 PDT) - BCOS Village Contest Overview - Reddcoin
BHV - cont...(10:00-17:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-registration required)
BHV - The Digital Physiome - How wearables can (and are) transforming healthcare - Jennifer Goldsack,Jessilyn Dunn
BTV - cont...(10:45-11:45 PDT) - Velociraptor - Dig Deeper - Mike Cohen
BTV - cont...(10:45-12:15 PDT) - Windows Forensics 101 (Beginner) - Surya Teja Masanam
CCV - Getting Started with Decentralized Object Storage - Storj Team
CHV - Remotely Rooting Charging Station for fun and maybe profit - Huajiang "Kevin2600" Chen,Wu Ming
CLV - cont...(07:00-12:15 PDT) - Cloud Village CTF - Registration -
CLV - Cloud Village CTF -
CLV - The Fault in Our Stars - Attack vectors for APIs using AWS API Gateway Lambda Authorizers - Alexandre Sieira,Leonardo Viveiros
CLV - (11:45-12:05 PDT) - Exploiting the O365 Duo 2FA Misconfiguration (Lightning Talk) - Cassandra Young
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(06:00-11:59 PDT) - DEF CON Bike Ride -
CON - cont...(09:00-15:59 PDT) - Darknet-NG -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:30 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-14:59 PDT) - Secure Coding Tournament CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF - Qualifiers Part 1 -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-13:59 PDT) - Beverage Cooling Contraption Contest -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(10:00-15:59 PDT) - CMD+CTRL -
CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -
CPV - Welcome to Gold Bug -
CPV - (11:30-12:30 PDT) - How expensive is quantum factoring, really? - Craig Gidney
DC - cont...(08:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - 2021 - Our Journey Back To The Future Of Windows Vulnerabilities and the 0-days we brought back with us - Eran Segal,Tomer Bar
DC - Caught you - reveal and exploit IPC logic bugs inside Apple - Chuanda Ding,Yuebin Sun,Zhipeng Huo
DC - (11:30-12:30 PDT) - Community Roundtable - We can build it. We have the technology. So why aren't we? -

DC - (11:30-12:30 PDT) - Community Roundtable - Toward a Global IoT Code of Practice -
DDV - cont...(10:00-16:59 PDT) - Data Duplication Village - Open -
DL - cont...(10:00-11:50 PDT) - AIS Tools - Gary Kessler
DL - cont...(10:00-11:50 PDT) - Mooltipass - Mathieu Stephan
DL - cont...(10:00-11:50 PDT) - WiFi Kraken Lite - Mike Spicer,Henry Hill
HHV - Use a PortaProg to flash, dump, and test ISP and UPDI chips - Bradán Lane,Sara Cladlow
HRV - cont...(09:00-15:59 PDT) - Ham Radio Exams -
HRV - "Ask a Ham" Q&A -
HTSV - cont...(10:00-11:50 PDT) - AIS Tools Demo (DEF CON) - Gary Kessler
ICSV - cont...(10:30-11:30 PDT) - Tabletop Exercise - GRIMM
ICSV - (11:30-12:30 PDT) - Your Infrastructure is Encrypted: Protecting Critical Infrastructure from Ransomware - David Etue,Ernie Bio,Jamil Jaffer,Jennifer DeTrani
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(10:45-11:30 PDT) - Representation Matters - Camille Eddy,Chloe Messdaghi
IOTV - (11:45-12:30 PDT) - 1.21 Gigawatts! Vulnerabilities in Solar Panel Controllers - Waylon Grange
LBV - cont...(10:30-11:30 PDT) - Tools 101
LBV - (11:30-12:30 PDT) - Intro to RFID Hacking
LPV - Key Duplication - It's not just for the movies! - Tony Virelli
PHV - MITRE Engage: A Framework for Adversary Engagement Operations - Stan Bar,Gabby Raymond,Maretta Morovitz
PYV - Racing cryptoexchanges or how I manipulated the balances - Vahagan Vardanyan
RCV - cont...(10:55-11:25 PDT) - Using Passive DNS for gathering Business Intelligence - Andy Dennis
RCV - (11:35-12:05 PDT) - So You Want to OPSEC, Eh? - Ritu Gill
SEV - cont...(10:00-11:59 PDT) - SECTF4Kids (Pre-Registration Required) - Ryan M,Colin H
VMV - A Deep Dive on Vulnerability Disclosure for Election Systems - Tod Beardsley
VMV - (11:30-11:59 PDT) - Wireless Odyssey or why is the federal government permitting devices with wireless networking capability in federally certified voting machines? - Susan Greenhalgh
WS - cont...(10:00-13:59 PDT) - The Joy of Reverse Engineering: Learning With Ghidra and WinDbg - Wesley McGrew
WS - cont...(10:00-13:59 PDT) - Inspecting Signals from Satellites to Shock Collars - Eric Escobar,Trenton Ivey
WS - cont...(10:00-13:59 PDT) - Analysis 101 and 102 for the Incident Responder - Kristy Westphal
WS - cont...(10:00-13:59 PDT) - House of Heap Exploitation - James Dolan,Maxwell Dulin,Nathan Kirkland,Zachary Minneker

Friday - 12:00 PDT

Return to Index - Locations Legend

AIV - Algorithmic Ethics Bug Bounty Contest Announcement - Rumman Chowdhury
AIV - (12:30-12:59 PDT) - Microsoft ML Security Evasion Competition Details - Hyrum Anderson
APV - Cross-document messaging technology, how to hack it, and how to use it safely. - Chen Gour-Arie
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -
ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -
ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -
ASV - cont...(10:00-15:59 PDT) - Antenny -
ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -
ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -
ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -
ASV - cont...(11:30-12:59 PDT) - AIAA CubeSat Hacking Workshop - Virtual Lab #1 -
ASV - Threat Modeling for Space Hitchhikers - James Pavur
ASV - (12:30-12:55 PDT) - Evaluating Wireless Attacks on Real-World Avionics Hardware - Leeloo Granger
AVV - Adversary Village Kick-off - Abhijith B R
AVV - (12:15-12:59 PDT) - Adversary Village Keynote - David Kennedy
BCV - Polyswarm Talk - Kevin Leffew
BHV - cont...(10:00-17:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-registration required)
BHV - The Next Critical Infrastructure: Understanding the Bioeconomy - Charles Fracchia,Nathan Case
BICV - (12:30-12:30 PDT) - The Action Plan for Cyber Diversity! - Keith Chapman
BTV - cont...(10:45-12:15 PDT) - Windows Forensics 101 (Beginner) - Surya Teja Masanam
BTV - This is what we thought would happen in 2021 - Gert-Jan Bruggink
CAHV - F**k You, Pay Me - Knowing your worth and getting paid - Alyssa Miller,Liana McCrea
CAHV - Resume Reviewing
CAHV - Career Coaching
CCV - (12:30-12:59 PDT) - Privacy on Public Blockchains with SGX - Secret Network Team
CHV - Commercial Transportation: Trucking Hacking - Ben Gardiner
CLV - cont...(07:00-12:15 PDT) - Cloud Village CTF - Registration -
CLV - cont...(11:00-12:15 PDT) - Cloud Village CTF -
CLV - cont...(11:45-12:05 PDT) - Exploiting the O365 Duo 2FA Misconfiguration (Lightning Talk) - Cassandra Young
CLV - Attacking Modern Environments Series: Attack Vectors on Terraform Environments - Mazin Ahmed
CLV - (12:50-13:20 PDT) - Kubernetes Goat - Kubernetes Security Learning (Tool Demo) - Madhu Akula
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(09:00-15:59 PDT) - Darknet-NG -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:30 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-14:59 PDT) - Secure Coding Tournament CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF - Qualifiers Part 1 -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-13:59 PDT) - Beverage Cooling Contraption Contest -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(10:00-15:59 PDT) - CMD+CTRL -
CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -
CON - Blacks in Cybersecurity CTF -
CPV - cont...(11:30-12:30 PDT) - How expensive is quantum factoring, really? - Craig Gidney
CPV - (12:30-13:10 PDT) - CPV Through the Looking-Glass: How to Backdoor Diffie-Hellman (DC 24)
DC - cont...(08:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - cont...(11:30-12:30 PDT) - Community Roundtable - We can build it. We have the technology. So why aren't we? -

DC - cont...(11:30-12:30 PDT) - Community Roundtable - Toward a Global IoT Code of Practice -

DC - DHS REBOOTING CRITICAL INFRASTRUCTURE PROTECTION Panel with DEF CON Policy Panel - Lily Newman,Alexander Klimburg,Faye Francy,Eric Goldstein,Amelie Koran,Danny McPherson

DC - Your House is My House: Use of Offensive Enclaves In Adversarial Operations - Dimitry "Op_Nomad" Snezhkov

DC - Do you like to read? I know how to take over your Kindle with an e-book - Slava Makkaveev

DC - (12:30-12:50 PDT) - The Mechanics of Compromising Low Entropy RSA Keys - Austin Allshouse

DC - (12:30-12:50 PDT) - Worming through IDEs - David Dworken

DDV - cont...(10:00-16:59 PDT) - Data Duplication Village - Open -

DL - Solitude - Dan Hastings

DL - Siembol - Marian Novotny

HHV - The Black Box and the Brain Box: When Electronics and Deception Collide - Gigs

HHV - (12:30-13:30 PDT) - Walkthrough of DC 28 HHV Challenges - rehr

HRV - cont...(09:00-15:59 PDT) - Ham Radio Exams -

HRV - (12:30-13:30 PDT) - Spectrum Coordination for Amateur Radio - Bryan Fields

HTSV - Intro to SeaTF, Salty Sensor, and Tin Foil Competitions

ICSV - cont...(11:30-12:30 PDT) - Your Infrastructure is Encrypted: Protecting Critical Infrastructure from Ransomware - David Etue,Ernie Bio,Jamil Jaffer,Jennifer DeTrani

ICSV - (12:30-12:59 PDT) - Do We Really Want to Live in the Cyberpunk World? - Mert Can Kilic

IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -

IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -

IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -

IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -

IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -

IOTV - cont...(11:45-12:30 PDT) - 1.21 Gigawatts! Vulnerabilities in Solar Panel Controllers - Waylon Grange

IOTV - (12:45-13:15 PDT) - LED Light Lunacy! - Victor Hanna

LBV - cont...(11:30-12:30 PDT) - Intro to RFID Hacking

LPV - Intro To Lockpicking - TOOOL

PHV - Hunting Evil with Wireshark - Michael Wylie

PHV - Seeing Through The Windows: Centralizing Windows Logs For Greater Visibility - Matthew Gracie

PYV - Automated Tear Machines - Meadow Ellis

RCV - cont...(11:35-12:05 PDT) - So You Want to OPSEC, Eh? - Ritu Gill

RCV - (12:15-12:59 PDT) - OSINT and the Hermit Kingdom. Leveraging online sources to learn more about the worlds most secret nation - Nick Roy

SEV - (12:30-13:30 PDT) - Judging by the Cover: Profiling & Targeting Through Social Media - Christina Lekati

SOC - Friends of Bill W. -

VMV - A Journalist's Perspective on Fake News - Bob Sullivan

VMV - (12:30-12:59 PDT) - Are Barcodes on Ballots Bad? - Kevin Skoglund

WS - cont...(10:00-13:59 PDT) - The Joy of Reverse Engineering: Learning With Ghidra and WinDbg - Wesley McGrew

WS - cont...(10:00-13:59 PDT) - Inspecting Signals from Satellites to Shock Collars - Eric Escobar,Trenton Ivey

WS - cont...(10:00-13:59 PDT) - Analysis 101 and 102 for the Incident Responder - Kristy Westphal

WS - cont...(10:00-13:59 PDT) - House of Heap Exploitation - James Dolan,Maxwell Dulin,Nathan Kirkland,Zachary Minneker

Friday - 13:00 PDT

Return to Index - Locations Legend

AIV - Shell Language Processing (SLP) - Dmitrijs Trizna
AIV - (13:30-14:30 PDT) - Trailblazing the AI for Cybersecurity Discipline: Overview of the Field and Promising Future Directions - Sagar Samtani
APV - Signed, Sealed, Delivered: Abusing Trust in Software Supply Chain Attacks - Cheryl Biswas
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -
ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -
ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -
ASV - cont...(10:00-15:59 PDT) - Antenny -
ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -
ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -
ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -
ASV - Unboxing the Spacecraft Software BlackBox – Hunting for Vulnerabilities - Brandon Bailey
ASV - Understanding Space in the Cyber Domain -
AVV - Look at me, I'm the Adversary now: Introduction to Adversary Emulation and its place in Security Operations - Samuel Kimmons
AVV - (13:45-14:45 PDT) - From On-Prem to the Cloud - Hybrid AD attack path - Sergey Chubarov
BCV - Catching (and Fixing) an Unlimited Burn Vulnerability - Nadir Akhtar
BHV - cont...(10:00-17:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-registration required)
BHV - "Who Bears the Risk?" Why a Market Incentives Perspective is Critical to Protecting Patients from Cyber Threats - Matt McMahon,Shannon Lantzky
BHV - (13:30-14:30 PDT) - At least ten questions for “Bad HIPPA Takes” (@BadHIPPA), 2021’s best tweeter on privacy, pandemic, and snark. - Lucia Savage
BTV - (13:30-13:59 PDT) - Forensicating Endpoint Artifacts in the World of Cloud Storage Services - Renzon Cruz
CAHV - cont...(12:00-15:59 PDT) - Resume Reviewing
CAHV - cont...(12:00-15:59 PDT) - Career Coaching
CAHV - Hacking Your Career: The Options - Chris Sperry,Deb Herrity,Jennifer Haverman
CHV - From CTF to CVE - Bill Hatzer
CLV - cont...(12:50-13:20 PDT) - Kubernetes Goat - Kubernetes Security Learning (Tool Demo) - Madhu Akula
CLV - (13:20-14:05 PDT) - Hunting for AWS Exposed Resources - Felipe Pr0teus Espósito
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(09:00-15:59 PDT) - Darknet-NG -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:30 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-14:59 PDT) - Secure Coding Tournament CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF - Qualifiers Part 1 -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-13:59 PDT) - Beverage Cooling Contraption Contest -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(10:00-15:59 PDT) - CMD+CTRL -
CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -
CON - cont...(12:00-17:59 PDT) - Blacks in Cybersecurity CTF -
CPV - cont...(12:30-13:10 PDT) - CPV Through the Looking-Glass: How to Backdoor Diffie-Hellman (DC 24)
DC - cont...(08:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - Ransomeware’s Big Year – from nuisance to “scourge”? - DEF CON Policy Panel
DC - Sleight of ARM: Demystifying Intel Houdini - Brian Hong
DC - eBPF, I thought we were friends! - Guillaume Fournier,Sylvain Afchain,Sylvain Baubeau
DC - Policy Debrief - Myths and Legends of Section 230 -

DDV - cont...(10:00-16:59 PDT) - Data Duplication Village - Open -
DL - cont...(12:00-13:50 PDT) - Solitude - Dan Hastings
DL - cont...(12:00-13:50 PDT) - Siembol - Marian Novotny
HHV - cont...(12:30-13:30 PDT) - Walkthrough of DC 28 HHV Challenges - rehr
HHV - (13:30-14:30 PDT) - A Lazy r2 Solve of @mediumrehr Challenge 6 - Ben Gardiner
HRV - cont...(09:00-15:59 PDT) - Ham Radio Exams -
HRV - cont...(12:30-13:30 PDT) - Spectrum Coordination for Amateur Radio - Bryan Fields
HTSV - AIS Protocol Internals (Abridged) - Gary Kessler
ICSV - Tabletop Exercise - GRIMM
ICSV - Beetlejuice: The Lessons We Should Have Learned For ICS Cybersecurity - Tim Yardley
ICSV - (13:30-13:59 PDT) - Scripts and Tools to Help Your ICS InfoSec Journey - Don C. Weber
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(12:45-13:15 PDT) - LED Light Lunacy! - Victor Hanna
IOTV - (13:30-14:15 PDT) - 5 years of IoT vulnerability research and countless 0days - A retrospective - Alex "Jay" Balan
LBV - (13:30-14:30 PDT) - Alarm Bypass
LPV - Are We Still Doing it? 10 Locksport Hobbies that go Beyond Lock Picking - Lock Noob
PHV - cont...(12:00-13:59 PDT) - Hunting Evil with Wireshark - Michael Wylie
PYV - What happens when businesses decide to enroll cryptocurrency cards - Timur Yunusov
SEV - cont...(12:30-13:30 PDT) - Judging by the Cover: Profiling & Targeting Through Social Media - Christina Lekati
SEV - (13:30-14:30 PDT) - SE Team vs. Red Team - Ryan MacDougall
SOC - A&E Pool Party! -
VMV - Hack the Conspiracies - Barb Byrum
VMV - (13:30-13:59 PDT) - Kickoff Remarks (recorded in-person in Las Vegas) - Harri Hursti
WS - cont...(10:00-13:59 PDT) - The Joy of Reverse Engineering: Learning With Ghidra and WinDbg - Wesley McGrew
WS - cont...(10:00-13:59 PDT) - Inspecting Signals from Satellites to Shock Collars - Eric Escobar,Trenton Ivey
WS - cont...(10:00-13:59 PDT) - Analysis 101 and 102 for the Incident Responder - Kristy Westphal
WS - cont...(10:00-13:59 PDT) - House of Heap Exploitation - James Dolan,Maxwell Dulin,Nathan Kirkland,Zachary Minneker

Friday - 14:00 PDT

Return to Index - Locations Legend

AIV - cont...(13:30-14:30 PDT) - Trailblazing the AI for Cybersecurity Discipline: Overview of the Field and Promising Future Directions - Sagar Samtani
AIV - (14:30-14:59 PDT) - AI Policy Talk: "An AI Security ISAC" and "An AI Playbook" - Sagar Samtani
APV - Poking bots for fun and profit in the age of asynchronous stuff - Emanuel Rodrigues
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -
ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -
ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -
ASV - cont...(10:00-15:59 PDT) - Antenny -
ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -
ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -
ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -
ASV - cont...(13:00-15:59 PDT) - Understanding Space in the Cyber Domain -
ASV - AIAA CubeSat Hacking Workshop - Virtual Lab #2 -
ASV - Don't fear the BUS, it won't run you over. - Nicholas Childs
ASV - (14:30-14:55 PDT) - CPDLC: Man-in-the-middle attacks and how to defend against them - Joshua Smailes
AVV - cont...(13:45-14:45 PDT) - From On-Prem to the Cloud - Hybrid AD attack path - Sergey Chubarov
AVV - (14:45-15:45 PDT) - Exploiting Blue Team OPSEC failures with RedELK - Marc Smeets
BCV - Blockchain Security Tools - Mila Paul
BCV - (14:30-15:59 PDT) - Workshop - Decentralized Cloud
BHV - cont...(10:00-17:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-registration required)
BHV - cont...(13:30-14:30 PDT) - At least ten questions for “Bad HIPPA Takes” (@BadHIPPA), 2021’s best tweeter on privacy, pandemic, and snark. - Lucia Savage
BHV - (14:30-14:59 PDT) - Open-Source Vaccine Developer Kits (VDKs) with RaDVaC - Alex Hoekstra
BICV - (14:30-14:30 PDT) - The Big Cleanup: Tackling The Remnants of Systematic Discrimination in the Tech Industry - Maurice Turner
BTV - MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part1 - Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges
BTV - (14:15-15:15 PDT) - Adventures in Pro Bono Digital Forensics Work - John Bambenek
CAHV - cont...(12:00-15:59 PDT) - Resume Reviewing
CAHV - cont...(12:00-15:59 PDT) - Career Coaching
CAHV - Making the Leap - Changing Careers - Danyelle Davis
CCV - Hardware Wallet Show and Tell - Michael Schloh von Bennewitz
CHV - Bug Hunter's Guide to Bashing for a Car Hacking Bug Bash or Contest - Jay Turla
CLV - cont...(13:20-14:05 PDT) - Hunting for AWS Exposed Resources - Felipe Pr0teus Espósito
CLV - WhoC - Peeking under the hood of CaaS offerings - Yuval Avrahami
CLV - (14:35-16:59 PDT) - Kubernetes Security 101: Best Practices to Secure your Cluster (Workshop) - Magno Logan
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(09:00-15:59 PDT) - Darknet-NG -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:30 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-14:59 PDT) - Secure Coding Tournament CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF - Qualifiers Part 1 -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(10:00-15:59 PDT) - CMD+CTRL -
CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -
CON - cont...(12:00-17:59 PDT) - Blacks in Cybersecurity CTF -
CPV - Playing God: How ambiguities in state and federal breach notification laws give lawyers too much discretion in deciding whether or not to disclose potential data breaches - Anthony Hendricks,Jordan Sessler
CPV - (14:45-14:59 PDT) - Lightning Talk: Differential Privacy and Census Data - Wendy Edwards

DC - cont...(08:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - MAVSH> Attacking from Above - Sach
DC - Hacking Humans with AI as a Service - Eugene Lim,Glenice Tan,Tan Kee Hock
DC - Rotten code, aging standards, & pwning IPv4 parsing across nearly every mainstream programming language - Kelly Kaoudis,Sick Codes
DC - (14:30-15:30 PDT) - Community Roundtable - Zero Trust, Critical Software, and a Cyber Safety Review Board -
DC - (14:30-15:30 PDT) - Policy Debrief - Global Cyber Capacity Building - triple challenge or triple opportunity? -
DDV - cont...(10:00-16:59 PDT) - Data Duplication Village - Open -
DL - Kubestriker - Vasant Chinnipilli
DL - Zuthaka - Lucas Bonastre
DL - Open Bridge - Constantine Macris
DL - Empire - Anthony "Cx01N" Rose,Vincent "Vinnybod" Rose
HHV - cont...(13:30-14:30 PDT) - A Lazy r2 Solve of @mediumrehr Challenge 6 - Ben Gardiner
HHV - (14:30-14:59 PDT) - Meetup: PCB Proto and Rework - K
HRV - cont...(09:00-15:59 PDT) - Ham Radio Exams -
HRV - Discord Practice Net -
HTSV - In-person broadcast via demolabs - Constantine Macris
ICSV - Consider the (Data) Source - Dan Gunter
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(13:30-14:15 PDT) - 5 years of IoT vulnerability research and countless 0days - A retrospective - Alex "Jay" Balan
IOTV - (14:30-15:15 PDT) - BLUEMONDAY Series – Exploitation & Mapping of vulnerable devices at scale through self-registration services (DATTO/ EGNYTE/ SYNOLOGY/ MERAKI/ GEOVISION) - Ken Pyle
LBV - cont...(13:30-14:30 PDT) - Alarm Bypass
LPV - (14:15-14:45 PDT) - Intro To Lockpicking - TOOOL
RCV - Finding Hidden Gems via URL Shortener Services - Utku Sen
RCV - (14:40-15:10 PDT) - Using OSINT to Aid in Human Trafficking and Smuggling Cases - Rae
RGV - The Neuroscience of Magic (Registration required) - Daniel Roy
SEV - cont...(13:30-14:30 PDT) - SE Team vs. Red Team - Ryan MacDougall
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - BADASS Meetup (Virtual) -

Friday - 15:00 PDT

Return to Index - Locations Legend

AIV - Identifying Excel 4.0 Macro strains using Anomaly Detection - Elad Ciuraru,Tal Leibovich
AIV - (15:30-16:30 PDT) - Workshop on Microsoft Counterfit - Will Pearce
APV - Scaling static analysis for free: add additional codebases with a single line of code and no money - Erin Browning,Tim Faraci
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -
ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -
ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -
ASV - cont...(10:00-15:59 PDT) - Antenny -
ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -
ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -
ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -
ASV - cont...(13:00-15:59 PDT) - Understanding Space in the Cyber Domain -
ASV - cont...(14:00-15:59 PDT) - AIAA CubeSat Hacking Workshop - Virtual Lab #2 -
ASV - Developing Aerospace Security Training 3D Models - Kevin Hood
ASV - (15:30-15:55 PDT) - Collecting CANs: a Bridge Less Traveled - Peace Barry
AVV - cont...(14:45-15:45 PDT) - Exploiting Blue Team OPSEC failures with RedELK - Marc Smeets
AVV - (15:45-16:45 PDT) - Everything is a C2 if you're brave enough - Luis Ángel Ramírez Mendoza,Mauro Cáseres Rozanowski
BCV - cont...(14:30-15:59 PDT) - Workshop - Decentralized Cloud
BHV - cont...(10:00-17:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-registration required)
BHV - Truth, Trust, and Biodefense - Eric Perakslis
BHV - (15:30-15:59 PDT) - Healthcare Innovation With People of All Abilities - Joel Isaac,Pia Zaragoza
BTV - cont...(14:00-17:59 PDT) - MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part1 - Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges
BTV - cont...(14:15-15:15 PDT) - Adventures in Pro Bono Digital Forensics Work - John Bambenek
BTV - (15:30-16:30 PDT) - Uncovering covert network behaviors within critical infrastructure environments - Michael Raggo,Chester Hosmer
CAHV - cont...(12:00-15:59 PDT) - Resume Reviewing
CAHV - cont...(12:00-15:59 PDT) - Career Coaching
CAHV - This Job Ad Sucks - Kirsten Renner
CHV - Remote Adversarial Phantom Attacks against Tesla and Mobileye - Ben Nassi
CLV - cont...(14:35-16:59 PDT) - Kubernetes Security 101: Best Practices to Secure your Cluster (Workshop) - Magno Logan
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(09:00-15:59 PDT) - Darknet-NG -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:30 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF - Qualifiers Part 1 -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(10:00-15:59 PDT) - CMD+CTRL -
CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -
CON - cont...(12:00-17:59 PDT) - Blacks in Cybersecurity CTF -
CPV - So What? The CFAA after Van Buren - Kendra Albert
CPV - (15:30-16:30 PDT) - CPV Through the Looking-Glass: Adversarial Fashion (DC 27)
DC - cont...(08:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - cont...(14:30-15:30 PDT) - Community Roundtable - Zero Trust, Critical Software, and a Cyber Safety Review Board -
DC - cont...(14:30-15:30 PDT) - Policy Debrief - Global Cyber Capacity Building - triple challenge or triple opportunity? -

DC - UFOs: Misinformation, Disinformation, and the Basic Truth - Richard Thieme AKA neuralcowboy
DC - Abusing SAST tools! When scanners do more than just scanning - Rotem Bar
DC - ProxyLogon is Just the Tip of the Iceberg, A New Attack Surface on Microsoft Exchange Server! - Orange Tsai
DC - (15:30-16:30 PDT) - Community Roundtable - 10 years after SOPA: where are we now? -
DDV - cont...(10:00-16:59 PDT) - Data Duplication Village - Open -
DL - cont...(14:00-15:50 PDT) - Kubestriker - Vasant Chinnipilli
DL - cont...(14:00-15:50 PDT) - Zuthaka - Lucas Bonastre
DL - cont...(14:00-15:50 PDT) - Open Bridge - Constantine Macris
DL - cont...(14:00-15:50 PDT) - Empire - Anthony "Cx01N" Rose,Vincent "Vinnybod" Rose
HHV - Robo Sumo On site - ShortTie
HHV - (15:30-15:59 PDT) - Meetup: Legacy Hardware - K
HRV - cont...(09:00-15:59 PDT) - Ham Radio Exams -
HTSV - cont...(14:00-15:50 PDT) - In-person broadcast via demolabs - Constantine Macris
ICSV - Approaches to Attract, Develop, and Retain an Industrial Cybersecurity Workforce - John Ellis,Julia Atkinson
ICSV - (15:30-15:59 PDT) - It Takes a Village (and a generous grant): Students Performing ICS Security Assessments - Alexander Vigovskiy,Christopher Von Reybyton,Dennis Skarr
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(14:30-15:15 PDT) - BLUEMONDAY Series – Exploitation & Mapping of vulnerable devices at scale through self-registration services (DATTO/ EGNYTE/ SYNOLOGY/ MERAKI/ GEOVISION) - Ken Pyle
IOTV - (15:30-16:15 PDT) - “Alexa, have you been compromised?” — Exploitation of Voice Assistants in Healthcare (and other business contexts) - Hutch (Justin Hutchens)
LPV - Doors, Cameras, and Mantraps OH MY! - Dylan The Magician
RCV - cont...(14:40-15:10 PDT) - Using OSINT to Aid in Human Trafficking and Smuggling Cases - Rae
RCV - (15:20-16:05 PDT) - Venator: Hunting & Smashing Trolls on Twitter - Mauro Cáseres Rozanowski
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(14:00-15:59 PDT) - BADASS Meetup (Virtual) -
WS - Windows Internals - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - Secure messaging over unsecured transports - Ash
WS - Learning to Hack Bluetooth Low Energy with BLE CTF - Ryan Holeman
WS - Writing Golang Malware - Benjamin Kurtz

Friday - 16:00 PDT

Return to Index - Locations Legend

AIV - cont...(15:30-16:30 PDT) - Workshop on Microsoft Counterfit - Will Pearce
AIV - (16:30-16:59 PDT) - AI Discord Happy Hour - Open Discussion on AIV Discord about the State of AI Security
APV - DFDs Ain't That Bad - Izar Tarandach,Matthew Coles
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - Holistic View of a Flight with Crowd Sourced Data - Allan Tart
AVV - cont...(15:45-16:45 PDT) - Everything is a C2 if you're brave enough - Luis Ángel Ramírez Mendoza,Mauro Cáseres Rozanowski
AVV - (16:45-17:45 PDT) - Designing a C2 Framework - Daniel "Rasta" Duggan
BCV - Surviving 51% Attacks on Blockchains - Yaz Khoury
BCV - (16:30-17:30 PDT) - Do You Really Own Your NFTs? - Francesco Piccoli,Steven Yang
BHV - cont...(10:00-17:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-registration required)
BHV - No Aggregation Without Representation - Andrea Downing
BTV - cont...(14:00-17:59 PDT) - MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part1 - Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges
BTV - cont...(15:30-16:30 PDT) - Uncovering covert network behaviors within critical infrastructure environments - Michael Raggo,Chester Hosmer
BTV - (16:30-17:59 PDT) - Watch Out! And just skip the packer - Felipe Duarte
BTV - (16:45-17:15 PDT) - A SERVERLESS SIEM: DETECTING ALL BADDIES ON A BUDGET - Chen Cao
CCV - State of Cryptocurrency Ransomware AMA - Guillermo Christensen
CLV - cont...(14:35-16:59 PDT) - Kubernetes Security 101: Best Practices to Secure your Cluster (Workshop) - Magno Logan
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:30 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-16:59 PDT) - Red Team Village CTF - Qualifiers Part 1 -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cybersecurity CTF -
CPV - cont...(15:30-16:30 PDT) - CPV Through the Looking-Glass: Adversarial Fashion (DC 27)
CPV - (16:30-17:30 PDT) - Piecing Together Your Personal Privacy Profile - Margaret Fero
DC - cont...(08:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - cont...(15:30-16:30 PDT) - Community Roundtable - 10 years after SOPA: where are we now? -
DC - Defending against nation-state (legal) attack: how to build a privacy-protecting service in the era of ubiquitous surveillance - Bill "Woody" Woodcock
DC - Bundles of Joy: Breaking macOS via Subverted Applications Bundles - Patrick Wardle
DC - The Unbelievable Insecurity of the Big Data Stack: An Offensive Approach to Analyzing Huge and Complex Big Data Infrastructures - Sheila A. Berta
DC - Community Roundtable - Volunteer Hacker Fire Department -
DDV - cont...(10:00-16:59 PDT) - Data Duplication Village - Open -
HRV - Remote Ham Radio Exams -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(15:30-16:15 PDT) - “Alexa, have you been compromised?” — Exploitation of Voice Assistants in Healthcare (and other business contexts) - Hutch (Justin Hutchens)
IOTV - (16:30-17:15 PDT) - IoT Testing Crash Course - Tim Jensen (EapolSniper)
LBV - Expoiting Retail Security with Tiktok's Hacker Community

LPV - (16:15-16:45 PDT) - Intro To Lockpicking - TOOOL
RCV - cont...(15:20-16:05 PDT) - Venator: Hunting & Smashing Trolls on Twitter - Mauro Cáseres Rozanowski
RCV - (16:15-16:45 PDT) - People Hunting: A Pentesters Perspective - Mishaal Khan
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - QueerCon Virtual Pool Party
SOC - QueerCon Party -
WS - cont...(15:00-18:59 PDT) - Windows Internals - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(15:00-18:59 PDT) - Secure messaging over unsecured transports - Ash
WS - cont...(15:00-18:59 PDT) - Learning to Hack Bluetooth Low Energy with BLE CTF - Ryan Holeman
WS - cont...(15:00-18:59 PDT) - Writing Golang Malware - Benjamin Kurtz

Friday - 17:00 PDT

Return to Index - Locations Legend

APV - (17:30-17:35 PDT) - AppSec Quiz Time! - Eden Stroet
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
AVV - cont...(16:45-17:45 PDT) - Designing a C2 Framework - Daniel "Rasta" Duggan
AVV - (17:45-19:59 PDT) - (Workshop) Tradecraft Development in Adversary Simulations - Fatih Ozavci
BCV - cont...(16:30-17:30 PDT) - Do You Really Own Your NFTs? - Francesco Piccoli,Steven Yang
BHV - cont...(10:00-17:59 PDT) - Biohacking Village CTF: Hospital Under Siege (Pre-registration required)
BHV - Lets Get Real About The Future State of Healthcare - Christian Dameff,Jeff 'R3plicant' Tully
BTV - cont...(14:00-17:59 PDT) - MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part1 - Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges
BTV - cont...(16:30-17:59 PDT) - Watch Out! And just skip the packer - Felipe Duarte
BTV - cont...(16:45-17:15 PDT) - A SERVERLESS SIEM: DETECTING ALL BADDIES ON A BUDGET - Chen Cao
BTV - (17:30-17:59 PDT) - Scope X: Hunt in the Ocean! - Meisam Eslahi
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:30 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(12:00-17:59 PDT) - Blacks in Cybersecurity CTF -
CON - EFF Tech Trivia -
CPV - cont...(16:30-17:30 PDT) - Piecing Together Your Personal Privacy Profile - Margaret Fero
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - Do No harm; Health Panel : Live version - A DEF CON Policy Panel - DEF CON Policy Panel
DC - Phantom Attack: Evading System Call Monitoring - Junyuan Zeng,Rex Guo
DC - Warping Reality - creating and countering the next generation of Linux rootkits using eBPF - PatH
HHV - (17:30-17:59 PDT) - Meetup: Some HHV challenges - rehr
HRV - cont...(16:00-17:59 PDT) - Remote Ham Radio Exams -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(16:30-17:15 PDT) - IoT Testing Crash Course - Tim Jensen (EapolSniper)
IOTV - (17:30-18:15 PDT) - Defending IoT in the Future of High-Tech Warfare - Harshit Agrawal
LBV - cont...(16:00-17:59 PDT) - Expoiting Retail Security with Tiktok's Hacker Community
LPV - Law School for Lockpickers - Preston Thomas
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(16:00-17:59 PDT) - QueerCon Virtual Pool Party
SOC - cont...(16:00-17:59 PDT) - QueerCon Party -
SOC - Friends of Bill W. -
WS - cont...(15:00-18:59 PDT) - Windows Internals - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(15:00-18:59 PDT) - Secure messaging over unsecured transports - Ash
WS - cont...(15:00-18:59 PDT) - Learning to Hack Bluetooth Low Energy with BLE CTF - Ryan Holeman
WS - cont...(15:00-18:59 PDT) - Writing Golang Malware - Benjamin Kurtz

Friday - 18:00 PDT

Return to Index - Locations Legend

AVV - cont...(17:45-19:59 PDT) - (Workshop) Tradecraft Development in Adversary Simulations - Fatih Ozavci
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(17:00-19:59 PDT) - EFF Tech Trivia -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - cont...(17:00-18:59 PDT) - Do No harm; Health Panel : Live version - A DEF CON Policy Panel - DEF CON Policy Panel
DC - Response Smuggling: Pwning HTTP/1.1 Connections - Martin Doyhenard
DC - How I use a JSON Deserialization 0day to Steal Your Money On The Blockchain - Hao Xing,Zekai Wu
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(17:30-18:15 PDT) - Defending IoT in the Future of High-Tech Warfare - Harshit Agrawal
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - Lawyers Meet -
SOC - Hacker Karaoke (Virtual) -
WS - cont...(15:00-18:59 PDT) - Windows Internals - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(15:00-18:59 PDT) - Secure messaging over unsecured transports - Ash
WS - cont...(15:00-18:59 PDT) - Learning to Hack Bluetooth Low Energy with BLE CTF - Ryan Holeman
WS - cont...(15:00-18:59 PDT) - Writing Golang Malware - Benjamin Kurtz

Friday - 19:00 PDT

Return to Index - Locations Legend

AVV - cont...(17:45-19:59 PDT) - (Workshop) Tradecraft Development in Adversary Simulations - Fatih Ozavci
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(17:00-19:59 PDT) - EFF Tech Trivia -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-19:59 PDT) - Lawyers Meet -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -

Friday - 20:00 PDT

Return to Index - Locations Legend

AVV - Panel discussion: Adversary simulation, emulation or purple teaming - How would you define it? - Tomer Bar,Samuel Kimmons,Anant Shrivastava,Vincent Yiu,Martin Ingesen,Joe Vest
CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - Hacker Jeopardy -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - DEF CON Movie Night - Tron -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -
SOC - Vampire the Masquerade (Party) -
SOC - War Story Bunker -

Friday - 21:00 PDT

Return to Index - Locations Legend

CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(20:00-21:59 PDT) - Hacker Jeopardy -
DC - cont...(20:00-21:59 PDT) - DEF CON Movie Night - Tron -
MUS - Music - Thaad - Thaad
MUS - Music - Yesterday & Tomorrow - Yesterday & Tomorrow
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -
SOC - cont...(20:00-21:59 PDT) - War Story Bunker -
SOC - Gothcon 2021 (Virtual) -

Friday - 22:00 PDT

Return to Index - Locations Legend

CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - Whose Slide Is It Anyway -
MUS - Music - FuzzyNop - FuzzyNop
MUS - Music - Terrestrial Access Network - Terrestrial Access Network
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -

Friday - 23:00 PDT

Return to Index - Locations Legend

CON - cont...(00:00-23:59 PDT) - Coindroids -
CON - cont...(10:00-23:55 PDT) - Car Hacking CTF -
CON - cont...(22:00-23:59 PDT) - Whose Slide Is It Anyway -
MUS - Music - n0x08 - n0x08
MUS - Music - Z3NPI - Z3NPI
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -

Saturday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Saturday - 00:00 PDT

Return to Index - Locations Legend

MUS - Music - Scotch & Bubbles - Scotch & Bubbles

Saturday - 01:00 PDT

Return to Index - Locations Legend

MUS - Music - Magik Plan - Magik Plan

Saturday - 08:00 PDT

Return to Index - Locations Legend

HHV - (08:30-08:59 PDT) - Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables - Federico Lucifredi
RFV - The Basics of Breaking BLE - Part 2: Doing More With Less - freqy

Saturday - 09:00 PDT

AIV - Welcome to AI Village - AI Village Organizers

AIV - (09:30-10:59 PDT) - Intro to ML Workshop - Gavin Klondike

APV - AppSec Village Welcome and Introductions

APV - Borrow a mentor

APV - Scaling AppSec through Education - Grant Ongers (rewtd)

ASV - A-ISAC CTF -- Pre-registration Required -

ASV - California Cyber Innovation Challenge CTF -- Pre-registration Required -

ASV - (09:30-10:50 PDT) - VDP in aviation: Experiences and lessons learnt as a researcher - Matt Gaffney

BTV - I know who has access to my cloud, do you? - Igal Flegmann

BTV - Wireshark for Incident Response & Threat Hunting - Michael Wylie

CON - OpenSOC Blue Team CTF -

CON - Trace Labs OSINT Search Party CTF - Briefing -

CON - Darknet-NG -

DC - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -

DC - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf

HHV - (09:30-10:30 PDT) - Use a PortaProg to flash, dump, and test ISP and UPDI chips - Bradán Lane,Sara Cladlow

PHV - APT Hunting with Splunk - John Stoner

PHV - Seeing the Forest Through the Trees – Foundations of Event Log Analysis - Jake Williams

Saturday - 10:00 PDT

Return to Index - Locations Legend

AIV - cont...(09:30-10:59 PDT) - Intro to ML Workshop - Gavin Klondike
APV - I used AppSec skills to hack IoT, and so can you - Alexei Kojenov
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(09:00-16:59 PDT) - California Cyber Innovation Challenge CTF -- Pre-registration Required -
ASV - cont...(09:30-10:50 PDT) - VDP in aviation: Experiences and lessons learnt as a researcher - Matt Gaffney
ASV - Antenny -
ASV - ARINC 429 Lab -
ASV - Deep Space Networking -
ASV - Hack-A-Sat2 Satellite Platform -
ASV - HACMS Live Demo -
ASV - Lego Spike Hub -
ASV - Understanding Space in the Cyber Domain -
ASV - ADSB Demo and Paper Airplanes -
AVV - The Way of The Adversary - Phillip Wylie
BCV - Welcome Note - Nathan,Ron Stoner
BCV - (10:15-11:30 PDT) - Key Note – The Three Amigos: Money Laundering, Cryptocurrencies, and Smart Contracts - Daniel Garrie,David Cass
BHV - How to Not Miss The Point: Reflections on Race, Health, and Equity - Nia Johnson
BHV - CTF: Hospital Under Siege (Pre-registration required)
BICV - (10:30-10:30 PDT) - Black Cyber Exodus: The Mis-Education (Certification) of Black Cyber - Stephen Pullum
BTV - cont...(09:00-10:30 PDT) - Wireshark for Incident Response & Threat Hunting - Michael Wylie
BTV - (10:15-11:15 PDT) - Use DNS to detect your domains are abused for phishing - Karl Lovink a.k.a. Cyb0rg42,Arnold Holzel
CCV - What Is Zero Knowledge - Sarang Noether, Ph.D.
CLV - Extracting all the Azure Passwords - Karl Fosaaen
CLV - (10:45-11:30 PDT) - Windows Server Containers are Broken - Here's How You Can Break Out - Daniel Prizmant
CON - cont...(09:00-16:59 PDT) - Darknet-NG -
CON - cont...(09:00-15:59 PDT) - OpenSOC Blue Team CTF -
CON - DEF CON 29 CTF by OOO -
CON - Red Team Village CTF - Qualifiers Part 2 -
CON - Red Alert ICS CTF -
CON - Trace Labs OSINT Search Party CTF -
CON - CMD+CTRL -
CON - Hack3r Runw@y -
CPV - CPV Through the Looking-Glass: Cryptography Codes and Secret Writing (DC 26)
CPV - Workshop & CTF: Practical Cryptographic Attacks - Daniel Crowley
DC - cont...(09:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf
DC - DEF CON Vendor Area Open
DC - Privacy Without Monopoly: Paternalism Works Well, But Fails Badly - Cory Doctorow
DC - High-Stakes Updates | BIOS RCE OMG WTF BBQ - Jesse Michael,Mickey Shkatov
DC - Crossover Episode: The Real-Life Story of the First Mainframe Container Breakout - Chad Rikansrud (Bigendian Smalls),Ian Coldwater
DC - Community Roundtable - Supply Chain in the COVID Era -
DC - Community Roundtable - We need to talk about Norm – Discussions on International cyber norms in diplomacy -
DDV - Data Duplication Village - Open -
DL - Kubernetes Goat - Madhu Akula
DL - Ruse - Mike Kiser
DL - PMapper - Erik Steringer
DL - Depthcharge - Jon Szymaniak
HHV - cont...(09:30-10:30 PDT) - Use a PortaProg to flash, dump, and test ISP and UPDI chips - Bradán Lane,Sara Cladlow

HHV - (10:30-10:59 PDT) - The Black Box and the Brain Box: When Electronics and Deception Collide - Gigs
HTSV - OSINT Tales: What the Public Knows About Russia's New Mega-Submarine - H I Sutton
ICSV - CybatiWorks Mission Station Workshop - Matthew Luallen
IOTV - Pentesting 101 -
IOTV - I used AppSec skills to hack IoT, and so can you - Alexei Kojenov
IOTV - UART to UBOOT to ROOT -
IOTV - IoT Village Capture the Flag (CTF) -
IOTV - IoT Village Labs -
IOTV - Black Box Challenges -
LBV - Bypass 101
LPV - Intro To Lockpicking - TOOOL
PHV - cont...(09:00-10:59 PDT) - APT Hunting with Splunk - John Stoner
PHV - *nix Processes. Starting, Stopping, and Everything In Between - Nick Roy
RCV - Adversary Infrastructure Tracking with Mihari - Manabu Niseki
RCV - (10:40-11:10 PDT) - The Bug Hunter's Recon Methodology - Tushar Verma
SEV - SECTF4Teens - Chris Silvers,Kris Silvers
VMV - Voting Village Keynote Remarks - Thomas Hicks
VMV - (10:30-10:59 PDT) - Secrets of Social Media PsyOps - BiaSciLab
WS - From Zero to Hero in Web Security Research - Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki
WS - Bug bounty Hunting Workshop - David Patten,Philippe Delteil
WS - Hacking the Metal: An Introduction to Assembly Language Programming - eigentourist
WS - Digital Forensics and Incident Response Against the Dark Arts: The Battle of Malicious Email and Downloaders - Michael Register,Michael Solomon

Saturday - 11:00 PDT

Return to Index - Locations Legend

AIV - The Coming AI Hackers - Bruce Schneier

APV - The Curious case of knowing the unknown - Vandana Verma Sehgal

ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -

ASV - cont...(09:00-16:59 PDT) - California Cyber Innovation Challenge CTF -- Pre-registration Required -

ASV - cont...(10:00-15:59 PDT) - Antenny -

ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -

ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -

ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -

ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -

ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -

ASV - cont...(10:00-12:59 PDT) - Understanding Space in the Cyber Domain -

ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -

ASV - Decoding NOAA Weather Sat Signals -

ASV - (11:30-12:59 PDT) - AIAA CubeSat Hacking Workshop - Virtual Lab #3 -

ASV - (11:30-11:55 PDT) - Defending the Unmanned Aerial Vehicle: Advancements in UAV Intrusion Detection - Jason Whelan

AVV - (Workshop) From zero to hero: creating a reflective loader in C# - Jean Francois Maes

BCV - cont...(10:15-11:30 PDT) - Key Note – The Three Amigos: Money Laundering, Cryptocurrencies, and Smart Contracts - Daniel Garrie,David Cass

BCV - (11:30-11:59 PDT) - Tryptich Talk - Sarang Noether, Ph.D.

BHV - cont...(10:00-17:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)

BHV - Chinese Military Bioweapons and Intimidation Operations: Part III - RedDragon

BTV - cont...(10:15-11:15 PDT) - Use DNS to detect your domains are abused for phishing - Karl Lovink a.k.a. Cyb0rg42,Arnold Holzel

BTV - Tricks for the Triage of Adversarial Software - Dylan Barker,Quinten Bowen

BTV - BTV Presents: Malware Station - Maldoc Workshop - Clay (ttheveii0x)

BTV - (11:30-11:59 PDT) - What Machine Learning Can and Can't Do for Security - Wendy Edwards

CHV - My other car is your car: compromising the Tesla Model X keyless entry system - Lennert Wouters

CLV - cont...(10:45-11:30 PDT) - Windows Server Containers are Broken - Here's How You Can Break Out - Daniel Prizmant

CLV - (11:30-12:15 PDT) - AWS cloud attack vectors and security controls - Kavisha Sheth

CON - cont...(09:00-16:59 PDT) - Darknet-NG -

CON - cont...(09:00-15:59 PDT) - OpenSOC Blue Team CTF -

CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -

CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -

CON - cont...(10:00-11:59 PDT) - Red Team Village CTF - Qualifiers Part 2 -

CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -

CON - cont...(10:00-15:59 PDT) - Trace Labs OSINT Search Party CTF -

CON - cont...(10:00-15:59 PDT) - CMD+CTRL -

CPV - cont...(10:00-11:30 PDT) - CPV Through the Looking-Glass: Cryptography Codes and Secret Writing (DC 26)

CPV - cont...(10:00-17:30 PDT) - Workshop & CTF: Practical Cryptographic Attacks - Daniel Crowley

CPV - (11:30-12:30 PDT) - Breaking Historical Ciphers with Modern Algorithms - Elonka Dunin,Klaus Schmeh

DC - cont...(09:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -

DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf

DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open

DC - Wibbly Wobbly, Timey Wimey – What's Really Inside Apple's U1 Chip - Alexander Heinrich,jiska

DC - UPnProxyPot: fake the funk, become a blackhat proxy, MITM their TLS, and scrape the wire - Chad Seaman

DC - (11:30-12:30 PDT) - Community Roundtable - If only you knew -

DL - cont...(10:00-11:50 PDT) - Kubernetes Goat - Madhu Akula

DL - cont...(10:00-11:50 PDT) - Ruse - Mike Kiser

DL - cont...(10:00-11:50 PDT) - PMapper - Erik Steringer

DL - cont...(10:00-11:50 PDT) - Depthcharge - Jon Szymaniak
HHV - Walkthrough of DC 28 HHV Challenges - rehr
HRV - Amateur Radio Mesh Networking: Enabling Higher Data-rate Communications - Tyler Gardner
HTSV - Cyber-SHIP Lab Talk and Demo - Kevin Jones,Kimberley Tam
ICSV - cont...(10:00-11:59 PDT) - CybatiWorks Mission Station Workshop - Matthew Luallen
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - You're Doing IoT RNG - Allan Cecil - dwangoAC,Dan Petro - AltF4
LBV - Bypassing Retail Security Tags
LPV - Hybrid PhySec tools - best of both worlds or just weird? - d1dymu5
PHV - Linux Binary Analysis w/ Strace - Jared Stroud
RCV - cont...(10:40-11:10 PDT) - The Bug Hunter’s Recon Methodology - Tushar Verma
RCV - (11:20-11:50 PDT) - Can I Make My Own Social Threat Score? - MasterChen
SEV - cont...(10:00-11:59 PDT) - SECTF4Teens - Chris Silvers,Kris Silvers
VMV - How to Weaponize RLAs to Discredit an Election - Carsten Schürmann
VMV - (11:30-11:59 PDT) - High Turnout, Wide Margins - Brianna Lennon,Eric Fey
WS - cont...(10:00-13:59 PDT) - From Zero to Hero in Web Security Research - Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki
WS - cont...(10:00-13:59 PDT) - Bug bounty Hunting Workshop - David Patten,Philippe Delteil
WS - cont...(10:00-13:59 PDT) - Hacking the Metal: An Introduction to Assembly Language Programming - eigentourist
WS - cont...(10:00-13:59 PDT) - Digital Forensics and Incident Response Against the Dark Arts: The Battle of Malicious Email and Downloaders - Michael Register,Michael Solomon

Saturday - 12:00 PDT

Return to Index - Locations Legend

AIV - Never a dill moment: Exploiting machine learning pickle files - Suha Sabi Hussain

AIV - (12:30-12:59 PDT) - Replication as a Security Threat: How to Save Millions By Recreating Someone Else's Model - Stella Biderman

APV - CSP is broken, let's fix it - Amir Shaked

APV - (Workshop) - Integrating DAST tools into developers' test process - Joe Schottman

ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -

ASV - cont...(09:00-16:59 PDT) - California Cyber Innovation Challenge CTF -- Pre-registration Required -

ASV - cont...(10:00-15:59 PDT) - Antenny -

ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -

ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -

ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -

ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -

ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -

ASV - cont...(10:00-12:59 PDT) - Understanding Space in the Cyber Domain -

ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -

ASV - cont...(11:30-12:59 PDT) - AIAA CubeSat Hacking Workshop - Virtual Lab #3 -

ASV - Federal Perspective on Aerospace Cybersecurity - Larry Grossman,Steve Luczynski

ASV - In Space, No One Can Hear You Hack -

ASV - (12:30-13:20 PDT) - Lost In Space: No-one Can Hear Your Breach (Choose Wisely) - Elizabeth Wharton

AVV - cont...(11:00-13:15 PDT) - (Workshop) From zero to hero: creating a reflective loader in C# - Jean Francois Maes

BCV - Ethereum Hacks & How to Stop Them - Michael Lewellen

BHV - cont...(10:00-17:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)

BHV - (12:30-13:30 PDT) - Cloud security for healthcare and life sciences - MIchelle Holko

BICV - (12:30-12:30 PDT) - The OPSEC of Protesting - Ochaun Marshall

BTV - cont...(11:00-12:30 PDT) - Tricks for the Triage of Adversarial Software - Dylan Barker,Quinten Bowen

BTV - cont...(11:00-12:30 PDT) - BTV Presents: Malware Station - Maldoc Workshop - Clay (ttheveii0x)

BTV - (12:15-12:45 PDT) - How do you ALL THE CLOUDS? - henry

CAHV - National Service Panel - Amelie Koran,Elizabeth Schweinsberg,Joe Billingsley,Teri Williams

CAHV - Resume Reviewing

CAHV - Career Coaching

CHV - Not so Passive: Vehicle Identification and Tracking via Passive Keyless Entry - Nick Ashworth

CLV - cont...(11:30-12:15 PDT) - AWS cloud attack vectors and security controls - Kavisha Sheth

CLV - (12:15-12:45 PDT) - Using Barq to perform AWS Post-Exploitation Actions - Mohammed Aldoub

CLV - (12:45-13:30 PDT) - Shift Left Using Cloud: Implementing baseline security into your deployment lifecycle - Avinash Jain

CON - cont...(09:00-16:59 PDT) - Darknet-NG -

CON - cont...(09:00-15:59 PDT) - OpenSOC Blue Team CTF -

CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -

CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -

CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -

CON - cont...(10:00-15:59 PDT) - Trace Labs OSINT Search Party CTF -

CON - cont...(10:00-15:59 PDT) - CMD+CTRL -

CON - Red Team Village CTF - Qualifier Prizes and Announcements -

CPV - cont...(10:00-17:30 PDT) - Workshop & CTF: Practical Cryptographic Attacks - Daniel Crowley

CPV - cont...(11:30-12:30 PDT) - Breaking Historical Ciphers with Modern Algorithms - Elonka Dunin,Klaus Schmeh

CPV - (12:30-13:15 PDT) - CPV Through the Looking-Glass: Cryptanalysis in the Time of Ransomware (DC 25)

DC - cont...(09:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -

DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf

DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open

DC - cont...(11:30-12:30 PDT) - Community Roundtable - If only you knew -

DC - Bring Your Own Print Driver Vulnerability - Jacob Baines

DC - Racketeer Toolkit. Prototyping Controlled Ransomware Operations - Dimitry "Op_Nomad" Snezhkov
DC - Time Turner - Hacking RF Attendance Systems (To Be in Two Places at Once) - Vivek Nair
DC - (12:30-12:50 PDT) - Hack the hackers: Leaking data over SSL/TLS - Ionut Cernica
DC - (12:30-12:50 PDT) - A new class of DNS vulnerabilities affecting many DNS-as-Service platforms - Ami Luttwak,Shir Tamari
DL - Tracee - Yaniv Agman
DL - USBSamurai - Luca Bongiorni
DL - Git Wild Hunt - Rod Soto,José Hernandez
HHV - A Lazy r2 Solve of @mediumrehr Challenge 6 - Ben Gardiner
HRV - Ham Radio Exams -
HTSV - Hack the Sea Cabana Party -
HTSV - Cyber in the Under Sea - David Strachan
ICSV - Fireside Chat - August Cole - August Cole
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - Strategic Trust and Deception in the Internet of Things - Juneau Jones
IOTV - (12:45-13:30 PDT) - MIPS-X - The next IoT Frontier - Patrick Ross,Zoltán Balázs
LBV - Tools 101 & Q&A
LPV - Intro To Lockpicking - TOOOL
PHV - Security Investigations with Splunk - Robert Wagner
PHV - RCE via Meow Variant along with an Example 0day - Özkan Mustafa AKKUŞ
RCV - Let the bugs come to me - how to build cloud-based recon automation at scale - Ryan Elkins
RGV - Twitter Q&A regarding Top 10 BOGUS Biometrics! - Vic Harkness
SEV - (12:30-13:30 PDT) - Using SE to create insider threats and win all the things - Lisa Forte
SOC - Friends of Bill W. -
VMV - Keeping Your Information Security Policy Up to Date - Sang-Oun Lee
VMV - (12:30-12:59 PDT) - Social Media Security = Election Security - Sebastian Bay
WS - cont...(10:00-13:59 PDT) - From Zero to Hero in Web Security Research - Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki
WS - cont...(10:00-13:59 PDT) - Bug bounty Hunting Workshop - David Patten,Philippe Delteil
WS - cont...(10:00-13:59 PDT) - Hacking the Metal: An Introduction to Assembly Language Programming - eigentourist
WS - cont...(10:00-13:59 PDT) - Digital Forensics and Incident Response Against the Dark Arts: The Battle of Malicious Email and Downloaders - Michael Register,Michael Solomon

Saturday - 13:00 PDT

Return to Index - Locations Legend

AIV - Who's Afraid of Thomas Bayes? - Erick Galinkin

AIV - (13:30-13:59 PDT) - Risks of ML Systems in Health Care: The Real Story - Barton Rhodes

APV - cont...(12:00-14:30 PDT) - (Workshop) - Integrating DAST tools into developers' test process - Joe Schottman

APV - When nothing goes right, push left. Designing logs for future breach investigations - Vee

ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -

ASV - cont...(09:00-16:59 PDT) - California Cyber Innovation Challenge CTF -- Pre-registration Required -

ASV - cont...(10:00-15:59 PDT) - Antenny -

ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -

ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -

ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -

ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -

ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -

ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -

ASV - cont...(12:00-15:59 PDT) - In Space, No One Can Hear You Hack -

ASV - cont...(12:30-13:20 PDT) - Lost In Space: No-one Can Hear Your Breach (Choose Wisely) - Elizabeth Wharton

AVV - cont...(11:00-13:15 PDT) - (Workshop) From zero to hero: creating a reflective loader in C# - Jean Francois Maes

AVV - (13:15-13:59 PDT) - (Tool Demo) Red Team Credentials Reconnaissance (OLD with a TWIST) - Shantanu Khandelwal

BCV - Certified Ethereum Professional (CEP) Overview - Abstrct

BCV - (13:30-13:59 PDT) - Sla(sh*t)ing happens when you stake - Nadir Akhtar,Y L

BHV - cont...(10:00-17:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)

BHV - cont...(12:30-13:30 PDT) - Cloud security for healthcare and life sciences - MIchelle Holko

BHV - (13:30-13:59 PDT) - Securing the Internet of Biological Things - Thom Dixon

BTV - (13:45-14:15 PDT) - Leveraging NGFWs for Threat Hunting - Drimacus

CAHV - cont...(12:00-15:59 PDT) - Resume Reviewing

CAHV - cont...(12:00-15:59 PDT) - Career Coaching

CAHV - Selling Yourself as a Security Professional - Preston Pierce

CCV - Monero Scaling Opportunities and Challenges - Francisco Cabañas

CHV - Fuzzing CAN / CAN FD ECU's and Network - Samir Bhagwat

CLV - cont...(12:45-13:30 PDT) - Shift Left Using Cloud: Implementing baseline security into your deployment lifecycle - Avinash Jain

CLV - (13:30-13:50 PDT) - CSPM2CloudTrail - Extending CSPM Tools with (Near) Real-Time Detection Signatures (Lightning Talk) - Rodrigo "Sp0oKeR" Montoro

CLV - (13:50-14:35 PDT) - Azure Active Directory Hacking Wars - Batuhan Sancak

CON - cont...(09:00-16:59 PDT) - Darknet-NG -

CON - cont...(09:00-15:59 PDT) - OpenSOC Blue Team CTF -

CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -

CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -

CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -

CON - cont...(10:00-15:59 PDT) - Trace Labs OSINT Search Party CTF -

CON - cont...(10:00-15:59 PDT) - CMD+CTRL -

CON - Red Team Village CTF - Finals Part 1 -

CPV - cont...(10:00-17:30 PDT) - Workshop & CTF: Practical Cryptographic Attacks - Daniel Crowley

CPV - cont...(12:30-13:15 PDT) - CPV Through the Looking-Glass: Cryptanalysis in the Time of Ransomware (DC 25)

DC - cont...(09:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -

DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf

DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open

DC - TEMPEST radio station - Paz Hameiri

DC - PINATA: PIN Automatic Try Attack - Salvador Mendoza

DC - Defeating Physical Intrusion Detection Alarm Wires - Bill Graydon

DC - Community Roundtable - RANSOMWARE: Combatting Ransomware on a Global Stage / The realities of responding to ransomware -

DL - cont...(12:00-13:50 PDT) - Tracee - Yaniv Agman

DL - cont...(12:00-13:50 PDT) - USBSamurai - Luca Bongiorni

DL - cont...(12:00-13:50 PDT) - Git Wild Hunt - Rod Soto,José Hernandez

HHV - Meetup: Some HHV challenges - rehr

HRV - cont...(12:00-17:59 PDT) - Ham Radio Exams -

HRV - (13:30-14:30 PDT) - Amateur Radio Digital Modes Primer - Jon Marler

HTSV - cont...(12:00-14:59 PDT) - Hack the Sea Cabana Party -

HTSV - Sea Pods - Grant Romundt

ICSV - Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure - Lauren Zabierek

ICSV - (13:30-13:59 PDT) - Fortifying ICS - Hardening and Testing - Dieter Sarrazyn

IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -

IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -

IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -

IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -

IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -

IOTV - cont...(12:45-13:30 PDT) - MIPS-X - The next IoT Frontier - Patrick Ross,Zoltán Balázs

IOTV - (13:45-14:30 PDT) - Mind the Gap - Managing Insecurity in Enterprise IoT - Cheryl Biswas

LBV - Electronic Warfare & Q&A

LPV - How I defeated the Western Electric 30c - N thing

PHV - cont...(12:00-13:59 PDT) - Security Investigations with Splunk - Robert Wagner

SEV - cont...(12:30-13:30 PDT) - Using SE to create insider threats and win all the things - Lisa Forte

SEV - (13:30-14:30 PDT) - The Innocent Lives Foundation: A Beacon of Light in a Dark World - John McCombs

SOC - A&E Pool Party! -

VMV - New Hampshire SB43 Forensic Audit - Harri Hursti

VMV - (13:30-13:59 PDT) - Why Hacking Voters Is Easier Than Hacking Ballots - Maurice Turner

WS - cont...(10:00-13:59 PDT) - From Zero to Hero in Web Security Research - Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki

WS - cont...(10:00-13:59 PDT) - Bug bounty Hunting Workshop - David Patten,Philippe Delteil

WS - cont...(10:00-13:59 PDT) - Hacking the Metal: An Introduction to Assembly Language Programming - eigentourist

WS - cont...(10:00-13:59 PDT) - Digital Forensics and Incident Response Against the Dark Arts: The Battle of Malicious Email and Downloaders - Michael Register,Michael Solomon

Saturday - 14:00 PDT

Return to Index - Locations Legend

AIV - The Real History of Adversarial Machine Learning - Eugene Neelou
APV - cont...(12:00-14:30 PDT) - (Workshop) - Integrating DAST tools into developers' test process - Joe Schottman
APV - How I broke into Mexico City's justice system application and database - Alfonso Ruiz Cruz
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(09:00-16:59 PDT) - California Cyber Innovation Challenge CTF -- Pre-registration Required -
ASV - cont...(10:00-15:59 PDT) - Antenny -
ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -
ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -
ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -
ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -
ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -
ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -
ASV - cont...(12:00-15:59 PDT) - In Space, No One Can Hear You Hack -
ASV - AIAA CubeSat Hacking Workshop - Virtual Lab #4 -
ASV - (14:30-14:55 PDT) - True Story: Hackers in the Aerospace Sector - Declyn S.,Ginny Spicer,Olivia Stella,Steve Luczynski,Thomas Bristow
AVV - Operation Bypass: Catch My Payload If You Can - Matthew Eidelberg
BCV - EIP-1559 Panel
BHV - cont...(10:00-17:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)
BHV - The Real Story on Patching Medical Devices - Michael Murray
BICV - (14:30-14:30 PDT) - 40 cores and a CPU - Nico "Socks" Smith
BTV - cont...(13:45-14:15 PDT) - Leveraging NGFWs for Threat Hunting - Drimacus
BTV - BTV Presents: Forensics Station - Workshop 1 - Omenscan
BTV - MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part 2 - Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges
BTV - (14:30-15:30 PDT) - Modern Authentication for the Security Admin - Bailey Bercik,Mark Morowczynski
CAHV - cont...(12:00-15:59 PDT) - Resume Reviewing
CAHV - cont...(12:00-15:59 PDT) - Career Coaching
CAHV - Career Hacking: Tips and Tricks to Making the Most of your Career - Andy Piazza
CHV - Build Automotive Gateways with Ease - Don Hatfield
CLV - cont...(13:50-14:35 PDT) - Azure Active Directory Hacking Wars - Batuhan Sancak
CLV - (14:35-16:59 PDT) - Onions In the Cloud Make the CISO Proud (Workshop) - Wes Lambert
CON - cont...(09:00-16:59 PDT) - Darknet-NG -
CON - cont...(09:00-15:59 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-15:59 PDT) - Trace Labs OSINT Search Party CTF -
CON - cont...(10:00-15:59 PDT) - CMD+CTRL -
CON - cont...(13:00-16:59 PDT) - Red Team Village CTF - Finals Part 1 -
CPV - cont...(10:00-17:30 PDT) - Workshop & CTF: Practical Cryptographic Attacks - Daniel Crowley
CPV - Staying Fresh While the Feds Watch: Changes in Government Surveillance and Why it Matters - Anthony Hendricks
DC - cont...(09:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - cont...(13:00-14:59 PDT) - Community Roundtable - RANSOMWARE: Combatting Ransomware on a Global Stage / The realities of responding to ransomware -
DC - Sneak into buildings with KNXnet/IP - Claire Vacherot
DC - SPARROW: A Novel Covert Communication Scheme Exploiting Broadcast Signals in LTE, 5G & Beyond - Chuck McAuley,Reza Soosahabi
DC - Over-the-air remote code execution on the DEF CON 27 badge via Near Field Magnetic Inductance or World’s first

NFMI exploitation, sorta or OTARCEDC27NFMIOMGWTFBBQ - Seth Kintigh

DL - ParseAndC - Parbati Kumar Manna

DL - WiFi Kraken Lite - Henry Hill

DL - WiFi Kraken Lite - Henry Hill

DL - Shutter - Dimitry "Op_Nomad" Snezhkov

HHV - Meetup: Sourcing Parts & The Global Parts Shortage - bombnav

HRV - cont...(12:00-17:59 PDT) - Ham Radio Exams -

HRV - cont...(13:30-14:30 PDT) - Amateur Radio Digital Modes Primer - Jon Marler

HTSV - cont...(12:00-14:59 PDT) - Hack the Sea Cabana Party -

HTSV - Cyber Operations and Operational Wargames on Port Infrastructure - Tom Mouatt,Ed McGrady,John Curry

ICSV - Crippling the Grid: Examination of Dependencies and Cyber Vulnerabilities - Joe Slowik

ICSV - (14:30-14:59 PDT) - Leveraging SBOMs to Enhance ICS Security - Thomas Pace

IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -

IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -

IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -

IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -

IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -

IOTV - cont...(13:45-14:30 PDT) - Mind the Gap - Managing Insecurity in Enterprise IoT - Cheryl Biswas

IOTV - (14:45-15:30 PDT) - Reverse Supply Chain Attack - A Dangerous Pathway To Medical Facilities' Networks - Barak Hadad,Gal Kaufman

LBV - cont...(13:00-14:30 PDT) - Electronic Warfare & Q&A

LBV - (14:30-15:59 PDT) - Alarm Bypass & Q&A

LPV - (14:15-14:45 PDT) - Intro To Lockpicking - TOOOL

RCV - How vigilant researchers can uncover APT attacks for fun and non profit - Ladislav Baco

RCV - (14:40-15:10 PDT) - .GOV Doppelgänger: Your Häx Dollars at Work - Anthony Kava

SEV - cont...(13:30-14:30 PDT) - The Innocent Lives Foundation: A Beacon of Light in a Dark World - John McCombs

SEV - (14:30-15:30 PDT) - Make Them Want To Tell You: The Science of Elicitation - Christopher Hadnagy

SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Saturday - 15:00 PDT

Return to Index - Locations Legend

AIV - RTV/AIV Red Teaming AI Roundtable - Rich Harang,Anita Nikolich
APV - A Deep Dive Into Supply Chain Vulnerabilities: And How SecDevOps Can Save the Day - Adam Schaal
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(09:00-16:59 PDT) - California Cyber Innovation Challenge CTF -- Pre-registration Required -
ASV - cont...(10:00-15:59 PDT) - Antenny -
ASV - cont...(10:00-15:59 PDT) - ARINC 429 Lab -
ASV - cont...(10:00-15:59 PDT) - Deep Space Networking -
ASV - cont...(10:00-15:59 PDT) - Hack-A-Sat2 Satellite Platform -
ASV - cont...(10:00-15:59 PDT) - HACMS Live Demo -
ASV - cont...(10:00-15:59 PDT) - Lego Spike Hub -
ASV - cont...(10:00-15:59 PDT) - ADSB Demo and Paper Airplanes -
ASV - cont...(12:00-15:59 PDT) - In Space, No One Can Hear You Hack -
ASV - cont...(14:00-15:59 PDT) - AIAA CubeSat Hacking Workshop - Virtual Lab #4 -
ASV - Drone Security Research Series – Ep6 Hacking with drones - Matt Gaffney
AVV - (Tool Demo) PurpleSharp: Automated Adversary Simulation - Mauricio Velazco
AVV - (15:45-16:30 PDT) - Phish Like An APT - Sanne Maasakkers
BCV - Evils in the DeFi world - Minzhi He,Peiyu Wang
BHV - cont...(10:00-17:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)
BHV - OWASP & CSA IoT: Impacting Medical Security - Aaron Guzman
BTV - cont...(14:00-15:30 PDT) - BTV Presents: Forensics Station - Workshop 1 - Omenscan
BTV - cont...(14:00-17:59 PDT) - MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part 2 - Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges
BTV - cont...(14:30-15:30 PDT) - Modern Authentication for the Security Admin - Bailey Bercik,Mark Morowczynski
BTV - (15:45-16:45 PDT) - Uncomfortable Networking - Charles Rumford
CAHV - cont...(12:00-15:59 PDT) - Resume Reviewing
CAHV - cont...(12:00-15:59 PDT) - Career Coaching
CCV - Triptych - Sarang Noether, Ph.D.
CHV - Safety Third: Defeating Chevy StabiliTrak for Track Time Fun - Eric Gershman
CLV - cont...(14:35-16:59 PDT) - Onions In the Cloud Make the CISO Proud (Workshop) - Wes Lambert
CON - cont...(09:00-16:59 PDT) - Darknet-NG -
CON - cont...(09:00-15:59 PDT) - OpenSOC Blue Team CTF -
CON - cont...(10:00-15:59 PDT) - Hack3r Runw@y -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(10:00-15:59 PDT) - Trace Labs OSINT Search Party CTF -
CON - cont...(10:00-15:59 PDT) - CMD+CTRL -
CON - cont...(13:00-16:59 PDT) - Red Team Village CTF - Finals Part 1 -
CPV - cont...(10:00-17:30 PDT) - Workshop & CTF: Practical Cryptographic Attacks - Daniel Crowley
CPV - CPV Through the Looking-Glass: Hacking on Multi-Party Computation (DC 25)
CPV - (15:30-16:30 PDT) - Gold Bug Q&A -
DC - cont...(09:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - Hacking G Suite: The Power of Dark Apps Script Magic - Matthew Bryant
DC - Central bank digital currency, threats and vulnerabilities - Ian Vitek
DC - Breaking Secure Bootloaders - Christopher Wade
DL - cont...(14:00-15:50 PDT) - ParseAndC - Parbati Kumar Manna
DL - cont...(14:00-15:50 PDT) - WiFi Kraken Lite - Henry Hill
DL - cont...(14:00-15:50 PDT) - WiFi Kraken Lite - Henry Hill
DL - cont...(14:00-15:50 PDT) - Shutter - Dimitry "Op_Nomad" Snezhkov
HHV - Meetup: OSS ASIC - Josh Marks

HRV - cont...(12:00-17:59 PDT) - Ham Radio Exams -
HRV - How to Contact the ISS with a $30 Radio - Gregg Horton
HTSV - US Coast Guard 2021 Cyber Strategic Outlook - Michael Chien
ICSV - Smart Meters: I'm Hacking Infrastructure and So Should You - Hash Salehi
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(14:45-15:30 PDT) - Reverse Supply Chain Attack - A Dangerous Pathway To Medical Facilities' Networks - Barak Hadad,Gal Kaufman
IOTV - (15:45-16:15 PDT) - Ethics at the Edge: IoT as the Embodiment of AI for Rampant Intelligence Actuation - Ria Cheruvu
LBV - cont...(14:30-15:59 PDT) - Alarm Bypass & Q&A
LPV - The Coat Hanger Talk: A Noob's Look Into the Thieves World - De
RCV - cont...(14:40-15:10 PDT) - .GOV Doppelgänger: Your Häx Dollars at Work - Anthony Kava
RCV - (15:20-16:05 PDT) - OSINT for Sex Workers - Kala Kinyon
SEV - cont...(14:30-15:30 PDT) - Make Them Want To Tell You: The Science of Elicitation - Christopher Hadnagy
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
WS - Network Analysis with Wireshark - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - Analysis 101 and 102 for the Incident Responder - Kristy Westphal
WS - Evading Detection a Beginner's Guide to Obfuscation - Anthony "Cx01N" Rose,Jake "Hubbl3" Krasnov,Vincent "Vinnybod" Rose
WS - Advanced Wireless Attacks Against Enterprise Networks - Solstice

Saturday - 16:00 PDT

Return to Index - Locations Legend

AIV - Where We're Going We Don't Need Labels: Anomaly Detection for 2FA - Rebecca Lynch,Stefano Meschiari
AIV - (16:30-16:59 PDT) - AI Discord Happy Hour - Open Discussion on AIV Discord about the State of AI Security
APV - DevSecOps: Merging Security and Software Engineering - Magno Logan DELETE ME
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
ASV - cont...(09:00-16:59 PDT) - California Cyber Innovation Challenge CTF -- Pre-registration Required -
ASV - Fuzzing NASA Core Flight System Software - Ronald Broberg
AVV - cont...(15:45-16:30 PDT) - Phish Like An APT - Sanne Maasakkers
AVV - (16:30-17:15 PDT) - (Tool Demo) Tenacity: An Adversary Emulation Tool for Persistence - Atul Nair,Harshal Tupsamudre
BCV - The Wild West of DeFi Exploits - Anna Szeto
BHV - cont...(10:00-17:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)
BHV - cont...(15:00-16:45 PDT) - OWASP & CSA IoT: Impacting Medical Security - Aaron Guzman
BHV - (16:45-16:59 PDT) - A Cohort of Pirate Ships - Alex Pearlman
BICV - (16:30-16:30 PDT) - How Bias and Discrimination in Cybersecurity will have us locked up or dead - Tennisha Martin
BTV - cont...(14:00-17:59 PDT) - MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part 2 - Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges
BTV - cont...(15:45-16:45 PDT) - Uncomfortable Networking - Charles Rumford
BTV - (16:30-17:59 PDT) - Ransomware ATT&CK and Defense with the Elastic Stack - Ben Hughes,Daniel Chen,Fred Mastrippolito
CCV - (16:30-16:59 PDT) - Cryptocurrency Trivia! - Justin Ehrenhofer
CLV - cont...(14:35-16:59 PDT) - Onions In the Cloud Make the CISO Proud (Workshop) - Wes Lambert
CON - cont...(09:00-16:59 PDT) - Darknet-NG -
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - cont...(13:00-16:59 PDT) - Red Team Village CTF - Finals Part 1 -
CPV - cont...(10:00-17:30 PDT) - Workshop & CTF: Practical Cryptographic Attacks - Daniel Crowley
CPV - cont...(15:30-16:30 PDT) - Gold Bug Q&A -
CPV - (16:30-17:30 PDT) - The threat hiding in daylight: Police Monitoring legislation and individual privacy in chat - Vic Huang,Joy Ho
DC - cont...(09:00-16:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - New Phishing Attacks Exploiting OAuth Authentication Flows - Jenko Hwong
DC - PunkSPIDER and IOStation: Making a Mess All Over the Internet - _hyp3ri0n aka Alejandro Caceres,Jason Hopper
DC - Adventures in MitM-land: Using Machine-in-the-Middle to Attack Active Directory Authentication Schemes - Eyal Karni,Sagi Sheinfeld,Yaron Zinar
DC - Community Roundtable - Thinking About Election Security -
DC - Community Roundtable - Implementing Cyber Solarium Commission Policy -
HHV - Meetup: Certification Processes (UL, FCC, etc.) - ShortTie
HRV - cont...(12:00-17:59 PDT) - Ham Radio Exams -
HRV - Getting started with low power & long distance communications - QRP - Eric Escobar
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - cont...(15:45-16:15 PDT) - Ethics at the Edge: IoT as the Embodiment of AI for Rampant Intelligence Actuation - Ria Cheruvu
IOTV - (16:30-16:59 PDT) - IoT devices as government witnesses: Can IoT devices ever be secure if law enforcement has unlimited access to their data? - Anthony Hendricks,Jordan Sessler
LBV - (16:30-16:59 PDT) - Bypass 101

LPV - (16:15-16:45 PDT) - Intro To Lockpicking - TOOOL
RCV - cont...(15:20-16:05 PDT) - OSINT for Sex Workers - Kala Kinyon
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - QueerCon Party -
WS - cont...(15:00-18:59 PDT) - Network Analysis with Wireshark - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(15:00-18:59 PDT) - Analysis 101 and 102 for the Incident Responder - Kristy Westphal
WS - cont...(15:00-18:59 PDT) - Evading Detection a Beginner's Guide to Obfuscation - Anthony "Cx01N" Rose,Jake "Hubbl3" Krasnov,Vincent "Vinnybod" Rose
WS - cont...(15:00-18:59 PDT) - Advanced Wireless Attacks Against Enterprise Networks - Solstice

Saturday - 17:00 PDT

Return to Index - Locations Legend

APV - Can’t Stop the Code: Embrace the Code - Alton Crossley
APV - (17:45-17:50 PDT) - AppSec Quiz Time! - Eden Stroet
ASV - cont...(09:00-17:59 PDT) - A-ISAC CTF -- Pre-registration Required -
AVV - cont...(16:30-17:15 PDT) - (Tool Demo) Tenacity: An Adversary Emulation Tool for Persistence - Atul Nair,Harshal Tupsamudre
AVV - (17:15-18:15 PDT) - C2Centipede: APT level C2 communications for common reverse HTTP shell tools - Jose Garduno
BHV - cont...(10:00-17:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)
BHV - The Little Things - Mixæl Laufer
BHV - (17:30-17:59 PDT) - Playing with FHIR: hacking and securing healthcare APIs - Alissa Knight,Mitch Parker
BTV - cont...(14:00-17:59 PDT) - MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part 2 - Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges
BTV - cont...(16:30-17:59 PDT) - Ransomware ATT&CK and Defense with the Elastic Stack - Ben Hughes,Daniel Chen,Fred Mastrippolito
BTV - Structured Analytical Techniques for Improving Information Security Analyses - Rabbit
CCV - Monero After Party - Monero Sound
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-17:59 PDT) - Red Alert ICS CTF -
CON - Trace Labs OSINT Search Party CTF - Award Ceremony -
CPV - cont...(10:00-17:30 PDT) - Workshop & CTF: Practical Cryptographic Attacks - Daniel Crowley
CPV - cont...(16:30-17:30 PDT) - The threat hiding in daylight: Police Monitoring legislation and individual privacy in chat - Vic Huang,Joy Ho
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - You're Doing IoT RNG - Allan Cecil - dwangoAC,Dan Petro - AltF4
DC - Hacking the Apple AirTags - Thomas Roth
DC - Don't Dare to Exploit - An Attack Surface Tour of SharePoint Server - Steven Seeley,Yuhao Weng,Zhiniang Peng
HRV - cont...(12:00-17:59 PDT) - Ham Radio Exams -
HRV - Remote Ham Radio Exams -
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
IOTV - (17:15-17:59 PDT) - The Journey of Establishing IoT Trustworthiness and IoT Security Foundation - Amit Elazari,Anahit Tarkhanyan,Ria Cheruvu
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(16:00-17:59 PDT) - QueerCon Party -
SOC - DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup -
SOC - Friends of Bill W. -
WS - cont...(15:00-18:59 PDT) - Network Analysis with Wireshark - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(15:00-18:59 PDT) - Analysis 101 and 102 for the Incident Responder - Kristy Westphal
WS - cont...(15:00-18:59 PDT) - Evading Detection a Beginner's Guide to Obfuscation - Anthony "Cx01N" Rose,Jake "Hubbl3" Krasnov,Vincent "Vinnybod" Rose
WS - cont...(15:00-18:59 PDT) - Advanced Wireless Attacks Against Enterprise Networks - Solstice

Saturday - 18:00 PDT

Return to Index - Locations Legend

AVV - cont...(17:15-18:15 PDT) - C2Centipede: APT level C2 communications for common reverse HTTP shell tools - Jose Garduno
AVV - (18:15-18:45 PDT) - Lightning talk: Autonomous lateral movement - Stephan Wampouille
AVV - (18:45-19:45 PDT) - Game Theory: Understanding and Strategy and Deception - Juneau Jones
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - HACKERS INTO THE UN? Engaging in the cyber discussions on war & peace - DEF CON Policy Panel
DC - Offensive Golang Bonanza: Writing Golang Malware - Benjamin Kurtz
DC - Vulnerability Exchange: One Domain Account For More Than Exchange Server RCE - Tianze Ding
HRV - cont...(17:00-18:59 PDT) - Remote Ham Radio Exams -
IOTV - cont...(10:00-18:30 PDT) - Pentesting 101 -
IOTV - cont...(10:00-18:30 PDT) - UART to UBOOT to ROOT -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Capture the Flag (CTF) -
IOTV - cont...(10:00-18:30 PDT) - IoT Village Labs -
IOTV - cont...(10:00-18:30 PDT) - Black Box Challenges -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(17:00-18:59 PDT) - DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup -
SOC - QueerCon Virtual Chat Mixer
SOC - Hacker Karaoke (Virtual) -
WS - cont...(15:00-18:59 PDT) - Network Analysis with Wireshark - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(15:00-18:59 PDT) - Analysis 101 and 102 for the Incident Responder - Kristy Westphal
WS - cont...(15:00-18:59 PDT) - Evading Detection a Beginner's Guide to Obfuscation - Anthony "Cx01N" Rose,Jake "Hubbl3" Krasnov,Vincent "Vinnybod" Rose
WS - cont...(15:00-18:59 PDT) - Advanced Wireless Attacks Against Enterprise Networks - Solstice

Saturday - 19:00 PDT

Return to Index - Locations Legend

AVV - cont...(18:45-19:45 PDT) - Game Theory: Understanding and Strategy and Deception - Juneau Jones
AVV - (19:45-20:30 PDT) - (Tool Demo) New generation of PEAS - Carlos Polop
CON - cont...(10:00-19:59 PDT) - DEF CON 29 CTF by OOO -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf
DC - cont...(10:00-19:59 PDT) - DEF CON Vendor Area Open
DC - (Replay) UFOs: Misinformation, Disinformation, and the Basic Truth - Richard Thieme AKA neuralcowboy
DC - (Replay) Racketeer Toolkit. Prototyping Controlled Ransomware Operations - Dimitry "Op_Nomad" Snezhkov
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -

Saturday - 20:00 PDT

Return to Index - Locations Legend

AVV - cont...(19:45-20:30 PDT) - (Tool Demo) New generation of PEAS - Carlos Polop
AVV - (20:30-21:30 PDT) - Panel discussion: Is Adversary Emulation Too ___ For You? - Jamie Williams,Cat Self,Tim Schulz,Michael Long,Frank Duff,Jose Barajas
CON - Hacker Jeopardy -
CON - Drunk Hacker History -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf
DC - DEF CON Movie Night - Upgrade -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -
SOC - Hacker Flairgrounds -
SOC - Gothcon 2021 -

Saturday - 21:00 PDT

Return to Index - Locations Legend

AVV - cont...(20:30-21:30 PDT) - Panel discussion: Is Adversary Emulation Too ___ For You? - Jamie Williams,Cat Self,Tim Schulz,Michael Long,Frank Duff,Jose Barajas
CON - cont...(20:00-21:59 PDT) - Hacker Jeopardy -
CON - cont...(20:00-21:59 PDT) - Drunk Hacker History -
DC - cont...(20:00-21:59 PDT) - DEF CON Movie Night - Upgrade -
MUS - Music - Ohm-i - Ohm-i
MUS - Music - mattrix - mattrix
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -
SOC - cont...(20:00-22:59 PDT) - Hacker Flairgrounds -
SOC - Vetcon Meetup (Hybrid) -

Saturday - 22:00 PDT

Return to Index - Locations Legend

ASV - (22:30-23:30 PDT) - The Hangar – Cocktail Making Event -
MUS - Music - Krisz Klink - Krisz Klink
MUS - Music - Icetre Normal - Icetre Normal
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -
SOC - cont...(20:00-22:59 PDT) - Hacker Flairgrounds -

Saturday - 23:00 PDT

Return to Index - Locations Legend

ASV - cont...(22:30-23:30 PDT) - The Hangar – Cocktail Making Event -
MUS - Music - Miss Jackalope - Miss Jackalope
MUS - Music - Nina Lowe - Nina Lowe
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -
SOC - cont...(18:00-23:59 PDT) - Hacker Karaoke (Virtual) -

Sunday

This Schedule is tentative and may be changed at any time. Check at an Info Booth for the latest.

Sunday - 00:00 PDT

Return to Index - Locations Legend

MUS - Music - Zebbler Encanti Experience - Zebbler Encanti Experience

Sunday - 01:00 PDT

Return to Index - Locations Legend

MUS - Music - CTRL/rsm - CTRL/rsm

Sunday - 06:00 PDT

Return to Index - Locations Legend

IOTV - IoT Village Labs -

Sunday - 07:00 PDT

Return to Index - Locations Legend

BHV - Table Top Exercise - Biologia et Machina (Pre-registration Required)
IOTV - cont...(06:00-10:59 PDT) - IoT Village Labs -

Sunday - 08:00 PDT

Return to Index - Locations Legend

IOTV - cont...(06:00-10:59 PDT) - IoT Village Labs -

Sunday - 09:00 PDT

Return to Index - Locations Legend

AIV - The State of AI Ethics - Abishek Gupta
AIV - (09:30-10:59 PDT) - Intro to ML Workshop - Gavin Klondike
APV - AppSec Village Welcome and Introductions
APV - "The Poisoned Diary": Supply Chain Attacks on Install scripts - Yakov Shafranovich
APV - Borrow a mentor
CON - Darknet-NG -
DC - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
HHV - Walkthrough of DC 28 HHV Challenges - rehr
IOTV - cont...(06:00-10:59 PDT) - IoT Village Labs -
PHV - Intrusion Analysis and Threat Hunting with Suricata - Peter Manev,Josh Stroschein

Sunday - 10:00 PDT

Return to Index - Locations Legend

AIV - cont...(09:30-10:59 PDT) - Intro to ML Workshop - Gavin Klondike
APV - Encryption for Developers - James McKee (punkcoder)
AVV - Panel discussion: Resilient cyber space: The role of hacker and security communities - Abhijith B R,Jay Turla,Manu Zacharia,Aseem Jakhar,Omar Santos,Dave Lewis,Dhillon ‘L33tdawg’ Kannabhiran
BCV - Welcome Note - Nathan,Ron Stoner
BCV - (10:15-11:30 PDT) - Surviving DeFi: How to Prevent Economic Attacks - Jan Gorzny
BHV - Cyber Defense Matrix in Healthcare - Sounil Yu
BHV - CTF: Hospital Under Siege (Pre-registration required)
BHV - (10:30-10:59 PDT) - Internet-of-Ingestible-Things Security by Design - Mariam Elgabry
BTV - BTV Presents: Threat Report Roulette - Blind Hacker JoeB,Will Thomas,Ricky Banda,Karan Aditya Ghoshal,Danny D. Henderson Jr,Christopher Russell,Jorge Orchilles,Ch33r10
CLV - Identifying toxic combinations of permissions in your cloud infrastructure - Michael Raggo
CLV - (10:45-11:15 PDT) - I know who has access to my cloud, do you? - Igal Flegmann
CON - cont...(09:00-23:59 PDT) - Darknet-NG -
CON - DEF CON 29 CTF by OOO -
CON - Red Team Village CTF - Finals Part 2 -
CPV - CPV Through the Looking-Glass: Cicada (DC 26)
CPV - Workshop: Practically Protecting Phone Privacy (Pre-registration required) - Mauricio Tavares,Matt Nash
CPV - (10:35-13:59 PDT) - CPV Through the Looking-Glass: CPV Day 3 (DC 28)
DC - cont...(09:00-13:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - DEF CON Vendor Area Open
DC - A Discussion with Agent X - Agent X
DC - Hi! I'm DOMAIN\Steve, please let me access VLAN2 - Justin Perdok
DC - Taking Apart and Taking Over ICS & SCADA Ecosystems: A Case Study of Mitsubishi Electric - Mars Cheng,Selmon Yang
DDV - Data Duplication Village - Last Chance Pickup Only -
DL - reNgine - Yogesh Ojha
DL - Frack - William Vermaak
HHV - A Lazy r2 Solve of @mediumrehr Challenge 6 - Ben Gardiner
HTSV - Less Jaw Work, More Paw Work: Why We Need to Start “Doing” Cyber - Cliff Neve
ICSV - Bottom-Up and Top-Down: Exploiting Vulnerabilities In the OT Cloud Era - Sharon Brizinov,Uri Katz
ICSV - (10:30-10:59 PDT) - Detecting Attackers Using Your Own Sensors with State Estimation - Stefan Stephenson-Moe
IOTV - cont...(06:00-10:59 PDT) - IoT Village Labs -
IOTV - IoT Village Capture the Flag (CTF) -
LPV - Intro To Lockpicking - TOOOL
PHV - cont...(09:00-10:59 PDT) - Intrusion Analysis and Threat Hunting with Suricata - Peter Manev,Josh Stroschein
WS - Windows Internals - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - From Zero to Hero in Web Security Research - Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki
WS - Modern Malware Analysis for Threat Hunters - Aaron Rosenmund,Ryan Chapman
WS - Hacking the Metal: An Introduction to Assembly Language Programming - eigentourist

Sunday - 11:00 PDT

Return to Index - Locations Legend

AIV - Potential Pitfalls Protecting Patient Privacy - Brian Martin
AIV - (11:30-11:59 PDT) - Robustness of client-side scanning for illegal content detection on E2EE platforms - Shubham Jain
APV - AppSec 101: A Journey from Engineer to Hacker - Arjun Gopalakrishna
AVV - (Tool Demo) Prelude Operator - David Hunt,Alex Manners
AVV - (11:45-12:30 PDT) - APT: A Short History and An Example Attack - Mark Loveless
BCV - cont...(10:15-11:30 PDT) - Surviving DeFi: How to Prevent Economic Attacks - Jan Gorzny
BCV - (11:30-12:30 PDT) - Breaking Future Crypto Custody - Mehow Powers,Chris Odom
BHV - cont...(10:00-12:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)
BHV - Fishing or Hunting - Ohad Zaidenberg
BTV - (11:15-12:15 PDT) - BTV Presents: Welcome to #IRLIFE. A live IR TableTop Panel - Clay (ttheveii0x),plug,Ch33r10,Bassem Helmy,Wayland,O'Shea (sirmudbl00d),Ben (Innismir),Tino aka Paladin316,Neumann (aka scsideath)
CCV - DEX trading without leaking your identity: RAILGUN - Railgun Team
CLV - cont...(10:45-11:15 PDT) - I know who has access to my cloud, do you? - Igal Flegmann
CLV - (11:15-11:59 PDT) - Understanding common Google Cloud misconfiguration using GCP Goat - Joshua Jebaraj
CON - cont...(09:00-23:59 PDT) - Darknet-NG -
CON - cont...(10:00-13:59 PDT) - DEF CON 29 CTF by OOO -
CON - cont...(10:00-11:59 PDT) - Red Team Village CTF - Finals Part 2 -
CPV - cont...(10:00-13:59 PDT) - Workshop: Practically Protecting Phone Privacy (Pre-registration required) - Mauricio Tavares,Matt Nash
CPV - cont...(10:35-13:59 PDT) - CPV Through the Looking-Glass: CPV Day 3 (DC 28)
DC - cont...(09:00-13:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-15:59 PDT) - DEF CON Vendor Area Open
DC - The PACS-man Comes For Us All: We May Be Vaccinated, but Physical Access Control Still Sucks - Anze Jensterle,Babak Javadi,Eric Betts,Nick Draffen
DC - Glitching RISC-V chips: MTVEC corruption for hardening ISA - Adam 'pi3' Zabrocki,Alex Matrosov
DC - Fuzzing Linux with Xen - Tamas K Lengyel
DL - cont...(10:00-11:50 PDT) - reNgine - Yogesh Ojha
DL - cont...(10:00-11:50 PDT) - Frack - William Vermaak
HHV - (11:30-12:30 PDT) - Use a PortaProg to flash, dump, and test ISP and UPDI chips - Bradán Lane,Sara Cladlow
HRV - Ham Radio Exams -
HRV - An Introduction to RF Test Equipment - Kurits Kopf
HTSV - Hack the Wind - Mary Ann Hoppa
ICSV - Top 20 Secure PLC Coding Practices - Sarah Fluchs,Vivek Ponnada
IOTV - cont...(10:00-11:59 PDT) - IoT Village Capture the Flag (CTF) -
LPV - Safecracking for Everyone! - Jared Dygert
SOC - (11:30-12:30 PDT) - QueerCon End-of-Con Chat
WS - cont...(10:00-13:59 PDT) - Windows Internals - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(10:00-13:59 PDT) - From Zero to Hero in Web Security Research - Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki
WS - cont...(10:00-13:59 PDT) - Modern Malware Analysis for Threat Hunters - Aaron Rosenmund,Ryan Chapman
WS - cont...(10:00-13:59 PDT) - Hacking the Metal: An Introduction to Assembly Language Programming - eigentourist

Return to Index - Locations Legend

AIV - Twitter Ethics Bug Bounty: Winners and Wrap-up - Rumman Chowdhury
APV - Car Hacking + Bug Hunting Field Guide for Appsec Hackers - Jay Turla DELETE ME
AVV - cont...(11:45-12:30 PDT) - APT: A Short History and An Example Attack - Mark Loveless
AVV - (12:30-13:15 PDT) - (Tool Demo) ImproHound - Identify AD tiering violations - Jonas Bülow Knudsen
BCV - cont...(11:30-12:30 PDT) - Breaking Future Crypto Custody - Mehow Powers,Chris Odom
BHV - cont...(10:00-12:59 PDT) - CTF: Hospital Under Siege (Pre-registration required)
BHV - Red vs Blue vs Green : The ultimate battle of opinions (or is it) - Ken Kato,Vee Schmitt
BTV - cont...(11:15-12:15 PDT) - BTV Presents: Welcome to #IRLIFE. A live IR TableTop Panel - Clay (ttheveii0x),plug,Ch33r10,Bassem Helmy,Wayland,O'Shea (sirmudbl00d),Ben (Innismir),Tino aka Paladin316,Neumann (aka scsideath)
BTV - (12:30-12:59 PDT) - Year of Mentoring: BTV's Meet-a-Mentor Turns One - muteki
CLV - PK-WHY - Kevin Chen
CLV - (12:20-13:05 PDT) - Cloud Security Orienteering - Rami McCarthy
CON - cont...(09:00-23:59 PDT) - Darknet-NG -
CON - cont...(10:00-13:59 PDT) - DEF CON 29 CTF by OOO -
CON - Red Team Village CTF - Closing Ceremony -
CPV - cont...(10:00-13:59 PDT) - Workshop: Practically Protecting Phone Privacy (Pre-registration required) - Mauricio Tavares,Matt Nash
CPV - cont...(10:35-13:59 PDT) - CPV Through the Looking-Glass: CPV Day 3 (DC 28)
DC - cont...(09:00-13:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-15:59 PDT) - DEF CON Vendor Area Open
DC - DoS: Denial of Shopping – Analyzing and Exploiting (Physical) Shopping Cart Immobilization Systems - Joseph Gabay
DC - No Key? No PIN? No Combo? No Problem! P0wning ATMs For Fun and Profit - Roy Davis
DC - Breaking TrustZone-M: Privilege Escalation on LPC55S69 - Laura Abbott,Rick Altherr
DL - Cotopaxi - Jakub Botwicz
HHV - cont...(11:30-12:30 PDT) - Use a PortaProg to flash, dump, and test ISP and UPDI chips - Bradán Lane,Sara Cladlow
HRV - cont...(11:00-13:59 PDT) - Ham Radio Exams -
HRV - cont...(11:00-12:30 PDT) - An Introduction to RF Test Equipment - Kurits Kopf
HTSV - Cyber Risk Management in the MTS - Josie Long,Kelley Edwards
ICSV - ICS Cyber Threat Intelligence (CTI) Information Sharing Between Brazil and the United States - Helio Sant'ana,John Felker,Max Campos,Paul de Souza,Tom VanNorman
LPV - Intro To Lockpicking - TOOOL
PHV - Hands-On TCP Deep Dive with Wireshark - Chris Greer
SOC - cont...(11:30-12:30 PDT) - QueerCon End-of-Con Chat
SOC - Friends of Bill W. -
WS - cont...(10:00-13:59 PDT) - Windows Internals - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(10:00-13:59 PDT) - From Zero to Hero in Web Security Research - Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki
WS - cont...(10:00-13:59 PDT) - Modern Malware Analysis for Threat Hunters - Aaron Rosenmund,Ryan Chapman
WS - cont...(10:00-13:59 PDT) - Hacking the Metal: An Introduction to Assembly Language Programming - eigentourist

Sunday - 13:00 PDT

Return to Index - Locations Legend

AIV - Wrap Up - AI Village Organizers
APV - AppSec Village Capture the Flag Ends -
APV - 0-Days & Nat 20's - CVSSv3 Through the Lens of Dungeons & Dragons - Alex "RedWedgeX" Hoffman
AVV - cont...(12:30-13:15 PDT) - (Tool Demo) ImproHound - Identify AD tiering violations - Jonas Bülow Knudsen
AVV - (13:15-14:15 PDT) - Scaling Up Offensive Pipelines - Gil Biton
BHV - The Security of Your Digital DNA, from Inception to Death - Garrett Schumacher
BHV - (13:30-13:59 PDT) - It takes a village: Why you should join the Biohacking Village - Rob Suárez
BTV - (13:30-13:59 PDT) - BTV Closing Ceremony
CLV - cont...(12:20-13:05 PDT) - Cloud Security Orienteering - Rami McCarthy
CLV - Cloud Village Closing Keynote
CON - cont...(09:00-23:59 PDT) - Darknet-NG -
CON - cont...(10:00-13:59 PDT) - DEF CON 29 CTF by OOO -
CPV - cont...(10:00-13:59 PDT) - Workshop: Practically Protecting Phone Privacy (Pre-registration required) - Mauricio Tavares,Matt Nash
CPV - cont...(10:35-13:59 PDT) - CPV Through the Looking-Glass: CPV Day 3 (DC 28)
DC - cont...(09:00-13:59 PDT) - DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-15:59 PDT) - DEF CON Vendor Area Open
DC - Extension-Land: exploits and rootkits in your browser extensions - Barak Sternberg
DC - Why does my security camera scream like a Banshee? Signal analysis and RE of a proprietary audio-data encoding protocol - Rion Carter
DC - Timeless Timing Attacks - Mathy Vanhoef,Tom Van Goethem
DL - cont...(12:00-13:50 PDT) - Cotopaxi - Jakub Botwicz
HRV - cont...(11:00-13:59 PDT) - Ham Radio Exams -
HTSV - SeaTF, Pirate Hat, and Salty Sensor Results, Closing Statements - Brian Satira
ICSV - ICS Intrusion KillChain explained with real simulation - Javier Perez,Juan Escobar
ICSV - (13:30-13:59 PDT) - Building an ICS Firing Range (in our kitchen): Sharing Our Journey & Lessons Learned (so you don’t have to) - Moritz Thomas,Nico Leidecker
LPV - Bobby Pins, More Effective Than Lockpicks? - John the Greek
PHV - cont...(12:00-13:59 PDT) - Hands-On TCP Deep Dive with Wireshark - Chris Greer
SOC - A&E Pool Party! -
WS - cont...(10:00-13:59 PDT) - Windows Internals - Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman
WS - cont...(10:00-13:59 PDT) - From Zero to Hero in Web Security Research - Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki
WS - cont...(10:00-13:59 PDT) - Modern Malware Analysis for Threat Hunters - Aaron Rosenmund,Ryan Chapman
WS - cont...(10:00-13:59 PDT) - Hacking the Metal: An Introduction to Assembly Language Programming - eigentourist

Sunday - 14:00 PDT

Return to Index - Locations Legend

APV - Attacking Modern Environments Series: Attack Vectors on Terraform Environments - Mazin Ahmed
AVV - cont...(13:15-14:15 PDT) - Scaling Up Offensive Pipelines - Gil Biton
AVV - (14:15-15:15 PDT) - Signed, Sealed, Delivered: Comparing Chinese APTs behind Software Supply Chain Attacks - Cheryl Biswas
BHV - Biohacking Village Wrap-Up -
CON - cont...(09:00-23:59 PDT) - Darknet-NG -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - cont...(10:00-15:59 PDT) - DEF CON Vendor Area Open
DC - Robots with lasers and cameras (but no security): Liberating your vacuum from the cloud - Dennis Giese
DC - Old MacDonald Had a Barcode, E-I-E-I CAR - Richard Henderson
DC - Instrument and Find Out: Writing Parasitic Tracers for High(-Level) Languages - Jeff Dileo
DC - (14:30-14:50 PDT) - The Agricultural Data Arms Race: Exploiting a Tractor Load of Vulnerabilities In The Global Food Supply Chain - Sick Codes
HHV - Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables - Federico Lucifredi
HRV - Ham Radio Village Closing Commentary -
ICSV - ICS Jeopardy - Chris Sistrunk,Maggie Morganti,Mary Brooks,Tatyana Bolton
LBV - Bypass 101
LBV - (14:30-15:59 PDT) - Bypass Village Panel
LPV - (14:15-14:45 PDT) - Intro To Lockpicking - TOOOL
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Return to Index - Locations Legend

APV - AppSec Quiz Time! - Eden Stroet

AVV - cont...(14:15-15:15 PDT) - Signed, Sealed, Delivered: Comparing Chinese APTs behind Software Supply Chain Attacks - Cheryl Biswas

AVV - (15:15-15:59 PDT) - How I got COVID in a RedTeam: Social engineering and physical intrusion for realistic attack simulations. - Daniel Isler

CON - cont...(09:00-23:59 PDT) - Darknet-NG -

DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris

DC - cont...(10:00-15:59 PDT) - DEF CON Vendor Area Open

DC - (CANCELED) Discord Closing Ceremonies - Dark Tangent

HHV - The Black Box and the Brain Box: When Electronics and Deception Collide - Gigs

LBV - cont...(14:30-15:59 PDT) - Bypass Village Panel

LPV - Intro to high security locks and lockpicking - N thing

SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Sunday - 16:00 PDT

Return to Index - Locations Legend

AVV - Adversary Village Closing Ceremony - Adversary Village Team
CON - cont...(09:00-23:59 PDT) - Darknet-NG -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
DC - DEF CON Closing Ceremonies, Black Badge Ceremonies - Dark Tangent
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Sunday - 17:00 PDT

Return to Index - Locations Legend

CON - cont...(09:00-23:59 PDT) - Darknet-NG -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Sunday - 18:00 PDT

Return to Index - Locations Legend

CON - cont...(09:00-23:59 PDT) - Darknet-NG -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Sunday - 19:00 PDT

Return to Index - Locations Legend

CON - cont...(09:00-23:59 PDT) - Darknet-NG -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Sunday - 20:00 PDT

Return to Index - Locations Legend

CON - cont...(09:00-23:59 PDT) - Darknet-NG -
DC - cont...(09:00-20:59 PDT) - Chillout Lounges - DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Sunday - 21:00 PDT

Return to Index - Locations Legend

CON - cont...(09:00-23:59 PDT) - Darknet-NG -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Sunday - 22:00 PDT

Return to Index - Locations Legend

CON - cont...(09:00-23:59 PDT) - Darknet-NG -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Sunday - 23:00 PDT

Return to Index - Locations Legend

CON - cont...(09:00-23:59 PDT) - Darknet-NG -
SOC - cont...(13:00-23:59 PDT) - A&E Pool Party! -

Speaker List

Graduate Student
Ph.D.
Ph.D.
Ph.D.
_hyp3ri0n aka Alejandro Caceres
Özkan Mustafa AKKUŞ
Aaron Guzman
Aaron Rosenmund
Abhijith B R
Abhijith B R
Abishek Gupta
Abstrct
Abstrct
Acid T
Adam 'pi3' Zabrocki
Adam Schaal
Adversary Village Team
Agent X
AI Village Organizers
AI Village Organizers
AI Village Organizers
Alex "Jay" Balan
Alex "RedWedgeX" Hoffman
Alex Hoekstra
Alex Lomas
Alex Manners
Alex Matrosov
Alex Pearlman
Alexander Heinrich
Alexander Klimburg
Alexander Vigovskiy
Alexandre Sieira
Alexei Kojenov
Alexei Kojenov
Alfonso Ruiz Cruz
Alissa Knight
Alissa Knight
Allan Cecil - dwangoAC
Allan Cecil - dwangoAC
Allan Tart
Alton Crossley
Alyssa Miller
Amelie Koran
Amelie Koran
Ami Luttwak
Amir Shaked
Amit Elazari
Anahit Tarkhanyan
Anant Shrivastava
Andrea Downing
Andy Dennis

Andy Piazza
Ang Cui
Anita Nikolich
Anna Szeto
Anthony "Cx01N" Rose
Anthony "Cx01N" Rose
Anthony Hendricks
Anthony Hendricks
Anthony Hendricks
Anthony Kava
Anto Joseph
Anze Jensterle
Arjun Gopalakrishna
Arnold Holzel
Aseem Jakhar
Ash
Atul Nair
August Cole
Austin Allshouse
Avinash Jain
Babak Javadi
Bailey Bercik
Barak Hadad
Barak Sternberg
Barb Byrum
Barton Rhodes
Bassem Helmy
Batuhan Sancak
Ben (Innismir)
Ben Bornholm
Ben Bornholm
Ben Gardiner
Ben Gardiner
Ben Gardiner
Ben Gardiner
Ben Hughes
Ben Nassi
Ben S
Benjamin Kurtz
Benjamin Kurtz
BiaSciLab
Bill "Woody" Woodcock
Bill Graydon
Bill Hatzer
Blind Hacker JoeB
Bob Sullivan
bombnav
Bradán Lane
Bradán Lane
Bradán Lane
Brandon Bailey
Brian Behlendorf
Brian Hong
Brian Martin
Brian Satira

Brianna Lennon
Bruce Schneier
Bruce Schneier
Bryan Fields
Bryce Kerley
Byeongcheol Yoo
cablethief
Camille Eddy
Capt Aaron Bolen
Carlos Polop
Carsten Schürmann
Cassandra Young
Cat Self
Cat Self
Cat Self
Cedric Owens
cemaxecuter
Ch33r10
Ch33r10
Chad Rikansrud (Bigendian Smalls)
Chad Seaman
Charles Fracchia
Charles Rumford
Chen Cao
Chen Gour-Arie
Cheryl Biswas
Cheryl Biswas
Cheryl Biswas
Chester Hosmer
Chloe Messdaghi
Chris Greer
Chris Odom
Chris Silvers
Chris Sistrunk
Chris Sperry
Christian Dameff
Christina Lekati
Christopher Hadnagy
Christopher Russell
Christopher Von Reybyton
Christopher Wade
Chuanda Ding
Chuck McAuley
Claire Vacherot
Clay (ttheveii0x)
Clay (ttheveii0x)
Cliff Neve
Colin Cantrell
Colin H
Constantine Macris
Constantine Macris
Cory Doctorow
Craig Gidney
CTRL/rsm
CTRL/rsm

d1dymu5
Dabao Wang
Dan Borges
Dan Borges
Dan Gunter
Dan Hastings
Dan Petro - AltF4
Dan Petro - AltF4
Daniel "Rasta" Duggan
Daniel Chen
Daniel Crowley
Daniel Garrie
Daniel Isler
Daniel Prizmant
Daniel Roy
Danny D. Henderson Jr
Danny McPherson
Danyelle Davis
Dark Tangent
Dark Tangent
Dark Tangent
Dark Tangent
Darren Cofer
Dave Lewis
David Cass
David Dworken
David Etue
David Hunt
David Kennedy
David Patten
David Strachan
De
Deb Herrity
Declyn S.
Deep Therapy
DEF CON Policy Panel
DEF CON Policy Panel
DEF CON Policy Panel
Dennis Giese
Dennis Skarr
Dhillon ‘L33tdawg’ Kannabhiran
Dieter Sarrazyn
Dikla Barda
Dikla Barda
Dimitry "Op_Nomad" Snezhkov
Dimitry "Op_Nomad" Snezhkov
Dimitry "Op_Nomad" Snezhkov
Dimitry "Op_Nomad" Snezhkov
DJ Pie & Darren
DJ Pie & Darren
DJ Pie & Darren
DJ Pie & Darren
DJ St3rling
djdead
djdead

djdead
Dmitrijs Trizna
Don C. Weber
Don Hatfield
Dr. McGrew
Drimacus
Dylan Barker
Dylan The Magician
Ed McGrady
Eddie Perez
Eden Stroet
Eden Stroet
Eden Stroet
eigentourist
eigentourist
Elad Ciuraru
Elizabeth Biddlecome
Elizabeth Biddlecome
Elizabeth Biddlecome
Elizabeth Schweinsberg
Elizabeth Wharton
Elonka Dunin
Emanuel Rodrigues
Eran Segal
Erez Yalon
Eric Betts
Eric Escobar
Eric Escobar
Eric Escobar
Eric Fey
Eric Gershman
Eric Goldstein
Eric Perakslis
Erick Galinkin
Erik Steringer
Erin Browning
Ernie Bio
Eugene Lim
Eugene Neelou
Eyal Karni
Fatih Ozavci
Faye Francy
Federico Lucifredi
Federico Lucifredi
Federico Lucifredi
Felipe Duarte
Felipe Pr0teus Espósito
Francesco Piccoli
Francisco Cabañas
Frank Duff
Frank Pound
Fred Mastrippolito
freqy
FuzzyNop
FuzzyNop

Gabby Raymond
Gal Kaufman
Gal Nagli
Garrett Schumacher
Gary Kessler
Gary Kessler
Gary Kessler
Gavin Klondike
Gavin Klondike
Gavin Klondike
Gert-Jan Bruggink
Gigs
Gigs
Gigs
Gil Biton
Ginny Spicer
Glenice Tan
Gokul Alex
Grant Ongers (rewtd)
Grant Romundt
Gregg Horton
Guillaume Fournier
Guillermo Christensen
H I Sutton
Hao Xing
Harri Hursti
Harri Hursti
Harshal Tupsamudre
Harshit Agrawal
Hash Salehi
Hector Cuevas Cruz
Helio Sant'ana
Henry Hill
Henry Hill
Henry Hill
Henry Hill
Henry Hill
henry
Huajiang "Kevin2600" Chen
Hutch (Justin Hutchens)
Hyrum Anderson
Ian Coldwater
Ian Vitek
Icetre Normal
Igal Flegmann
Igal Flegmann
Ionut Cernica
Irvin Lemus
Irvin Lemus
Irvin Lemus
Izar Tarandach
Jacob Baines
Jake "Hubbl3" Krasnov
Jake Williams
Jakub Botwicz

James Dolan
James Kettle
James McKee (punkcoder)
James Pavur
Jamie Williams
Jamil Jaffer
Jan Gorzny
Jared Dygert
Jared Stroud
Jason Hopper
Jason Whelan
Javier Perez
Jay Turla DELETE ME
Jay Turla
Jay Turla
Jean Francois Maes
Jeff 'R3plicant' Tully
Jeff Dileo
Jenko Hwong
Jennifer DeTrani
Jennifer Goldsack
Jennifer Haverman
Jeremy Brown
Jesse Michael
Jessica Hoffman
Jessilyn Dunn
jiska
Joe Billingsley
Joe Schottman
Joe Slowik
Joe Vest
Joel Isaac
John Bambenek
John Curry
John Ellis
John Felker
John McCombs
John Stoner
John the Greek
Jon Marler
Jon Szymaniak
Jonas Bülow Knudsen
Jordan Sessler
Jordan Sessler
Jorge Orchilles
José Hernandez
Jose Barajas
Jose Garduno
Joseph Gabay
Josh Marks
Josh McIntyre
Josh Stroschein
JoshInGeneral
Joshua Jebaraj
Joshua Smailes

Josie Long

Joy Ho

Juan Escobar

Julia Atkinson

Juneau Jones

Juneau Jones

Junyuan Zeng

Justin Ehrenhofer

Justin Perdok

K

K

Kadan Stadelmann

Kaitlyn Handelman

Kaitlyn Handelman

Kaitlyn Handelman

Kala Kinyon

kampf

kampf

kampf

Karan Aditya Ghoshal

Karl Fosaaen

Karl Lovink a.k.a. Cyb0rg42

Katie Whiteley

Katie Whiteley

Kavisha Sheth

Keith Chapman

Kelley Edwards

Kelly Kaoudis

Ken Kato

Ken Pyle

Kendra Albert

Kevin Chen

Kevin Hood

Kevin Jones

Kevin Leffew

Kevin Skoglund

Kimberley Tam

Kirsten Renner

Klaus Schmeh

Kris Silvers

Kristy Westphal

Kristy Westphal

Krisz Klink

Kurits Kopf

Ladislav Baco

Larry Grossman

Laura Abbott

Lauren Zabierek

Leeloo Granger

Lennert Wouters

Leonardo Viveiros

Liana McCrea

Lily Newman

Lisa Forte

Lock Noob

Louigi Verona
Louigi Verona
Luca Bongiorni
Lucas Bonastre
Lucia Savage
Luis Ángel Ramírez Mendoza
Luis Gomes
Madhu Akula
Madhu Akula
Maggie Morganti
Magik Plan
Magno Logan DELETE ME
Magno Logan
Manabu Niseki
Manu Zacharia
Marc Smeets
Maretta Morovitz
Margaret Fero
Mariam Elgabry
Marian Novotny
Mark Loveless
Mark Morowczynski
Mars Cheng
Martin Doyhenard
Martin Ingesen
Mary Ann Hoppa
Mary Brooks
MasterChen
Mathieu Stephan
Mathy Vanhoef
Matt Gaffney
Matt Gaffney
Matt McMahon
Matt Nash
Matthew Bryant
Matthew Coles
Matthew Eidelberg
Matthew Gracie
Matthew Luallen
mattrix
Maurice Turner
Maurice Turner
Mauricio Tavares
Mauricio Velazco
Mauro Cáseres Rozanowski
Mauro Cáseres Rozanowski
Max Campos
Maxwell Dulin
Mazin Ahmed
Mazin Ahmed
Meadow Ellis
Mehmet Onder Key
Mehow Powers
Meisam Eslahi
Merin MC

Merin MC
Merin MC
Merin MC
Mert Can Kilic
Michael Chien
Michael Lewellen
Michael Long
Michael Murray
Michael Raggo
Michael Raggo
Michael Register
Michael Schloh von Bennewitz
Michael Solomon
Michael Whiteley
Michael Whiteley
Michael Wylie
Michael Wylie
MIchelle Holko
Mickey Shkatov
Mike Cohen
Mike Kiser
Mike Kiser
Mike Spicer
Mila Paul
Minzhi He
Mishaal Khan
Miss Jackalope
Mitch Parker
Mixæl Laufer
Mixmaster Morris
Mixmaster Morris
Mohammed Aldoub
Monero Sound
Moritz Thomas
muteki
n0x08
N thing
N thing
Nadir Akhtar
Nadir Akhtar
Nathan Case
Nathan Kirkland
Nathan
Nathan
Neumann (aka scsideath)
Nia Johnson
Nicholas Childs
Nick Ashworth
Nick Draffen
Nick Roy
Nick Roy
Nico "Socks" Smith
Nico Leidecker
Nina Alli
Nina Lowe

O'Shea (sirmudbl00d)
Ochaun Marshall
Oded Vanunu
Oded Vanunu
Ohad Zaidenberg
Ohm-i
Olivia Stella
Omar Santos
Omenscan
Orange Tsai
Parbati Kumar Manna
PatH
Patrick Ross
Patrick Wardle
Paul de Souza
Paul Vixie
Paz Hameiri
Peace Barry
Pedro Umbelino
Peiyu Wang
Peter Kacherginsky
Peter Manev
Phil Eveleigh
Philippe Delteil
Phillip Wylie
Pia Zaragoza
plug
plug
plug
Preston Pierce
Preston Thomas
PW Singer
Quinten Bowen
Rabbit
Rae
Railgun Team
Rami McCarthy
Rebecca Lynch
Reddcoin
RedDragon
rehr
rehr
rehr
rehr
rehr
rehr
Renzon Cruz
Rex Guo
Reza Soosahabi
Ria Cheruvu
Ria Cheruvu
Rich Harang
Richard Henderson
Richard Thieme AKA neuralcowboy
Richard Thieme AKA neuralcowboy

Rick Altherr
Ricky Banda
Rion Carter
Ritu Gill
Rob Suárez
Robert Wagner
Rod Soto
Rod Soto
Rodrigo "Sp0oKeR" Montoro
Roman Zaikin
Roman Zaikin
Ron Stoner
Ron Stoner
Ronald Broberg
Rotem Bar
Roy Davis
Roy Feng
Rumman Chowdhury
Rumman Chowdhury
Rusty Hodge
Rusty Hodge
Ryan Chapman
Ryan Elkins
Ryan Holeman
Ryan M
Ryan MacDougall
s1gns of l1fe
s1gns of l1fe
Sach
Sagar Samtani
Sagar Samtani
Sagi Sheinfeld
Salvador Mendoza
Sam Bowne
Sam Bowne
Sam Bowne
Samir Bhagwat
Samuel Kimmons
Samuel Kimmons
Sang-Oun Lee
Sanne Maasakkers
Sara Cladlow
Sara Cladlow
Sara Cladlow
Sarah Fluchs
Sarang Noether
Sarang Noether
Sarang Noether
Scotch & Bubbles
Sebastiaan Provost
Sebastian Bay
Secret Network Team
Selmon Yang
Sergey Chubarov
Seth Kintigh

Shannon Lantzky
Shantanu Khandelwal
Sharon Brizinov
Sheila A. Berta
Shinchul Park
Shir Tamari
ShortTie
ShortTie
Shubham Jain
Sick Codes
Sick Codes
singe
Slava Makkaveev
Solstice
Sounil Yu
Stan Bar
Stefan Stephenson-Moe
Stefano Meschiari
Stella Biderman
Stephan Wampouille
Stephen Pullum
Steve Luczynski
Steve Luczynski
Steve Wood
Steven Seeley
Steven Yang
Storj Team
Suha Sabi Hussain
Sunny Wear
Surya Teja Masanam
Susan Greenhalgh
Sylvain Afchain
Sylvain Baubeau
Tal Leibovich
Tamas K Lengyel
Tan Kee Hock
Tanya Janca
Tatyana Bolton
Ted Harrington
Tennisha Martin
Tense Future
Teri Williams
Terrestrial Access Network
Thaad
Thom Dixon
Thomas Bristow
Thomas Hicks
Thomas Pace
Thomas Roth
Tianze Ding
Tilottama Sanyal
Tilottama Sanyal
Tim Faraci
Tim Jensen (EapolSniper)
Tim Schulz

Tim Yardley
Timur Yunusov
Tino aka Paladin316
Tod Beardsley
Tom Mouatt
Tom Van Goethem
Tom VanNorman
Tomer Bar
Tomer Bar
Tony Virelli
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
TOOOL
Trenton Ivey
Tushar Verma
Tyler Gardner
Uri Katz
Utku Sen
Vahagan Vardanyan
Vandana Verma Sehgal
Vasant Chinnipilli
Vee Schmitt
Vee
Vic Harkness
Vic Harkness
Vic Huang
Victor Hanna
Vincent "Vinnybod" Rose
Vincent "Vinnybod" Rose
Vincent Yiu
Vivek Nair
Vivek Ponnada
Wayland
Waylon Grange
Wendy Edwards
Wendy Edwards
Wes Lambert
Wes Lambert
Wesley McGrew
Will Pearce
Will Thomas
William Vermaak
Wu Ming
Y L
Yaara Shriki
Yaara Shriki
Yakov Shafranovich

Yaniv Agman
Yaron Zinar
Yaz Khoury
Yesterday & Tomorrow
Yogesh Ojha
Yuebin Sun
Yuhao Weng
Yuval Avrahami
Z3NPI
Zachary Minneker
Zebbler Encanti Experience
Zekai Wu
Zhiniang Peng
Zhipeng Huo
Zoltán Balázs

Talk List

.GOV Doppelgänger: Your Häx Dollars at Work - RCV
"Ask a Ham" Q&A - HRV
"The Poisoned Diary": Supply Chain Attacks on Install scripts - APV
"Who Bears the Risk?" Why a Market Incentives Perspective is Critical to Protecting Patients from Cyber Threats - BHV
(CANCELED) Discord Closing Ceremonies - DC
(Replay) Racketeer Toolkit. Prototyping Controlled Ransomware Operations - DC
(Replay) UFOs: Misinformation, Disinformation, and the Basic Truth - DC
(Tool Demo) ImproHound - Identify AD tiering violations - AVV
(Tool Demo) New generation of PEAS - AVV
(Tool Demo) Prelude Operator - AVV
(Tool Demo) PurpleSharp: Automated Adversary Simulation - AVV
(Tool Demo) Red Team Credentials Reconnaissance (OLD with a TWIST) - AVV
(Tool Demo) Tenacity: An Adversary Emulation Tool for Persistence - AVV
(Workshop) - Integrating DAST tools into developers' test process - APV
(Workshop) From zero to hero: creating a reflective loader in C# - AVV
(Workshop) Tradecraft Development in Adversary Simulations - AVV
*nix Processes. Starting, Stopping, and Everything In Between - PHV
0-Days & Nat 20's - CVSSv3 Through the Lens of Dungeons & Dragons - APV
1.21 Gigawatts! Vulnerabilities in Solar Panel Controllers - IOTV
2021 - Our Journey Back To The Future Of Windows Vulnerabilities and the 0-days we brought back with us - DC
40 cores and a CPU - BICV
5 years of IoT vulnerability research and countless 0days - A retrospective - IOTV
A Cohort of Pirate Ships - BHV
A Deep Dive Into Supply Chain Vulnerabilities: And How SecDevOps Can Save the Day - APV
A Deep Dive on Vulnerability Disclosure for Election Systems - VMV
A Discussion with Agent X - DC
A Journalist’s Perspective on Fake News - VMV
A Lazy r2 Solve of @mediumrehr Challenge 6 - HHV
A Lazy r2 Solve of @mediumrehr Challenge 6 - HHV
A Lazy r2 Solve of @mediumrehr Challenge 6 - HHV
A new class of DNS vulnerabilities affecting many DNS-as-Service platforms - DC
A SERVERLESS SIEM: DETECTING ALL BADDIES ON A BUDGET - BTV
A-ISAC CTF -- Pre-registration Required - ASV
A-ISAC CTF -- Pre-registration Required - ASV
A&E Pool Party! - SOC
A&E Pool Party! - SOC
A&E Pool Party! - SOC
A&E Pool Party! - SOC
“Alexa, have you been compromised?” — Exploitation of Voice Assistants in Healthcare (and other business contexts) - IOTV
Abusing SAST tools! When scanners do more than just scanning - DC
ADSB Demo and Paper Airplanes - ASV
ADSB Demo and Paper Airplanes - ASV
Advanced Wireless Attacks Against Enterprise Networks - WS
Adventures in MitM-land: Using Machine-in-the-Middle to Attack Active Directory Authentication Schemes - DC
Adventures in Pro Bono Digital Forensics Work - BTV
Adversary Infrastructure Tracking with Mihari - RCV
Adversary Village Closing Ceremony - AVV
Adversary Village Keynote - AVV
Adversary Village Kick-off - AVV
AI Policy Talk: "An AI Security ISAC" and "An AI Playbook" - AIV
AIAA CubeSat Hacking Workshop - Virtual Lab #1 - ASV

AIAA CubeSat Hacking Workshop - Virtual Lab #2 - ASV
AIAA CubeSat Hacking Workshop - Virtual Lab #3 - ASV
AIAA CubeSat Hacking Workshop - Virtual Lab #4 - ASV
AIAA CubeSat Hacking Workshop - World Premier of the videos - ASV
AIS Protocol Internals (Abridged) - HTSV
AIS Tools Demo (DEF CON) - HTSV
AIS Tools - DL
Algorithmic Ethics Bug Bounty Contest Announcement - AIV
Amateur Radio Digital Modes Primer - HRV
Amateur Radio Mesh Networking: Enabling Higher Data-rate Communications - HRV
An Introduction to RF Test Equipment - HRV
Analysis 101 and 102 for the Incident Responder - WS
Analysis 101 and 102 for the Incident Responder - WS
Antenny - ASV
Antenny - ASV
Approaches to Attract, Develop, and Retain an Industrial Cybersecurity Workforce - ICSV
AppSec 101: A Journey from Engineer to Hacker - APV
AppSec Quiz Time! - APV
AppSec Quiz Time! - APV
AppSec Quiz Time! - APV
AppSec Village Capture the Flag Ends - APV
AppSec Village Capture the Flag Starts - APV
APT Hunting with Splunk - PHV
APT: A Short History and An Example Attack - AVV
Are Barcodes on Ballots Bad? - VMV
Are We Still Doing it? 10 Locksport Hobbies that go Beyond Lock Picking - LPV
ARINC 429 Lab - ASV
ARINC 429 Lab - ASV
Assless Chaps: a novel combination of prior work to crack MSCHAPv2, fast (or why MSCHAPv2 is so broken, it’s showing it’s whole ass) - RFV
At least ten questions for “Bad HIPPA Takes” (@BadHIPPA), 2021’s best tweeter on privacy, pandemic, and snark. - BHV
ATM Transaction Reversal Frauds (And how to fight them) - PYV
Attack and Detect with Prelude Operator and Security Onion - BTV
Attacking Modern Environments Series: Attack Vectors on Terraform Environments - CLV
Attacking Modern Environments Series: Attack Vectors on Terraform Environments - APV
AutoDriving CTF - CON
Automated Tear Machines - PYV
AWS cloud attack vectors and security controls - CLV
Azure Active Directory Hacking Wars - CLV
BADASS Meetup (Virtual) - SOC
BCOS Village Contest Overview - BCV
Beetlejuice: The Lessons We Should Have Learned For ICS Cybersecurity - ICSV
Beverage Cooling Contraption Contest - CON
Biohacking Village CTF: Hospital Under Siege (Pre-Qual) (Pre-registration required) - BHV
Biohacking Village Welcome Keynote - BHV
Biohacking Village Wrap-Up - BHV
Black Box Challenges - IOTV
Black Box Challenges - IOTV
Black Cyber Exodus: The Mis-Education (Certification) of Black Cyber - BICV
Blacks in Cybersecurity CTF - CON
Blockchain as a Threat Modeling Thinking Tool - BCV
Blockchain Security Tools - BCV
BLUEMONDAY Series – Exploitation & Mapping of vulnerable devices at scale through self-registration services (DATTO/ EGNYTE/ SYNOLOGY/ MERAKI/ GEOVISION) - IOTV
Bobby Pins, More Effective Than Lockpicks? - LPV

Bottom-Up and Top-Down: Exploiting Vulnerabilities In the OT Cloud Era - ICSV
Breaking Future Crypto Custody - BCV
Breaking Historical Ciphers with Modern Algorithms - CPV
Breaking Secure Bootloaders - DC
Breaking TrustZone-M: Privilege Escalation on LPC55S69 - DC
Bring Your Own Print Driver Vulnerability - DC
BTV Presents: Forensics Station - Workshop 1 - BTV
BTV Presents: Malware Station - Maldoc Workshop - BTV
BTV Presents: Threat Report Roulette - BTV
BTV Presents: Welcome to #IRLIFE. A live IR TableTop Panel - BTV
Bug bounty Hunting Workshop - WS
Bug Hunter's Guide to Bashing for a Car Hacking Bug Bash or Contest - CHV
Build Automotive Gateways with Ease - CHV
Building an ICS Firing Range (in our kitchen): Sharing Our Journey & Lessons Learned (so you don't have to) - ICSV
Bundles of Joy: Breaking macOS via Subverted Applications Bundles - DC
C2Centipede: APT level C2 communications for common reverse HTTP shell tools - AVV
California Cyber Innovation Challenge CTF -- Pre-registration Required - ASV
Can I Make My Own Social Threat Score? - RCV
Can't Stop the Code: Embrace the Code - APV
Car Hacking + Bug Hunting Field Guide for Appsec Hackers - APV
Car Hacking CTF - CON
Career Hacking: Tips and Tricks to Making the Most of your Career - CAHV
Catching (and Fixing) an Unlimited Burn Vulnerability - BCV
Caught you - reveal and exploit IPC logic bugs inside Apple - DC
Central bank digital currency, threats and vulnerabilities - DC
Certified Ethereum Professional (CEP) Overview - BCV
Chillout Lounges - DC
Chillout Lounges - DC
Chillout Lounges - DC
Chillout Lounges - DC
Chinese Military Bioweapons and Intimidation Operations: Part III - BHV
Cloud security for healthcare and life sciences - BHV
Cloud Security Orienteering - CLV
Cloud Village CTF - Registration - CLV
Cloud Village CTF - CLV
CMD+CTRL - CON
CMD+CTRL - CON
Coindroids - CON
Collecting CANs: a Bridge Less Traveled - ASV
Colorful AppSec - APV
Commercial Transportation: Trucking Hacking - CHV
Community Roundtable - (De)Criminalizing Hacking Around the Globe - DC
Community Roundtable - 10 years after SOPA: where are we now? - DC
Community Roundtable - If only you knew - DC
Community Roundtable - Implementing Cyber Solarium Commission Policy - DC
Community Roundtable - RANSOMWARE: Combatting Ransomware on a Global Stage / The realities of responding to ransomware - DC
Community Roundtable - Supply Chain in the COVID Era - DC
Community Roundtable - Thinking About Election Security - DC
Community Roundtable - Toward a Global IoT Code of Practice - DC
Community Roundtable - Volunteer Hacker Fire Department - DC
Community Roundtable - We can build it. We have the technology. So why aren't we? - DC
Community Roundtable - We need to talk about Norm – Discussions on International cyber norms in diplomacy - DC
Community Roundtable - Zero Trust, Critical Software, and a Cyber Safety Review Board - DC
Consider the (Data) Source - ICSV

COSTA (Coinbase Secure Trait Analyzer) - BCV
Cotopaxi - DL
CPDLC: Man-in-the-middle attacks and how to defend against them - ASV
Crippling the Grid: Examination of Dependencies and Cyber Vulnerabilities - ICSV
Cross-document messaging technology, how to hack it, and how to use it safely. - APV
Crossover Episode: The Real-Life Story of the First Mainframe Container Breakout - DC
Cryptocurrency Trivia! - CCV
CSP is broken, let’s fix it - APV
CSPM2CloudTrail - Extending CSPM Tools with (Near) Real-Time Detection Signatures (Lightning Talk) - CLV
CybatiWorks Mission Station Workshop - ICSV
Cyber Defense Matrix in Healthcare - BHV
Cyber in the Under Sea - HTSV
Cyber Operations and Operational Wargames on Port Infrastructure - HTSV
Cyber Risk Management in the MTS - HTSV
Cyber-SHIP Lab Talk and Demo - HTSV
Darknet-NG - CON
Darknet-NG - CON
Darknet-NG - CON
Data Duplication Village - Last Chance Pickup Only - DDV
Data Duplication Village - Open for dropoff only - DDV
Data Duplication Village - Open - DDV
Data Duplication Village - Open - DDV
DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup - SOC
Decoding NOAA Weather Sat Signals - ASV
Deep Space Networking - ASV
Deep Space Networking - ASV
DEF CON 29 CTF by OOO - CON
DEF CON 29 CTF by OOO - CON
DEF CON 29 CTF by OOO - CON
DEF CON Bike Ride - CON
DEF CON Closing Ceremonies, Black Badge Ceremonies - DC
DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open - DC
DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open - DC
DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open - DC
DEF CON Human Registration (Badge Pickup) Open - DC
DEF CON Movie Night - Tron - DC
DEF CON Movie Night - Upgrade - DC
Defeating Physical Intrusion Detection Alarm Wires - DC
Defending against nation-state (legal) attack: how to build a privacy-protecting service in the era of ubiquitous surveillance - DC
Defending IoT in the Future of High-Tech Warfare - IOTV
Defending the Unmanned Aerial Vehicle: Advancements in UAV Intrusion Detection - ASV
DeFi Must Change or Hacks Will Accelerate - BCV
Depthcharge - DL
Designing a C2 Framework - AVV
Detecting Attackers Using Your Own Sensors with State Estimation - ICSV
Detection Challenges in Cloud Connected Credential Abuse Attacks - CLV
Developing Aerospace Security Training 3D Models - ASV
DevSecOps: Merging Security and Software Engineering - APV
DEX trading without leaking your identity: RAILGUN - CCV
DFDs Ain't That Bad - APV
DHS REBOOTING CRITICAL INFRASTRUCTURE PROTECTION Panel with DEF CON Policy Panel - DC
Digital Forensics and Incident Response Against the Dark Arts: The Battle of Malicious Email and Downloaders - WS
Discord Practice Net - HRV
Do No harm; Health Panel : Live version - A DEF CON Policy Panel - DC

Do We Really Want to Live in the Cyberpunk World? - ICSV
Do you like to read? I know how to take over your Kindle with an e-book - DC
Do You Really Own Your NFTs? - BCV
Don't Dare to Exploit - An Attack Surface Tour of SharePoint Server - DC
Don’t fear the BUS, it won’t run you over. - ASV
Doors, Cameras, and Mantraps OH MY! - LPV
DoS: Denial of Shopping – Analyzing and Exploiting (Physical) Shopping Cart Immobilization Systems - DC
Drone Security Research Series – Ep6 Hacking with drones - ASV
Drunk Hacker History - CON
eBPF, I thought we were friends! - DC
EFF Tech Trivia - CON
Empire - DL
Encryption for Developers - APV
ESP8266, do you know what's inside your IoT? - RFV
Ethereum Hacks & How to Stop Them - BCV
Ethics at the Edge: IoT as the Embodiment of AI for Rampant Intelligence Actuation - IOTV
Evading Detection a Beginner's Guide to Obfuscation - WS
Evaluating Wireless Attacks on Real-World Avionics Hardware - ASV
Everything is a C2 if you're brave enough - AVV
Evils in the DeFi world - BCV
Exploiting Blue Team OPSEC failures with RedELK - AVV
Exploiting the O365 Duo 2FA Misconfiguration (Lightning Talk) - CLV
Extension-Land: exploits and rootkits in your browser extensions - DC
Extracting all the Azure Passwords - CLV
F**k You, Pay Me - Knowing your worth and getting paid - CAHV
Federal Perspective on Aerospace Cybersecurity - ASV
Finding Hidden Gems via URL Shortener Services - RCV
Fireside Chat - August Cole - ICSV
Fishing or Hunting - BHV
Flash Loans Demystified - BCV
Forensicating Endpoint Artifacts in the World of Cloud Storage Services - BTV
Fortifying ICS - Hardening and Testing - ICSV
Frack - DL
Frag, You’re it - Hacking Laser Tag - RFV
Friends of Bill W. - SOC
Friends of Bill W. - SOC
Friends of Bill W. - SOC
Friends of Bill W. - SOC
Friends of Bill W. - SOC
Friends of Bill W. - SOC
Friends of Bill W. - SOC
From CTF to CVE - CHV
From On-Prem to the Cloud - Hybrid AD attack path - AVV
From Zero to Hero in Web Security Research - WS
From Zero to Hero in Web Security Research - WS
Fuzzing CAN / CAN FD ECU's and Network - CHV
Fuzzing Linux with Xen - DC
Fuzzing NASA Core Flight System Software - ASV
Game Theory: Understanding and Strategy and Deception - AVV
Getting Started with Decentralized Object Storage - CCV
Getting started with low power & long distance communications - QRP - HRV
Git Wild Hunt - DL
Glitching RISC-V chips: MTVEC corruption for hardening ISA - DC
Gold Bug Q&A - CPV
Gone Apple Pickin': Red Teaming macOS Environments in 2021 - DC

Gothcon 2021 (Virtual) - SOC
Gothcon 2021 - SOC
Hack the Conspiracies - VMV
Hack the hackers: Leaking data over SSL/TLS - DC
Hack the Sea Cabana Party - HTSV
Hack the Wind - HTSV
Hack-A-Sat 2: The Good, The Bad and the Cyber-Secure - ASV
Hack-A-Sat2 Satellite Platform - ASV
Hack-A-Sat2 Satellite Platform - ASV
Hack3r Runw@y - CON
Hack3r Runw@y - CON
Hacker Flairgrounds - SOC
Hacker Jeopardy - CON
Hacker Jeopardy - CON
Hacker Karaoke (Virtual) - SOC
Hacker Karaoke (Virtual) - SOC
HACKERS INTO THE UN? Engaging in the cyber discussions on war & peace - DC
Hacking G Suite: The Power of Dark Apps Script Magic - DC
Hacking Humans with AI as a Service - DC
Hacking the Apple AirTags - DC
Hacking the Metal: An Introduction to Assembly Language Programming - WS
Hacking the Metal: An Introduction to Assembly Language Programming - WS
Hacking to Save Democracy: What Technologists Need to Know About Election Administration - VMV
Hacking Your Career: The Options - CAHV
HACMS Live Demo - ASV
HACMS Live Demo - ASV
Ham Radio Exams - HRV
Ham Radio Exams - HRV
Ham Radio Exams - HRV
Ham Radio Village Closing Commentary - HRV
Hands-On TCP Deep Dive with Wireshark - PHV
Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables - HHV
Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables - HHV
Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables - HHV
Hardware Wallet Show and Tell - CCV
Healthcare Innovation With People of All Abilities - BHV
Hi! I'm DOMAIN\Steve, please let me access VLAN2 - DC
High Turnout, Wide Margins - VMV
High-Stakes Updates | BIOS RCE OMG WTF BBQ - DC
Holistic View of a Flight with Crowd Sourced Data - ASV
House of Heap Exploitation - WS
How Bias and Discrimination in Cybersecurity will have us locked up or dead - BICV
How do you ALL THE CLOUDS? - BTV
How expensive is quantum factoring, really? - CPV
How I broke into Mexico City's justice system application and database - APV
How I defeated the Western Electric 30c - LPV
How I got COVID in a RedTeam: Social engineering and physical intrusion for realistic attack simulations. - AVV
How I use a JSON Deserialization 0day to Steal Your Money On The Blockchain - DC
How to Contact the ISS with a $30 Radio - HRV
How to Not Miss The Point: Reflections on Race, Health, and Equity - BHV
How to Weaponize RLAs to Discredit an Election - VMV
How vigilant researchers can uncover APT attacks for fun and non profit - RCV
HTTP/2: The Sequel is Always Worse - DC
Hunting Evil with Wireshark - PHV
Hunting for AWS Exposed Resources - CLV

Hybrid PhySec tools - best of both worlds or just weird? - LPV
I know who has access to my cloud, do you? - BTV
I know who has access to my cloud, do you? - CLV
I used AppSec skills to hack IoT, and so can you - IOTV
I used AppSec skills to hack IoT, and so can you - APV
ICS Cyber Threat Intelligence (CTI) Information Sharing Between Brazil and the United States - ICSV
ICS Intrusion KillChain explained with real simulation - ICSV
ICS Jeopardy - ICSV
Identifying Excel 4.0 Macro strains using Anomaly Detection - AIV
Identifying toxic combinations of permissions in your cloud infrastructure - CLV
In Space, No One Can Hear You Hack - ASV
In-person broadcast via demolabs - HTSV
Inspecting Signals from Satellites to Shock Collars - WS
Instrument and Find Out: Writing Parasitic Tracers for High(-Level) Languages - DC
Internet Protocol (IP) - PHV
Internet-of-Ingestible-Things Security by Design - BHV
Intro to high security locks and lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro To Lockpicking - LPV
Intro to ML Workshop - AIV
Intro to ML Workshop - AIV
Intro to ML Workshop - AIV
Intrusion Analysis and Threat Hunting with Suricata - PHV
IoT devices as government witnesses: Can IoT devices ever be secure if law enforcement has unlimited access to their data? - IOTV
IoT Testing Crash Course - IOTV
IoT Village Capture the Flag (CTF) - IOTV
IoT Village Capture the Flag (CTF) - IOTV
IoT Village Capture the Flag (CTF) - IOTV
IoT Village Labs - IOTV
IoT Village Labs - IOTV
IoT Village Labs - IOTV
It Takes a Village (and a generous grant): Students Performing ICS Security Assessments - ICSV
It takes a village: Why you should join the Biohacking Village - BHV
Judging by the Cover: Profiling & Targeting Through Social Media - SEV
Keeping Your Information Security Policy Up to Date - VMV
Key Duplication - It's not just for the movies! - LPV
Key Note – The Three Amigos: Money Laundering, Cryptocurrencies, and Smart Contracts - BCV
Keynote - PW Singer - ICSV
Kickoff Remarks (recorded in-person in Las Vegas) - VMV
Kubernetes Goat - Kubernetes Security Learning (Tool Demo) - CLV
Kubernetes Goat - DL
Kubernetes Security 101: Best Practices to Secure your Cluster (Workshop) - CLV
Kubestriker - DL
Law School for Lockpickers - LPV
Lawyers Meet - SOC

Learning to Hack Bluetooth Low Energy with BLE CTF - WS

LED Light Lunacy! - IOTV

Lego Spike Hub - ASV

Lego Spike Hub - ASV

Less Jaw Work, More Paw Work: Why We Need to Start “Doing” Cyber - HTSV

Let the bugs come to me - how to build cloud-based recon automation at scale - RCV

Lets Get Real About The Future State of Healthcare - BHV

Leveraging NGFWs for Threat Hunting - BTV

Leveraging SBOMs to Enhance ICS Security - ICSV

Lightning talk: Autonomous lateral movement - AVV

Lightning Talk: Differential Privacy and Census Data - CPV

Linux Binary Analysis w/ Strace - PHV

Look at me, I'm the Adversary now: Introduction to Adversary Emulation and its place in Security Operations - AVV

Lost In Space: No-one Can Hear Your Breach (Choose Wisely) - ASV

MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part 2 - BTV

MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part1 - BTV

Make Them Want To Tell You: The Science of Elicitation - SEV

Making the DEF CON 29 Badge - DC

Making the Leap - Changing Careers - CAHV

MAVSH> Attacking from Above - DC

Meetup: Certification Processes (UL, FCC, etc.) - HHV

Meetup: Legacy Hardware - HHV

Meetup: OSS ASIC - HHV

Meetup: PCB Proto and Rework - HHV

Meetup: Some HHV challenges - HHV

Meetup: Some HHV challenges - HHV

Meetup: Some HHV challenges - HHV

Meetup: Sourcing Parts & The Global Parts Shortage - HHV

Microsoft ML Security Evasion Competition Details - AIV

Mind the Gap - Managing Insecurity in Enterprise IoT - IOTV

MIPS-X - The next IoT Frontier - IOTV

MITRE Engage: A Framework for Adversary Engagement Operations - PHV

Modern Authentication for the Security Admin - BTV

Modern Malware Analysis for Threat Hunters - WS

Monero After Party - CCV

Monero Scaling Opportunities and Challenges - CCV

Mooltipass - DL

Music - Abstrct - MUS

Music - Acid T - MUS

Music - CTRL/RSM - MUS

Music - CTRL/rsm - MUS

Music - Deep Therapy - MUS

Music - DJ St3rling - MUS

Music - Dr. McGrew - MUS

Music - FuzzyNop - MUS

Music - FuzzyNop - MUS

Music - Icetre Normal - MUS

Music - Krisz Klink - MUS

Music - Magik Plan - MUS

Music - mattrix - MUS

Music - Miss Jackalope - MUS

Music - n0x08 - MUS

Music - Nina Lowe - MUS

Music - Ohm-i - MUS

Music - Scotch & Bubbles - MUS

Music - Tense Future - MUS
Music - Terrestrial Access Network - MUS
Music - Thaad - MUS
Music - Yesterday & Tomorrow - MUS
Music - Z3NPI - MUS
Music - Zebbler Encanti Experience - MUS
My other car is your car: compromising the Tesla Model X keyless entry system - CHV
National Service Panel - CAHV
Network Analysis with Wireshark - WS
Never a dill moment: Exploiting machine learning pickle files - AIV
New Face, Who Dis? Protecting Privacy in an Era of Surveillance - CPV
New Hampshire SB43 Forensic Audit - VMV
New Phishing Attacks Exploiting OAuth Authentication Flows - DC
No Aggregation Without Representation - BHV
No Key? No PIN? No Combo? No Problem! P0wning ATMs For Fun and Profit - DC
Not so Passive: Vehicle Identification and Tracking via Passive Keyless Entry - CHV
Offensive Golang Bonanza: Writing Golang Malware - DC
Old MacDonald Had a Barcode, E-I-E-I CAR - DC
Onions In the Cloud Make the CISO Proud (Workshop) - CLV
Open Bridge - DL
Open-Source Vaccine Developer Kits (VDKs) with RaDVaC - BHV
OpenSOC Blue Team CTF - CON
OpenSOC Blue Team CTF - CON
Operation Bypass: Catch My Payload If You Can - AVV
OSINT and the Hermit Kingdom. Leveraging online sources to learn more about the worlds most secret nation - RCV
OSINT for Sex Workers - RCV
OSINT Tales: What the Public Knows About Russia's New Mega-Submarine - HTSV
Over-the-air remote code execution on the DEF CON 27 badge via Near Field Magnetic Inductance or World's first NFMI exploitation, sorta or OTARCEDC27NFMIOMGWTFBBQ - DC
OWASP & CSA IoT: Impacting Medical Security - BHV
Panel discussion: Adversary simulation, emulation or purple teaming - How would you define it? - AVV
Panel discussion: Is Adversary Emulation Too ___ For You? - AVV
Panel discussion: Resilient cyber space: The role of hacker and security communities - AVV
ParseAndC - DL
Pentesting 101 - IOTV
Pentesting 101 - IOTV
People Hunting: A Pentesters Perspective - RCV
Phantom Attack: Evading System Call Monitoring - DC
Phish Like An APT - AVV
Piecing Together Your Personal Privacy Profile - CPV
PINATA: PIN Automatic Try Attack - DC
PK-WHY - CLV
Playing God: How ambiguities in state and federal breach notification laws give lawyers too much discretion in deciding whether or not to disclose potential data breaches - CPV
Playing with FHIR: hacking and securing healthcare APIs - BHV
PMapper - DL
Poking bots for fun and profit in the age of asynchronous stuff - APV
Policy Debrief - Global Cyber Capacity Building - triple challenge or triple opportunity? - DC
Policy Debrief - Myths and Legends of Section 230 - DC
Polyswarm Talk - BCV
Potential Pitfalls Protecting Patient Privacy - AIV
Preventing Sandwich Attacks on DeFi Protocols using Recurrent and Recursive Zero Knowledge Proofs - BCV
Privacy on Public Blockchains with SGX - CCV
Privacy Without Monopoly: Paternalism Works Well, But Fails Badly - DC
ProxyLogon is Just the Tip of the Iceberg, A New Attack Surface on Microsoft Exchange Server! - DC

PunkSPIDER and IOStation: Making a Mess All Over the Internet - DC
QueerCon Party - SOC
QueerCon Party - SOC
QueerCon Party - SOC
Racing cryptoexchanges or how I manipulated the balances - PYV
Racketeer Toolkit. Prototyping Controlled Ransomware Operations - DC
Ransomeware’s Big Year – from nuisance to “scourge”? - DC
Ransomware ATT&CK and Defense with the Elastic Stack - BTV
RCE via Meow Variant along with an Example 0day - PHV
Ready, fire aim: Hacking State and Federal Law Enforcement Vehicles - CHV
Recon Village Keynote - RCV
Red Alert ICS CTF - CON
Red Alert ICS CTF - CON
Red Team Village CTF - Closing Ceremony - CON
Red Team Village CTF - Finals Part 1 - CON
Red Team Village CTF - Finals Part 2 - CON
Red Team Village CTF - Qualifier Prizes and Announcements - CON
Red Team Village CTF - Qualifiers Part 1 - CON
Red Team Village CTF - Qualifiers Part 2 - CON
Red vs Blue vs Green : The ultimate battle of opinions (or is it) - BHV
Remote Adversarial Phantom Attacks against Tesla and Mobileye - CHV
Remote Ham Radio Exams - HRV
Remote Ham Radio Exams - HRV
Remotely Rooting Charging Station for fun and maybe profit - CHV
reNgine - DL
Replication as a Security Threat: How to Save Millions By Recreating Someone Else’s Model - AIV
Representation Matters - IOTV
Response Smuggling: Pwning HTTP/1.1 Connections - DC
Retired but not forgotten – A look at IFEs - ASV
Reverse Supply Chain Attack - A Dangerous Pathway To Medical Facilities’ Networks - IOTV
RF Propagation and Visualization with DragonOS - RFV
Risks of ML Systems in Health Care: The Real Story - AIV
Robo Sumo On site - HHV
Robots with lasers and cameras (but no security): Liberating your vacuum from the cloud - DC
Robustness of client-side scanning for illegal content detection on E2EE platforms - AIV
Rotten code, aging standards, & pwning IPv4 parsing across nearly every mainstream programming language - DC
RTV/AIV Red Teaming AI Roundtable - AIV
Ruse - DL
Safecracking for Everyone! - LPV
Safety Third: Defeating Chevy StabiliTrak for Track Time Fun - CHV
Scaling AppSec through Education - APV
Scaling Blockchains: A Novel Approach - BCV
Scaling static analysis for free: add additional codebases with a single line of code and no money - APV
Scaling Up Offensive Pipelines - AVV
Scope X: Hunt in the Ocean! - BTV
Scripts and Tools to Help Your ICS InfoSec Journey - ICSV
SE Team vs. Red Team - SEV
Sea Pods - HTSV
SeaTF, Pirate Hat, and Salty Sensor Results, Closing Statements - HTSV
Secrets of Social Media PsyOps - VMV
SECTF4Kids (Pre-Registration Required) - SEV
SECTF4Teens - SEV
Secure Coding Tournament CTF - CON
Secure messaging over unsecured transports - WS
Securing the Internet of Biological Things - BHV

Security Investigations with Splunk - PHV
Seeing the Forest Through the Trees – Foundations of Event Log Analysis - PHV
Seeing Through The Windows: Centralizing Windows Logs For Greater Visibility - PHV
Selling Yourself as a Security Professional - CAHV
Shell Language Processing (SLP) - AIV
Shift Left Using Cloud: Implementing baseline security into your deployment lifecycle - CLV
Shutter - DL
Siembol - DL
Signed, Sealed, Delivered: Abusing Trust in Software Supply Chain Attacks - APV
Signed, Sealed, Delivered: Comparing Chinese APTs behind Software Supply Chain Attacks - AVV
Sla(sh*t)ing happens when you stake - BCV
Sleight of ARM: Demystifying Intel Houdini - DC
Smart Meters: I'm Hacking Infrastructure and So Should You - ICSV
Sneak into buildings with KNXnet/IP - DC
So What? The CFAA after Van Buren - CPV
So You Want to OPSEC, Eh? - RCV
Social Media Security = Election Security - VMV
Solitude - DL
SPARROW: A Novel Covert Communication Scheme Exploiting Broadcast Signals in LTE, 5G & Beyond - DC
Spectrum Coordination for Amateur Radio - HRV
State of Cryptocurrency Ransomware AMA - CCV
Staying Fresh While the Feds Watch: Changes in Government Surveillance and Why it Matters - CPV
Steal This Drone: High-Assurance Cyber Military Systems - ASV
Strategic Trust and Deception in the Internet of Things - IOTV
Structured Analytical Techniques for Improving Information Security Analyses - BTV
Subtle and Not So Subtle Ways to Lose Your Cryptocurrency - BCV
Summer of Fuzz: MacOS - APV
Surviving 51% Attacks on Blockchains - BCV
Surviving DeFi: How to Prevent Economic Attacks - BCV
Table Top Exercise - Deus Ex Machina (Pre-registration Required) - BHV
Taking Apart and Taking Over ICS & SCADA Ecosystems: A Case Study of Mitsubishi Electric - DC
TEMPEST radio station - DC
The Action Plan for Cyber Diversity! - BICV
The Agricultural Data Arms Race: Exploiting a Tractor Load of Vulnerabilities In The Global Food Supply Chain - DC
The Antenny Board Design and Fabrication Saga: Sweat and Tears Along the Supply Chain - ASV
The Basics of Breaking BLE - Part 2: Doing More With Less - RFV
The Big Cleanup: Tackling The Remnants of Systematic Discrimination in the Tech Industry - BICV
The Black Box and the Brain Box: When Electronics and Deception Collide - HHV
The Black Box and the Brain Box: When Electronics and Deception Collide - HHV
The Black Box and the Brain Box: When Electronics and Deception Collide - HHV
The Bug Hunter’s Recon Methodology - RCV
The Coat Hanger Talk: A Noob's Look Into the Thieves World - LPV
The Coming AI Hackers - AIV
The Coming AI Hackers - AIV
The Curious case of knowing the unknown - APV
The Digital Physiome - How wearables can (and are) transforming healthcare - BHV
The Fault in Our Stars - Attack vectors for APIs using AWS API Gateway Lambda Authorizers - CLV
The Hangar – Cocktail Making Event - ASV
The Innocent Lives Foundation: A Beacon of Light in a Dark World - SEV
The Journey of Establishing IoT Trustworthiness and IoT Security Foundation - IOTV
The Joy of Reverse Engineering: Learning With Ghidra and WinDbg - WS
The Little Things - BHV
The Mechanics of Compromising Low Entropy RSA Keys - DC
The Neuroscience of Magic (Registration required) - RGV
The Next Critical Infrastructure: Understanding the Bioeconomy - BHV

The OPSEC of Protesting - BICV

The PACS-man Comes For Us All: We May Be Vaccinated, but Physical Access Control Still Sucks - DC

The Real History of Adversarial Machine Learning - AIV

The Real Story on Patching Medical Devices - BHV

The Security of Your Digital DNA, from Inception to Death - BHV

The State of AI Ethics - AIV

The threat hiding in daylight: Police Monitoring legislation and individual privacy in chat - CPV

The Unbelievable Insecurity of the Big Data Stack: An Offensive Approach to Analyzing Huge and Complex Big Data Infrastructures - DC

The War for Control of DNS Encryption - PHV

The Way of The Adversary - AVV

The Wild West of DeFi Exploits - BCV

This is what we thought would happen in 2021 - BTV

This Job Ad Sucks - CAHV

Threat Modeling for Space Hitchhikers - ASV

Time Turner - Hacking RF Attendance Systems (To Be in Two Places at Once) - DC

Timeless Timing Attacks - DC

Tin Foil Hat Contest - CON

Top 10 BOGUS Biometrics! - RGV

Top 20 Secure PLC Coding Practices - ICSV

Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure - ICSV

Towards Understanding the Unlimited Approval in Ethereum - BCV

Toxic BBQ - SOC

Trace Labs OSINT Search Party CTF - Award Ceremony - CON

Trace Labs OSINT Search Party CTF - Briefing - CON

Trace Labs OSINT Search Party CTF - CON

Tracee - DL

Trailblazing the AI for Cybersecurity Discipline: Overview of the Field and Promising Future Directions - AIV

Tricks for the Triage of Adversarial Software - BTV

Triptych - CCV

True Story: Hackers in the Aerospace Sector - ASV

Truth, Trust, and Biodefense - BHV

Tryptich Talk - BCV

Twitter Ethics Bug Bounty: Winners and Wrap-up - AIV

Twitter Q&A regarding Top 10 BOGUS Biometrics! - RGV

UART to UBOOT to ROOT - IOTV

UART to UBOOT to ROOT - IOTV

UFOs: Misinformation, Disinformation, and the Basic Truth - DC

Unboxing the Spacecraft Software BlackBox – Hunting for Vulnerabilities - ASV

Uncomfortable Networking - BTV

Uncovering covert network behaviors within critical infrastructure environments - BTV

Understanding common Google Cloud misconfiguration using GCP Goat - CLV

Understanding Space in the Cyber Domain - ASV

Understanding Space in the Cyber Domain - ASV

UPnProxyPot: fake the funk, become a blackhat proxy, MITM their TLS, and scrape the wire - DC

US Coast Guard 2021 Cyber Strategic Outlook - HTSV

USBSamurai - DL

Use a PortaProg to flash, dump, and test ISP and UPDI chips - HHV

Use a PortaProg to flash, dump, and test ISP and UPDI chips - HHV

Use a PortaProg to flash, dump, and test ISP and UPDI chips - HHV

Use DNS to detect your domains are abused for phishing - BTV

Using Barq to perform AWS Post-Exploitation Actions - CLV

Using OSINT to Aid in Human Trafficking and Smuggling Cases - RCV

Using Passive DNS for gathering Business Intelligence - RCV

Using SE to create insider threats and win all the things - SEV

Using UAV in Military Zone Areas by GPS Spoofing with RF Devices - RFV
Vampire the Masquerade (Party) - SOC
VDP in aviation: Experiences and lessons learnt as a researcher - ASV
Velociraptor - Dig Deeper - BTV
Venator: Hunting & Smashing Trolls on Twitter - RCV
Vetcon Meetup (Hybrid) - SOC
Voting Village Keynote Remarks - VMV
Voting Village Logistical Information Broadcast (Discord, Youtube, Twitch) - VMV
Vulnerability Exchange: One Domain Account For More Than Exchange Server RCE - DC
Vulnerability Inheritance - Attacking companies and scoring bounties through 3rd party integrations - APV
Walkthrough of DC 28 HHV Challenges - HHV
Walkthrough of DC 28 HHV Challenges - HHV
Walkthrough of DC 28 HHV Challenges - HHV
War Story Bunker - SOC
Warping Reality - creating and countering the next generation of Linux rootkits using eBPF - DC
Watch Out! And just skip the packer - BTV
Web App Penetration Testing Workshop - PHV
Welcome Note - BCV
Welcome Note - BCV
Welcome to AI Village - AIV
Welcome To DEF CON - Dark Tangent & Making the DEF CON 29 Badge - DC
Welcome to Discord - DC
Welcome to Gold Bug - CPV
Welcome. A Short Tour of Good and Bad AI in 2021 - AIV
What happens when businesses decide to enroll cryptocurrency cards - PYV
What Is Zero Knowledge - CCV
What Machine Learning Can and Can't Do for Security - BTV
When nothing goes right, push left. Designing logs for future breach investigations - APV
When Penetration Testing Isn’t Penetration Testing At All - IOTV
Where We’re Going We Don’t Need Labels: Anomaly Detection for 2FA - AIV
Who's Afraid of Thomas Bayes? - AIV
WhoC - Peeking under the hood of CaaS offerings - CLV
Whose Slide Is It Anyway - CON
Why does my security camera scream like a Banshee? Signal analysis and RE of a proprietary audio-data encoding protocol - DC
Why don’t we have IoT, daddy? - BICV
Why Hacking Voters Is Easier Than Hacking Ballots - VMV
Wibbly Wobbly, Timey Wimey – What's Really Inside Apple's U1 Chip - DC
WiFi Kraken Lite - DL
WiFi Kraken Lite - DL
WiFi Kraken Lite - DL
Will Secure Element Really Help Strengthen the Security of Cryptocurrency Wallets? - BCV
Windows Forensics 101 (Beginner) - BTV
Windows Internals - WS
Windows Internals - WS
Windows Server Containers are Broken - Here's How You Can Break Out - CLV
Wireless Odyssey or why is the federal government permitting devices with wireless networking capability in federally certified voting machines? - VMV
Wireshark for Incident Response & Threat Hunting - BTV
Workshop & CTF: Practical Cryptographic Attacks - CPV
Workshop on Microsoft Counterfit - AIV
Workshop: Practically Protecting Phone Privacy (Pre-registration required) - CPV
Worming through IDEs - DC
Wrap Up - AIV
Writing Golang Malware - WS

AIV - AI Village

Hours: Fri: 09:00 - 17:00 - Sat: 09:00 - 17:00 - Sun: 09:00 - 14:00
Home Page: https://aivillage.org/
Sched Page: https://aivillage.org/events/2020/8/4/ai-village-def-con-28-safe-mode-w6wsl
DC Discord Chan: https://discord.com/channels/708208267699945503/732733090568339536

PDT Times	Title	speaker
Friday		
09:00 - 09:30	Welcome. A Short Tour of Good and Bad AI in 2021	AI Village Organizers
09:30 - 10:59	Intro to ML Workshop	Gavin Klondike
11:00 - 11:59	The Coming AI Hackers	Bruce Schneier
12:00 - 12:30	Algorithmic Ethics Bug Bounty Contest Announcement	Rumman Chowdhury
12:30 - 12:59	Microsoft ML Security Evasion Competition Details	Hyrum Anderson
13:00 - 13:30	Shell Language Processing (SLP)	Dmitrijs Trizna
13:30 - 14:30	Trailblazing the AI for Cybersecurity Discipline: . . .	Sagar Samtani
14:30 - 14:59	AI Policy Talk: "An AI Security ISAC" and "An AI P . . .	Sagar Samtani
15:00 - 15:30	Identifying Excel 4.0 Macro strains using Anomaly . . .	Elad Ciuraru,Tal Leibovic . . .
15:30 - 16:30	Workshop on Microsoft Counterfit	Will Pearce
16:30 - 16:59	AI Discord Happy Hour - Open Discussion on AIV Dis . . .	
Saturday		
09:00 - 09:30	Welcome to AI Village	AI Village Organizers
09:30 - 10:59	Intro to ML Workshop	Gavin Klondike
11:00 - 11:59	The Coming AI Hackers	Bruce Schneier
12:00 - 12:30	Never a dill moment: Exploiting machine learning p . . .	Suha Sabi Hussain
12:30 - 12:59	Replication as a Security Threat: How to Save Mill . . .	Stella Biderman
13:00 - 13:30	Who's Afraid of Thomas Bayes?	Erick Galinkin
13:30 - 13:59	Risks of ML Systems in Health Care: The Real Story	Barton Rhodes
14:00 - 14:59	The Real History of Adversarial Machine Learning	Eugene Neelou
15:00 - 15:59	RTV/AIV Red Teaming AI Roundtable	Rich Harang,Anita Nikolic . . .
16:00 - 16:30	Where We’re Going We Don’t Need Labels: Anomal . . .	Rebecca Lynch,Stefano Mes . . .
16:30 - 16:59	AI Discord Happy Hour - Open Discussion on AIV Dis . . .	
Sunday		
09:00 - 09:30	The State of AI Ethics	Abishek Gupta
09:30 - 10:59	Intro to ML Workshop	Gavin Klondike
11:30 - 11:59	Robustness of client-side scanning for illegal con . . .	Shubham Jain
11:00 - 11:30	Potential Pitfalls Protecting Patient Privacy	Brian Martin
12:00 - 12:59	Twitter Ethics Bug Bounty: Winners and Wrap-up	Rumman Chowdhury

PDT Times	Title	speaker
13:00 - 13:59	Wrap Up	AI Village Organizers

Return to Index

APV - AppSec Village

Home Page: https://www.appsecvillage.com/
Sched Page: https://www.appsecvillage.com/events/dc-2021
DC Discord Chan: https://discord.com/channels/708208267699945503/790973922949726228

PDT Times	Title	speaker
Friday		
09:00 - 09:05	AppSec Village Welcome and Introductions	
09:05 - 09:59	Colorful AppSec	Luis Gomes,Erez Yalon,Ped . . .
10:00 - 10:45	Summer of Fuzz: MacOS	Jeremy Brown
11:00 - 11:45	Vulnerability Inheritance - Attacking companies an . . .	Gal Nagli
11:00 - 10:59	AppSec Village Capture the Flag Starts	
12:00 - 12:45	Cross-document messaging technology, how to hack i . . .	Chen Gour-Arie
13:00 - 13:45	Signed, Sealed, Delivered: Abusing Trust in Softwa . . .	Cheryl Biswas
14:00 - 14:30	Poking bots for fun and profit in the age of async . . .	Emanuel Rodrigues
15:00 - 15:45	Scaling static analysis for free: add additional c . . .	Erin Browning,Tim Faraci. . .
16:00 - 16:59	DFDs Ain't That Bad	Izar Tarandach,Matthew Co . . .
17:30 - 17:35	AppSec Quiz Time!	Eden Stroet
Saturday		
09:00 - 09:05	AppSec Village Welcome and Introductions	
09:05 - 09:59	Borrow a mentor	
09:05 - 09:59	Scaling AppSec through Education	Grant Ongers (rewtd)
10:00 - 10:45	I used AppSec skills to hack IoT, and so can you	Alexei Kojenov
11:00 - 11:45	The Curious case of knowing the unknown	Vandana Verma Sehgal
12:00 - 12:45	CSP is broken, let's fix it	Amir Shaked
12:00 - 14:30	(Workshop) - Integrating DAST tools into developer . . .	Joe Schottman
13:00 - 13:45	When nothing goes right, push left. Designing logs . . .	Vee
14:00 - 14:45	How I broke into Mexico City's justice system appl . . .	Alfonso Ruiz Cruz
15:00 - 15:45	A Deep Dive Into Supply Chain Vulnerabilities: And . . .	Adam Schaal
16:00 - 16:45	DevSecOps: Merging Security and Software Engineeri . . .	Magno Logan DELETE ME
17:00 - 17:45	Can't Stop the Code: Embrace the Code	Alton Crossley
17:45 - 17:50	AppSec Quiz Time!	Eden Stroet
Sunday		
09:00 - 09:05	AppSec Village Welcome and Introductions	
09:05 - 09:45	"The Poisoned Diary": Supply Chain Attacks on Inst . . .	Yakov Shafranovich
09:05 - 09:45	Borrow a mentor	
10:00 - 10:45	Encryption for Developers	James McKee (punkcoder)
11:00 - 11:45	AppSec 101: A Journey from Engineer to Hacker	Arjun Gopalakrishna

PDT Times	Title	speaker
12:00 - 12:45	Car Hacking + Bug Hunting Field Guide for Appsec H . . .	Jay Turla DELETE ME
13:00 - 12:59	AppSec Village Capture the Flag Ends	
13:00 - 13:45	0-Days & Nat 20's - CVSSv3 Through the Lens of Dun . . .	Alex "RedWedgeX" Hoffman
14:00 - 14:45	Attacking Modern Environments Series: Attack Vecto . . .	Mazin Ahmed
15:00 - 15:15	AppSec Quiz Time!	Eden Stroet

Return to Index

ASV - Aerospace Village

Hours: Fri: 10:00 - 16:00 - Sat: 10:00 - 16:00
Home Page: https://aerospacevillage.org/
Sched Page: https://aerospacevillage.org/events/upcoming-events/def-con-29/def-con-29-schedule/
DC Discord Chan: https://discord.com/channels/708208267699945503/732393044363444264

PDT Times	Title	speaker
Friday		
09:00 - 09:25	Retired but not forgotten – A look at IFEs	Alex Lomas,Phil Eveleigh
09:30 - 10:20	The Antenny Board Design and Fabrication Saga: Swe . . .	Ang Cui
09:00 - 17:59	A-ISAC CTF -- Pre-registration Required	
10:30 - 11:20	Hack-A-Sat 2: The Good, The Bad and the Cyber-Secu . . .	Bryce Kerley,Capt Aaron B . . .
10:00 - 11:30	AIAA CubeSat Hacking Workshop - World Premier of t . . .	
10:00 - 15:59	ARINC 429 Lab	
10:00 - 15:59	Deep Space Networking	
10:00 - 15:59	Hack-A-Sat2 Satellite Platform	
10:00 - 15:59	Antenny	
10:00 - 15:59	HACMS Live Demo	
10:00 - 15:59	Lego Spike Hub	
10:00 - 15:59	ADSB Demo and Paper Airplanes	
11:30 - 11:55	Steal This Drone: High-Assurance Cyber Military Sy . . .	Darren Cofer
11:30 - 12:59	AIAA CubeSat Hacking Workshop - Virtual Lab #1	
12:00 - 12:25	Threat Modeling for Space Hitchhikers	James Pavur
12:30 - 12:55	Evaluating Wireless Attacks on Real-World Avionics . . .	Leeloo Granger
13:00 - 13:50	Unboxing the Spacecraft Software BlackBox – Hunt . . .	Brandon Bailey
13:00 - 15:59	Understanding Space in the Cyber Domain	
14:00 - 15:59	AIAA CubeSat Hacking Workshop - Virtual Lab #2	
14:00 - 14:25	Don’t fear the BUS, it won’t run you over.	Nicholas Childs
14:30 - 14:55	CPDLC: Man-in-the-middle attacks and how to defend . . .	Joshua Smailes
15:00 - 15:25	Developing Aerospace Security Training 3D Models	Kevin Hood
15:30 - 15:55	Collecting CANs: a Bridge Less Traveled	Peace Barry
16:00 - 16:25	Holistic View of a Flight with Crowd Sourced Data	Allan Tart
Saturday		
09:30 - 10:50	VDP in aviation: Experiences and lessons learnt as . . .	Matt Gaffney
09:00 - 17:59	A-ISAC CTF -- Pre-registration Required	
09:00 - 16:59	California Cyber Innovation Challenge CTF -- Pre-r . . .	
10:00 - 15:59	Antenny	
10:00 - 15:59	ARINC 429 Lab	
10:00 - 15:59	Deep Space Networking	

PDT Times	Title	speaker
10:00 - 15:59	Hack-A-Sat2 Satellite Platform	
10:00 - 15:59	HACMS Live Demo	
10:00 - 15:59	Lego Spike Hub	
10:00 - 12:59	Understanding Space in the Cyber Domain	
10:00 - 15:59	ADSB Demo and Paper Airplanes	
11:30 - 12:59	AIAA CubeSat Hacking Workshop - Virtual Lab #3	
11:30 - 11:55	Defending the Unmanned Aerial Vehicle: Advancement . . .	Jason Whelan
11:00 - 11:59	Decoding NOAA Weather Sat Signals	
12:00 - 12:25	Federal Perspective on Aerospace Cybersecurity	Larry Grossman,Steve Lucz . . .
12:30 - 13:20	Lost In Space: No-one Can Hear Your Breach (Choose . . .	Elizabeth Wharton
12:00 - 15:59	In Space, No One Can Hear You Hack	
14:00 - 15:59	AIAA CubeSat Hacking Workshop - Virtual Lab #4	
14:30 - 14:55	True Story: Hackers in the Aerospace Sector	Declyn S.,Ginny Spicer,Ol . . .
15:00 - 15:50	Drone Security Research Series – Ep6 Hacking wit . . .	Matt Gaffney
16:00 - 16:25	Fuzzing NASA Core Flight System Software	Ronald Broberg
22:30 - 23:30	The Hangar – Cocktail Making Event	

Return to Index

AVV - Adversary Village

Hours: Fri: 11:00 - 21:00 - Sat: 10:00 - 21:00 - Sun: 10:00 - 17:00
Home Page: https://adversaryvillage.org/index.html
Sched Page: https://adversaryvillage.org/adversary-events/DEFCON-29/
DC Discord Chan: https://discord.com/channels/708208267699945503/865456992101466192

PDT Times	Title	speaker
Friday		
12:00 - 12:15	Adversary Village Kick-off	Abhijith B R
12:15 - 12:59	Adversary Village Keynote	David Kennedy
13:00 - 13:45	Look at me, I'm the Adversary now: Introduction to . . .	Samuel Kimmons
13:45 - 14:45	From On-Prem to the Cloud - Hybrid AD attack path	Sergey Chubarov
14:45 - 15:45	Exploiting Blue Team OPSEC failures with RedELK	Marc Smeets
15:45 - 16:45	Everything is a C2 if you're brave enough	Luis Ángel Ramírez Mend . . .
16:45 - 17:45	Designing a C2 Framework	Daniel "Rasta" Duggan
17:45 - 19:59	(Workshop) Tradecraft Development in Adversary Sim . . .	Fatih Ozavci
20:00 - 20:59	Panel discussion: Adversary simulation, emulation . . .	Tomer Bar,Samuel Kimmons, . . .
Saturday		
10:00 - 10:59	The Way of The Adversary	Phillip Wylie
11:00 - 13:15	(Workshop) From zero to hero: creating a reflectiv . . .	Jean Francois Maes
13:15 - 13:59	(Tool Demo) Red Team Credentials Reconnaissance (O . . .	Shantanu Khandelwal
14:00 - 14:59	Operation Bypass: Catch My Payload If You Can	Matthew Eidelberg
15:00 - 15:45	(Tool Demo) PurpleSharp: Automated Adversary Simul . . .	Mauricio Velazco
15:45 - 16:30	Phish Like An APT	Sanne Maasakkers
16:30 - 17:15	(Tool Demo) Tenacity: An Adversary Emulation Tool . . .	Atul Nair,Harshal Tupsamu . . .
17:15 - 18:15	C2Centipede: APT level C2 communications for commo . . .	Jose Garduno
18:15 - 18:45	Lightning talk: Autonomous lateral movement	Stephan Wampouille
18:45 - 19:45	Game Theory: Understanding and Strategy and Decept . . .	Juneau Jones
19:45 - 20:30	(Tool Demo) New generation of PEAS	Carlos Polop
20:30 - 21:30	Panel discussion: Is Adversary Emulation Too ___ F . . .	Jamie Williams,Cat Self,T . . .
Sunday		
10:00 - 10:59	Panel discussion: Resilient cyber space: The role . . .	Abhijith B R,Jay Turla,Ma . . .
11:00 - 11:45	(Tool Demo) Prelude Operator	David Hunt,Alex Manners
11:45 - 12:30	APT: A Short History and An Example Attack	Mark Loveless
12:30 - 13:15	(Tool Demo) ImproHound - Identify AD tiering viola . . .	Jonas Bülow Knudsen
13:15 - 14:15	Scaling Up Offensive Pipelines	Gil Biton
14:15 - 15:15	Signed, Sealed, Delivered: Comparing Chinese APTs . . .	Cheryl Biswas
15:15 - 15:59	How I got COVID in a RedTeam: Social engineering a . . .	Daniel Isler
16:00 - 16:59	Adversary Village Closing Ceremony	Adversary Village Team

Return to Index

BCV - Blockchain Village

Hours: Fri: 10:00 - 17:30 - Sat: 10:00 - 18:00 - Sun: 10:00 - 13:30
Home Page: https://www.blockchainvillage.net/
Sched Page: https://www.blockchainvillage.net/schedule-2021/
DC Discord Chan: https://discord.com/channels/708208267699945503/732733136408019084

PDT Times	Title	speaker
Thursday		
17:00 - 16:59	COSTA (Coinbase Secure Trait Analyzer)	Peter Kacherginsky
17:00 - 16:59	DeFi Must Change or Hacks Will Accelerate	Kadan Stadelmann
21:00 - 20:59	Flash Loans Demystified	Anto Joseph
21:00 - 20:59	Blockchain as a Threat Modeling Thinking Tool	Shinchul Park, Graduate S . . .
21:00 - 20:59	Subtle and Not So Subtle Ways to Lose Your Cryptoc . . .	Josh McIntyre
21:00 - 20:59	Will Secure Element Really Help Strengthen the Sec . . .	Byeongcheol Yoo
21:00 - 20:59	Scaling Blockchains: A Novel Approach	Colin Cantrell
21:00 - 20:59	Towards Understanding the Unlimited Approval in Et . . .	Dabao Wang
21:00 - 20:59	Preventing Sandwich Attacks on DeFi Protocols usin . . .	Gokul Alex
Friday		
10:00 - 10:15	Welcome Note	
10:15 - 11:30	Key Note	
11:30 - 11:59	BCOS Village Contest Overview	Reddcoin
12:00 - 12:30	Polyswarm Talk	Kevin Leffew
13:00 - 13:59	Catching (and Fixing) an Unlimited Burn Vulnerabil . . .	Nadir Akhtar
14:30 - 15:59	Workshop - Decentralized Cloud	
14:00 - 14:30	Blockchain Security Tools	Mila Paul
16:00 - 16:30	Surviving 51% Attacks on Blockchains	Yaz Khoury
16:30 - 17:30	Do You Really Own Your NFTs?	Francesco Piccoli,Steven . . .
Saturday		
10:00 - 10:15	Welcome Note	Nathan,Ron Stoner
10:15 - 11:30	Key Note – The Three Amigos: Money Laundering, C . . .	Daniel Garrie,David Cass
11:30 - 11:59	Tryptich Talk	Sarang Noether, Ph.D.
12:00 - 12:59	Ethereum Hacks & How to Stop Them	Michael Lewellen
13:00 - 13:30	Certified Ethereum Professional (CEP) Overview	Abstrct
13:30 - 13:59	Sla(sh*t)ing happens when you stake	Nadir Akhtar,Y L
14:00 - 14:59	EIP-1559 Panel	
15:00 - 15:59	Evils in the DeFi world	Minzhi He,Peiyu Wang
16:00 - 16:30	The Wild West of DeFi Exploits	Anna Szeto
Sunday		

PDT Times	Title	speaker
10:15 - 11:30	Surviving DeFi: How to Prevent Economic Attacks	Jan Gorzny
10:00 - 10:15	Welcome Note	Nathan,Ron Stoner
11:30 - 12:30	Breaking Future Crypto Custody	Mehow Powers,Chris Odom

Return to Index

BHV - Bio Hacking Village

Home Page: https://www.villageb.io/
DC Discord Chan: https://discord.com/channels/708208267699945503/735273390528528415

PDT Times	Title	speaker
Thursday		
07:00 - 06:59	Table Top Exercise - Deus Ex Machina (Pre-registra . . .	
10:00 - 13:59	Biohacking Village CTF: Hospital Under Siege (Pre- . . .	
Friday		
10:00 - 10:45	Biohacking Village Welcome Keynote	Nina Alli
10:00 - 17:59	Biohacking Village CTF: Hospital Under Siege (Pre- . . .	
11:00 - 11:45	The Digital Physiome - How wearables can (and are) . . .	Jennifer Goldsack,Jessily . . .
12:00 - 12:59	The Next Critical Infrastructure: Understanding th . . .	Charles Fracchia,Nathan C . . .
13:30 - 14:30	At least ten questions for “Bad HIPPA Takes” (. . .	Lucia Savage
13:00 - 13:30	"Who Bears the Risk?" Why a Market Incentives Pers . . .	Matt McMahon,Shannon Lant . . .
14:30 - 14:59	Open-Source Vaccine Developer Kits (VDKs) with RaD . . .	Alex Hoekstra
15:00 - 15:30	Truth, Trust, and Biodefense	Eric Perakslis
15:30 - 15:59	Healthcare Innovation With People of All Abilities	Joel Isaac,Pia Zaragoza
16:00 - 16:59	No Aggregation Without Representation	Andrea Downing
17:00 - 17:30	Lets Get Real About The Future State of Healthcare	Christian Dameff,Jeff 'R3 . . .
Saturday		
10:00 - 10:59	How to Not Miss The Point: Reflections on Race, He . . .	Nia Johnson
10:00 - 17:59	CTF: Hospital Under Siege (Pre-registration requir . . .	
11:00 - 11:59	Chinese Military Bioweapons and Intimidation Opera . . .	RedDragon
12:30 - 13:30	Cloud security for healthcare and life sciences	MIchelle Holko
13:30 - 13:59	Securing the Internet of Biological Things	Thom Dixon
14:00 - 14:59	The Real Story on Patching Medical Devices	Michael Murray
15:00 - 16:45	OWASP & CSA IoT: Impacting Medical Security	Aaron Guzman
16:45 - 16:59	A Cohort of Pirate Ships	Alex Pearlman
17:00 - 17:30	The Little Things	Mixæl Laufer
17:30 - 17:59	Playing with FHIR: hacking and securing healthcare . . .	Alissa Knight,Mitch Parke . . .
Sunday		
07:00 - 06:59	Table Top Exercise - Biologia et Machina (Pre-regi . . .	
10:30 - 10:59	Internet-of-Ingestible-Things Security by Design	Mariam Elgabry
10:00 - 10:30	Cyber Defense Matrix in Healthcare	Sounil Yu
10:00 - 12:59	CTF: Hospital Under Siege (Pre-registration requir . . .	
11:00 - 11:59	Fishing or Hunting	Ohad Zaidenberg
12:00 - 12:59	Red vs Blue vs Green : The ultimate battle of opin . . .	Ken Kato,Vee Schmitt

PDT Times	Title	speaker
13:30 - 13:59	It takes a village: Why you should join the Biohac . . .	Rob Suárez
13:00 - 13:30	The Security of Your Digital DNA, from Inception t . . .	Garrett Schumacher
14:00 - 14:30	Biohacking Village Wrap-Up	

Return to Index

BICV - Blacks in Cybersecurity

Hours: Fri: 10:00 - 17:00 - Sat: 10:00 - 17:00
Home Page: https://www.blacksincyberconf.com/
Sched Page: https://www.blacksincyberconf.com/bic-village

PDT Times	Title	speaker
Friday		
10:30 - 10:30	Why don’t we have IoT, daddy?	Jessica Hoffman
12:30 - 12:30	The Action Plan for Cyber Diversity!	Keith Chapman
14:30 - 14:30	The Big Cleanup: Tackling The Remnants of Systemat . . .	Maurice Turner
Saturday		
10:30 - 10:30	Black Cyber Exodus: The Mis-Education (Certificati . . .	Stephen Pullum
12:30 - 12:30	The OPSEC of Protesting	Ochaun Marshall
14:30 - 14:30	40 cores and a CPU	Nico "Socks" Smith
16:30 - 16:30	How Bias and Discrimination in Cybersecurity will . . .	Tennisha Martin

Return to Index

BTV - Blue Team Village

Home Page: https://blueteamvillage.org/
Sched Page: https://dc29.blueteamvillage.org/call-for-content-2021/schedule/
DC Discord Chan: https://discord.com/channels/708208267699945503/732454317658734613

PDT Times	Title	speaker
Friday		
09:30 - 10:30	Yeet the leet with Osquery (Effective Threathuntin . . .	Sebastiaan Provost
09:30 - 10:59	Attack and Detect with Prelude Operator and Securi . . .	Wes Lambert
10:45 - 11:45	Velociraptor - Dig Deeper	Mike Cohen
10:45 - 12:15	Windows Forensics 101 (Beginner)	Surya Teja Masanam
12:00 - 12:30	This is what we thought would happen in 2021	Gert-Jan Bruggink
13:30 - 13:59	Forensicating Endpoint Artifacts in the World of C . . .	Renzon Cruz
14:15 - 15:15	Adventures in Pro Bono Digital Forensics Work	John Bambenek
14:00 - 17:59	MacOs Workshop - Hunt for Red Apples: Ocean Lotus . . .	Cat Self,plug,Ben Bornhol . . .
15:30 - 16:30	Uncovering covert network behaviors within critica . . .	Michael Raggo,Chester Hos . . .
16:45 - 17:15	A SERVERLESS SIEM: DETECTING ALL BADDIES ON A BUDG . . .	Chen Cao
16:30 - 17:59	Watch Out! And just skip the packer	Felipe Duarte
17:30 - 17:59	Scope X: Hunt in the Ocean!	Meisam Eslahi
Saturday		
09:00 - 09:15	I know who has access to my cloud, do you?	Igal Flegmann
09:00 - 10:30	Wireshark for Incident Response & Threat Hunting	Michael Wylie
10:15 - 11:15	Use DNS to detect your domains are abused for phis . . .	Karl Lovink a.k.a. Cyb0rg . . .
11:30 - 11:59	What Machine Learning Can and Can't Do for Securit . . .	Wendy Edwards
11:00 - 12:30	Tricks for the Triage of Adversarial Software	Dylan Barker,Quinten Bowe . . .
11:00 - 12:30	BTV Presents: Malware Station - Maldoc Workshop	Clay (ttheveii0x)
12:15 - 12:45	How do you ALL THE CLOUDS?	henry
13:45 - 14:15	Leveraging NGFWs for Threat Hunting	Drimacus
14:30 - 15:30	Modern Authentication for the Security Admin	Bailey Bercik,Mark Morowc . . .
14:00 - 15:30	BTV Presents: Forensics Station - Workshop 1	Omenscan
14:00 - 17:59	MacOs Workshop - Hunt for Red Apples: Ocean Lotus . . .	Cat Self,plug,Ben Bornhol . . .
15:45 - 16:45	Uncomfortable Networking	Charles Rumford
16:30 - 17:59	Ransomware ATT&CK and Defense with the Elastic Sta . . .	Ben Hughes,Daniel Chen,Fr . . .
17:00 - 17:30	Structured Analytical Techniques for Improving Inf . . .	Rabbit
Sunday		
10:00 - 10:59	BTV Presents: Threat Report Roulette	Blind Hacker JoeB,Will Th . . .
11:15 - 12:15	BTV Presents: Welcome to #IRLIFE. A live IR TableT . . .	Clay (ttheveii0x),plug,Ch . . .
12:30 - 12:59	Year of Mentoring: BTV’s Meet-a-Mentor Turns One	muteki

PDT Times	Title	speaker
13:30 - 13:59	BTV Closing Ceremony	

Return to Index

CAHV - Career Hacking Village

Home Page: https://www.youtube.com/CareerHackingVillage
DC Discord Chan: https://discord.com/channels/708208267699945503/732732774347309077

PDT Times	Title	speaker
Friday		
12:00 - 12:59	F**k You, Pay Me - Knowing your worth and getting . . .	Alyssa Miller,Liana McCre . . .
12:00 - 15:59	Resume Reviewing	
12:00 - 15:59	Career Coaching	
13:00 - 13:59	Hacking Your Career: The Options	Chris Sperry,Deb Herrity, . . .
14:00 - 14:59	Making the Leap - Changing Careers	Danyelle Davis
15:00 - 15:59	This Job Ad Sucks	Kirsten Renner
Saturday		
12:00 - 12:59	National Service Panel	Amelie Koran,Elizabeth Sc . . .
12:00 - 15:59	Resume Reviewing	
12:00 - 15:59	Career Coaching	
13:00 - 13:59	Selling Yourself as a Security Professional	Preston Pierce
14:00 - 14:59	Career Hacking: Tips and Tricks to Making the Most . . .	Andy Piazza

Return to Index

CCV - Cryptocurrency Village

Home Page: https://cryptocurrencyvillage.net/
Sched Page: https://cryptocurrencyvillage.net/#schedule
DC Discord Chan: https://discord.com/channels/708208267699945503/732733510288408676

PDT Times	Title	speaker
Friday		
11:00 - 11:30	Getting Started with Decentralized Object Storage	Storj Team
12:30 - 12:59	Privacy on Public Blockchains with SGX	Secret Network Team
14:00 - 14:59	Hardware Wallet Show and Tell	Michael Schloh von Bennew . . .
16:00 - 16:30	State of Cryptocurrency Ransomware AMA	Guillermo Christensen
Saturday		
10:00 - 10:15	What Is Zero Knowledge	Sarang Noether, Ph.D.
13:00 - 13:15	Monero Scaling Opportunities and Challenges	Francisco Cabañas
15:00 - 15:15	Triptych	Sarang Noether, Ph.D.
16:30 - 16:59	Cryptocurrency Trivia!	Justin Ehrenhofer
17:00 - 17:15	Monero After Party	Monero Sound
Sunday		
11:00 - 11:59	DEX trading without leaking your identity: RAILGUN	Railgun Team

Return to Index

CHV - Car Hacking Village

Hours: Fri: 10:00 - 16:30 - Sat: 10:00 - 16:30
Home Page: https://www.carhackingvillage.com/
DC Discord Chan: https://discord.com/channels/708208267699945503/732722838942777474

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Ready, fire aim: Hacking State and Federal Law Enf . . .	Alissa Knight
11:00 - 11:59	Remotely Rooting Charging Station for fun and mayb . . .	Huajiang "Kevin2600" Chen . . .
12:00 - 12:59	Commercial Transportation: Trucking Hacking	Ben Gardiner
13:00 - 13:59	From CTF to CVE	Bill Hatzer
14:00 - 14:59	Bug Hunter's Guide to Bashing for a Car Hacking Bu . . .	Jay Turla
15:00 - 15:59	Remote Adversarial Phantom Attacks against Tesla a . . .	Ben Nassi
Saturday		
11:00 - 11:59	My other car is your car: compromising the Tesla M . . .	Lennert Wouters
12:00 - 12:59	Not so Passive: Vehicle Identification and Trackin . . .	Nick Ashworth
13:00 - 13:59	Fuzzing CAN / CAN FD ECU's and Network	Samir Bhagwat
14:00 - 14:59	Build Automotive Gateways with Ease	Don Hatfield
15:00 - 15:59	Safety Third: Defeating Chevy StabiliTrak for Trac . . .	Eric Gershman

Return to Index

CLV - Cloud Village

Hours: Fri: 10:00 - 17:00 - Sat: 10:00 - 17:00 - Sun: 10:00 - 13:20
Home Page: https://cloud-village.org/
Sched Page: https://cloud-village.org/#talks
DC Discord Chan: https://discord.com/channels/708208267699945503/732733373172285520

PDT Times	Title	speaker
Friday		
07:00 - 12:15	Cloud Village CTF - Registration	
10:00 - 10:15	Cloud Village Opening Keynote	
10:15 - 10:59	Detection Challenges in Cloud Connected Credential . . .	Rod Soto
11:00 - 12:15	Cloud Village CTF	
11:00 - 11:45	The Fault in Our Stars - Attack vectors for APIs u . . .	Alexandre Sieira,Leonardo . . .
11:45 - 12:05	Exploiting the O365 Duo 2FA Misconfiguration (Ligh . . .	Cassandra Young
12:05 - 12:50	Attacking Modern Environments Series: Attack Vecto . . .	Mazin Ahmed
12:50 - 13:20	Kubernetes Goat - Kubernetes Security Learning (To . . .	Madhu Akula
13:20 - 14:05	Hunting for AWS Exposed Resources	Felipe Pr0teus Espósito
14:05 - 14:35	WhoC - Peeking under the hood of CaaS offerings	Yuval Avrahami
14:35 - 16:59	Kubernetes Security 101: Best Practices to Secure . . .	Magno Logan
Saturday		
10:00 - 10:45	Extracting all the Azure Passwords	Karl Fosaaen
10:45 - 11:30	Windows Server Containers are Broken - Here's How . . .	Daniel Prizmant
11:30 - 12:15	AWS cloud attack vectors and security controls	Kavisha Sheth
12:15 - 12:45	Using Barq to perform AWS Post-Exploitation Action . . .	Mohammed Aldoub
12:45 - 13:30	Shift Left Using Cloud: Implementing baseline secu . . .	Avinash Jain
13:30 - 13:50	CSPM2CloudTrail - Extending CSPM Tools with (Near) . . .	Rodrigo "Sp0oKeR" Montoro
13:50 - 14:35	Azure Active Directory Hacking Wars	Batuhan Sancak
14:35 - 16:59	Onions In the Cloud Make the CISO Proud (Workshop)	Wes Lambert
Sunday		
10:00 - 10:45	Identifying toxic combinations of permissions in y . . .	Michael Raggo
10:45 - 11:15	I know who has access to my cloud, do you?	Igal Flegmann
11:15 - 11:59	Understanding common Google Cloud misconfiguration . . .	Joshua Jebaraj
12:00 - 12:20	PK-WHY	Kevin Chen
12:20 - 13:05	Cloud Security Orienteering	Rami McCarthy
13:05 - 13:20	Cloud Village Closing Keynote	

Return to Index

CON - Contests

PDT Times	Title	speaker
Thursday		
10:00 - 16:59	Tin Foil Hat Contest	
18:00 - 17:59	AutoDriving CTF	
Friday		
00:00 - 23:59	Coindroids	
06:00 - 11:59	DEF CON Bike Ride	
09:00 - 15:59	Darknet-NG	
10:00 - 19:59	DEF CON 29 CTF by OOO	
10:00 - 17:30	OpenSOC Blue Team CTF	
10:00 - 14:59	Secure Coding Tournament CTF	
10:00 - 16:59	Red Team Village CTF - Qualifiers Part 1	
10:00 - 17:59	Red Alert ICS CTF	
10:00 - 13:59	Beverage Cooling Contraption Contest	
10:00 - 23:55	Car Hacking CTF	
10:00 - 15:59	CMD+CTRL	
10:00 - 15:59	Hack3r Runw@y	
10:00 - 11:59	DEF CON Scavenger Hunt	
12:00 - 17:59	Blacks in Cybersecurity CTF	
17:00 - 19:59	EFF Tech Trivia	
20:00 - 21:59	Hacker Jeopardy	
22:00 - 23:59	Whose Slide Is It Anyway	
Saturday		
09:00 - 15:59	OpenSOC Blue Team CTF	
09:00 - 09:59	Trace Labs OSINT Search Party CTF - Briefing	
09:00 - 16:59	Darknet-NG	
10:00 - 19:59	DEF CON 29 CTF by OOO	
10:00 - 11:59	Red Team Village CTF - Qualifiers Part 2	
10:00 - 17:59	Red Alert ICS CTF	
10:00 - 15:59	Trace Labs OSINT Search Party CTF	
10:00 - 15:59	CMD+CTRL	
10:00 - 15:59	Hack3r Runw@y	
12:00 - 12:59	Red Team Village CTF - Qualifier Prizes and Announ . . .	
13:00 - 16:59	Red Team Village CTF - Finals Part 1	
17:00 - 17:59	Trace Labs OSINT Search Party CTF - Award Ceremony	
20:00 - 21:59	Hacker Jeopardy	

PDT Times	Title	speaker
20:00 - 21:59	Drunk Hacker History	
Sunday		
09:00 - 23:59	Darknet-NG	
10:00 - 13:59	DEF CON 29 CTF by OOO	
10:00 - 11:59	Red Team Village CTF - Finals Part 2	
12:00 - 12:59	Red Team Village CTF - Closing Ceremony	

Return to Index

CPV - Crypto Privacy Village

Home Page: https://cryptovillage.org/
DC Discord Chan: https://discord.com/channels/708208267699945503/732734002011832320

PDT Times	Title	speaker
Friday		
10:00 - 10:59	New Face, Who Dis? Protecting Privacy in an Era of . . .	Mike Kiser
11:00 - 11:30	Welcome to Gold Bug	
11:30 - 12:30	How expensive is quantum factoring, really?	Craig Gidney
12:30 - 13:10	CPV Through the Looking-Glass: How to Backdoor Dif . . .	
14:00 - 14:45	Playing God: How ambiguities in state and federal . . .	Anthony Hendricks,Jordan . . .
14:45 - 14:59	Lightning Talk: Differential Privacy and Census Da . . .	Wendy Edwards
15:30 - 16:30	CPV Through the Looking-Glass: Adversarial Fashion . . .	
15:00 - 15:30	So What? The CFAA after Van Buren	Kendra Albert
16:30 - 17:30	Piecing Together Your Personal Privacy Profile	Margaret Fero
Saturday		
10:00 - 11:30	CPV Through the Looking-Glass: Cryptography Codes . . .	
10:00 - 17:30	Workshop & CTF: Practical Cryptographic Attacks	Daniel Crowley
11:30 - 12:30	Breaking Historical Ciphers with Modern Algorithms	Elonka Dunin,Klaus Schmeh
12:30 - 13:15	CPV Through the Looking-Glass: Cryptanalysis in th . . .	
14:00 - 14:59	Staying Fresh While the Feds Watch: Changes in Gov . . .	Anthony Hendricks
15:00 - 15:30	CPV Through the Looking-Glass: Hacking on Multi-Pa . . .	
15:30 - 16:30	Gold Bug Q&A	
16:30 - 17:30	The threat hiding in daylight: Police Monitoring I . . .	Vic Huang,Joy Ho
Sunday		
10:00 - 10:35	CPV Through the Looking-Glass: Cicada (DC 26)	
10:35 - 13:59	CPV Through the Looking-Glass: CPV Day 3 (DC 28)	
10:00 - 13:59	Workshop: Practically Protecting Phone Privacy (Pr . . .	Mauricio Tavares,Matt Nas . . .

Return to Index

DC - DEF CON Talks

Home Page: https://defcon.org/html/defcon-29/dc-29-index.html
Sched Page: https://defcon.org/html/defcon-29/dc-29-schedule.html

PDT Times	Title	speaker
Thursday		
07:00 - 19:59	DEF CON Human Registration (Badge Pickup) Open	
09:00 - 20:59	Chillout Lounges	djdead,DJ Pie & Darren,ka . . .
Friday		
08:00 - 16:59	DEF CON Human Registration (Badge Pickup) and Vacc . . .	
09:00 - 20:59	Chillout Lounges	djdead,DJ Pie & Darren,ka . . .
09:00 - 09:59	Welcome to Discord	Dark Tangent
09:00 - 09:59	Making the DEF CON 29 Badge	Katie Whiteley,Michael Wh . . .
10:00 - 10:59	Welcome To DEF CON - Dark Tangent & Making the DEF . . .	Dark Tangent,Katie Whitel . . .
10:00 - 10:45	Gone Apple Pickin': Red Teaming macOS Environments . . .	Cedric Owens
10:00 - 10:59	HTTP/2: The Sequel is Always Worse	James Kettle
10:00 - 19:59	DEF CON Vendor Area Open	
10:00 - 10:59	Community Roundtable - (De)Criminalizing Hacking A . . .	
11:00 - 11:45	2021 - Our Journey Back To The Future Of Windows V . . .	Eran Segal,Tomer Bar
11:00 - 11:59	Caught you - reveal and exploit IPC logic bugs ins . . .	Chuanda Ding,Yuebin Sun,Z . . .
11:30 - 12:30	Community Roundtable - We can build it. We have th . . .	
11:30 - 12:30	Community Roundtable - Toward a Global IoT Code of . . .	
12:00 - 12:59	DHS REBOOTING CRITICAL INFRASTRUCTURE PROTECTION P . . .	Lily Newman,Alexander Kli . . .
12:00 - 12:20	Your House is My House: Use of Offensive Enclaves . . .	Dimitry "Op_Nomad" Snezhk . . .
12:00 - 12:20	Do you like to read? I know how to take over your . . .	Slava Makkaveev
12:30 - 12:50	The Mechanics of Compromising Low Entropy RSA Keys	Austin Allshouse
12:30 - 12:50	Worming through IDEs	David Dworken
13:00 - 13:59	Ransomeware’s Big Year – from nuisance to “s . . .	DEF CON Policy Panel
13:00 - 13:45	Sleight of ARM: Demystifying Intel Houdini	Brian Hong
13:00 - 13:59	eBPF, I thought we were friends!	Guillaume Fournier,Sylvai . . .
13:00 - 13:59	Policy Debrief - Myths and Legends of Section 230	
14:00 - 14:45	MAVSH> Attacking from Above	Sach
14:00 - 14:45	Hacking Humans with AI as a Service	Eugene Lim,Glenice Tan,Ta . . .
14:00 - 14:59	Rotten code, aging standards, & pwning IPv4 parsin . . .	Kelly Kaoudis,Sick Codes
14:30 - 15:30	Community Roundtable - Zero Trust, Critical Softwa . . .	
14:30 - 15:30	Policy Debrief - Global Cyber Capacity Building - . . .	
15:00 - 15:59	UFOs: Misinformation, Disinformation, and the Basi . . .	Richard Thieme AKA neural . . .
15:00 - 15:45	Abusing SAST tools! When scanners do more than jus . . .	Rotem Bar

PDT Times	Title	speaker
15:00 - 15:59	ProxyLogon is Just the Tip of the Iceberg, A New A . . .	Orange Tsai
15:30 - 16:30	Community Roundtable - 10 years after SOPA: where . . .	
16:00 - 16:59	Defending against nation-state (legal) attack: how . . .	Bill "Woody" Woodcock
16:00 - 16:45	Bundles of Joy: Breaking macOS via Subverted Appli . . .	Patrick Wardle
16:00 - 16:59	The Unbelievable Insecurity of the Big Data Stack: . . .	Sheila A. Berta
16:00 - 16:59	Community Roundtable - Volunteer Hacker Fire Depar . . .	
17:00 - 18:59	Do No harm; Health Panel : Live version - A DEF CO . . .	DEF CON Policy Panel
17:00 - 17:45	Phantom Attack: Evading System Call Monitoring	Junyuan Zeng,Rex Guo
17:00 - 17:59	Warping Reality - creating and countering the next . . .	PatH
18:00 - 18:45	Response Smuggling: Pwning HTTP/1.1 Connections	Martin Doyhenard
18:00 - 18:59	How I use a JSON Deserialization 0day to Steal You . . .	Hao Xing,Zekai Wu
20:00 - 21:59	DEF CON Movie Night - Tron	
Saturday		
09:00 - 16:59	DEF CON Human Registration (Badge Pickup) and Vacc . . .	
09:00 - 20:59	Chillout Lounges	djdead,DJ Pie & Darren,ka . . .
10:00 - 19:59	DEF CON Vendor Area Open	
10:00 - 10:59	Privacy Without Monopoly: Paternalism Works Well, . . .	Cory Doctorow
10:00 - 10:45	High-Stakes Updates | BIOS RCE OMG WTF BBQ	Jesse Michael,Mickey Shka . . .
10:00 - 10:45	Crossover Episode: The Real-Life Story of the Firs . . .	Chad Rikansrud (Bigendian . . .
10:00 - 10:59	Community Roundtable - Supply Chain in the COVID E . . .	
10:00 - 10:59	Community Roundtable - We need to talk about Norm . . .	
11:00 - 11:59	Wibbly Wobbly, Timey Wimey – What's Really Insid . . .	Alexander Heinrich,jiska
11:00 - 11:45	UPnProxyPot: fake the funk, become a blackhat prox . . .	Chad Seaman
11:30 - 12:30	Community Roundtable - If only you knew	
12:00 - 12:59	Bring Your Own Print Driver Vulnerability	Jacob Baines
12:00 - 12:20	Racketeer Toolkit. Prototyping Controlled Ransomwa . . .	Dimitry "Op_Nomad" Snezhk . . .
12:00 - 12:20	Time Turner - Hacking RF Attendance Systems (To Be . . .	Vivek Nair
12:30 - 12:50	Hack the hackers: Leaking data over SSL/TLS	Ionut Cernica
12:30 - 12:50	A new class of DNS vulnerabilities affecting many . . .	Ami Luttwak,Shir Tamari
13:00 - 13:59	TEMPEST radio station	Paz Hameiri
13:00 - 13:45	PINATA: PIN Automatic Try Attack	Salvador Mendoza
13:00 - 13:45	Defeating Physical Intrusion Detection Alarm Wires	Bill Graydon
13:00 - 14:59	Community Roundtable - RANSOMWARE: Combatting Rans . . .	
14:00 - 14:59	Sneak into buildings with KNXnet/IP	Claire Vacherot
14:00 - 14:45	SPARROW: A Novel Covert Communication Scheme Explo . . .	Chuck McAuley,Reza Soosah . . .
14:00 - 14:45	Over-the-air remote code execution on the DEF CON . . .	Seth Kintigh
15:00 - 15:45	Hacking G Suite: The Power of Dark Apps Script Mag . . .	Matthew Bryant
15:00 - 15:45	Central bank digital currency, threats and vulnera . . .	Ian Vitek
15:00 - 15:59	Breaking Secure Bootloaders	Christopher Wade
16:00 - 16:45	New Phishing Attacks Exploiting OAuth Authenticati . . .	Jenko Hwong
16:00 - 16:45	PunkSPIDER and IOStation: Making a Mess All Over t . . .	_hyp3ri0n aka Alejandro C . . .
16:00 - 16:59	Adventures in MitM-land: Using Machine-in-the-Midd . . .	Eyal Karni,Sagi Sheinfeld . . .
16:00 - 16:59	Community Roundtable - Thinking About Election Sec . . .	

PDT Times	Title	speaker
16:00 - 16:59	Community Roundtable - Implementing Cyber Solarium . . .	
17:00 - 17:45	You're Doing IoT RNG	Allan Cecil - dwangoAC,Da . . .
17:00 - 17:45	Hacking the Apple AirTags	Thomas Roth
17:00 - 17:59	Don't Dare to Exploit - An Attack Surface Tour of . . .	Steven Seeley,Yuhao Weng, . . .
18:00 - 18:59	HACKERS INTO THE UN? Engaging in the cyber discuss . . .	DEF CON Policy Panel
18:00 - 18:45	Offensive Golang Bonanza: Writing Golang Malware	Benjamin Kurtz
18:00 - 18:59	Vulnerability Exchange: One Domain Account For Mor . . .	Tianze Ding
19:00 - 19:59	(Replay) UFOs: Misinformation, Disinformation, and . . .	Richard Thieme AKA neural . . .
19:00 - 19:30	(Replay) Racketeer Toolkit. Prototyping Controlled . . .	Dimitry "Op_Nomad" Snezhk . . .
20:00 - 21:59	DEF CON Movie Night - Upgrade	
Sunday		
09:00 - 13:59	DEF CON Human Registration (Badge Pickup) and Vacc . . .	
09:00 - 20:59	Chillout Lounges	DJ Pie & Darren,Louigi Ve . . .
10:00 - 15:59	DEF CON Vendor Area Open	
10:00 - 10:45	A Discussion with Agent X	Agent X
10:00 - 10:59	Hi! I'm DOMAIN\Steve, please let me access VLAN2	Justin Perdok
10:00 - 10:59	Taking Apart and Taking Over ICS & SCADA Ecosystem . . .	Mars Cheng,Selmon Yang
11:00 - 11:45	The PACS-man Comes For Us All: We May Be Vaccinate . . .	Anze Jensterle,Babak Java . . .
11:00 - 11:45	Glitching RISC-V chips: MTVEC corruption for harde . . .	Adam 'pi3' Zabrocki,Alex . . .
11:00 - 11:59	Fuzzing Linux with Xen	Tamas K Lengyel
12:00 - 12:45	DoS: Denial of Shopping – Analyzing and Exploiti . . .	Joseph Gabay
12:00 - 12:45	No Key? No PIN? No Combo? No Problem! P0wning ATMs . . .	Roy Davis
12:00 - 12:59	Breaking TrustZone-M: Privilege Escalation on LPC5 . . .	Laura Abbott,Rick Altherr
13:00 - 13:45	Extension-Land: exploits and rootkits in your brow . . .	Barak Sternberg
13:00 - 13:45	Why does my security camera scream like a Banshee? . . .	Rion Carter
13:00 - 13:59	Timeless Timing Attacks	Mathy Vanhoef,Tom Van Goe . . .
14:00 - 14:45	Robots with lasers and cameras (but no security): . . .	Dennis Giese
14:00 - 14:45	Old MacDonald Had a Barcode, E-I-E-I CAR	Richard Henderson
14:00 - 14:20	Instrument and Find Out: Writing Parasitic Tracers . . .	Jeff Dileo
14:30 - 14:50	The Agricultural Data Arms Race: Exploiting a Trac . . .	Sick Codes
15:00 - 15:59	(CANCELED) Discord Closing Ceremonies	Dark Tangent
16:00 - 16:59	DEF CON Closing Ceremonies, Black Badge Ceremonies	Dark Tangent

Return to Index

DDV - Data Duplication Village

Hours: Thur: 16:00 - 19:00 - Fri: 10:00 - 17:00 - Sat: 10:00 - 17:00 - Sun: 10:00 - 11:00
Home Page: https://dcddv.org/
Sched Page: https://dcddv.org/dc29-schedule
DC Discord Chan: https://discord.com/channels/708208267699945503/732732641694056478

PDT Times	Title	speaker
Thursday		
15:00 - 18:59	Data Duplication Village - Open for dropoff only	
Friday		
10:00 - 16:59	Data Duplication Village - Open	
Saturday		
10:00 - 09:59	Data Duplication Village - Open	
Sunday		
10:00 - 10:59	Data Duplication Village - Last Chance Pickup Only	

Return to Index

DL - DEF CON DemoLabs

Home Page: https://forum.defcon.org/node/236373

PDT Times	Title	speaker
Friday		
10:00 - 11:50	AIS Tools	Gary Kessler
10:00 - 11:50	Mooltipass	Mathieu Stephan
10:00 - 11:50	WiFi Kraken Lite	Mike Spicer,Henry Hill
12:00 - 13:50	Solitude	Dan Hastings
12:00 - 13:50	Siembol	Marian Novotny
14:00 - 15:50	Kubestriker	Vasant Chinnipilli
14:00 - 15:50	Zuthaka	Lucas Bonastre
14:00 - 15:50	Open Bridge	Constantine Macris
14:00 - 15:50	Empire	Anthony "Cx01N" Rose,Vinc . . .
Saturday		
10:00 - 11:50	Kubernetes Goat	Madhu Akula
10:00 - 11:50	Ruse	Mike Kiser
10:00 - 11:50	PMapper	Erik Steringer
10:00 - 11:50	Depthcharge	Jon Szymaniak
12:00 - 13:50	Tracee	Yaniv Agman
12:00 - 13:50	USBSamurai	Luca Bongiorni
12:00 - 13:50	Git Wild Hunt	Rod Soto,José Hernandez
14:00 - 15:50	ParseAndC	Parbati Kumar Manna
14:00 - 15:50	WiFi Kraken Lite	Henry Hill
14:00 - 15:50	WiFi Kraken Lite	Henry Hill
14:00 - 15:50	Shutter	Dimitry "Op_Nomad" Snezhk . . .
Sunday		
10:00 - 11:50	reNgine	Yogesh Ojha
10:00 - 11:50	Frack	William Vermaak
12:00 - 13:50	Cotopaxi	Jakub Botwicz

Return to Index

HHV - Hardware Hacking and Soldering Skills Village

Hours: Fri: 09:30 - 18:00 - Sat: 08:30 - 16:30 - Sun: 09:00 - 15:30
Home Page: https://dchhv.org/
Sched Page: https://dchhv.org/schedule/schedule.html
DC Discord Chan: https://discord.com/channels/708208267699945503/732728536149786665

PDT Times	Title	speaker
Friday		
09:30 - 09:59	Meetup: Some HHV challenges	rehr
10:00 - 10:30	Hardware Hacking 101: Rogue Keyboards and Eavesdro . . .	Federico Lucifredi
11:00 - 11:59	Use a PortaProg to flash, dump, and test ISP and U . . .	Bradán Lane,Sara Cladlow
12:00 - 12:30	The Black Box and the Brain Box: When Electronics . . .	Gigs
12:30 - 13:30	Walkthrough of DC 28 HHV Challenges	rehr
13:30 - 14:30	A Lazy r2 Solve of @mediumrehr Challenge 6	Ben Gardiner
14:30 - 14:59	Meetup: PCB Proto and Rework	K
15:00 - 15:30	Robo Sumo On site	ShortTie
15:30 - 15:59	Meetup: Legacy Hardware	K
17:30 - 17:59	Meetup: Some HHV challenges	rehr
Saturday		
08:30 - 08:59	Hardware Hacking 101: Rogue Keyboards and Eavesdro . . .	Federico Lucifredi
09:30 - 10:30	Use a PortaProg to flash, dump, and test ISP and U . . .	Bradán Lane,Sara Cladlow
10:30 - 10:59	The Black Box and the Brain Box: When Electronics . . .	Gigs
11:00 - 11:59	Walkthrough of DC 28 HHV Challenges	rehr
12:00 - 12:59	A Lazy r2 Solve of @mediumrehr Challenge 6	Ben Gardiner
13:00 - 13:30	Meetup: Some HHV challenges	rehr
14:00 - 14:30	Meetup: Sourcing Parts & The Global Parts Shortage	bombnav
15:00 - 15:30	Meetup: OSS ASIC	Josh Marks
16:00 - 16:30	Meetup: Certification Processes (UL, FCC, etc.)	ShortTie
Sunday		
09:00 - 09:59	Walkthrough of DC 28 HHV Challenges	rehr
10:00 - 10:59	A Lazy r2 Solve of @mediumrehr Challenge 6	Ben Gardiner
11:30 - 12:30	Use a PortaProg to flash, dump, and test ISP and U . . .	Bradán Lane,Sara Cladlow
14:00 - 14:30	Hardware Hacking 101: Rogue Keyboards and Eavesdro . . .	Federico Lucifredi
15:00 - 15:30	The Black Box and the Brain Box: When Electronics . . .	Gigs

Return to Index

HRV - Ham Radio Village

Hours: Sat: 11:00 - 16:45 - Sun: 11:00 - 16:45
Home Page: https://hamvillage.org/
Sched Page: https://hamvillage.org/dc29.html
DC Discord Chan: https://discord.com/channels/708208267699945503/732733631667372103

PDT Times	Title	speaker
Friday		
09:00 - 15:59	Ham Radio Exams	
10:00 - 10:15	Ham Radio Village Opening Remarks	
11:00 - 11:30	"Ask a Ham" Q&A	
12:30 - 13:30	Spectrum Coordination for Amateur Radio	Bryan Fields
14:00 - 14:30	Discord Practice Net	
16:00 - 17:59	Remote Ham Radio Exams	
Saturday		
11:00 - 11:59	Amateur Radio Mesh Networking: Enabling Higher Dat . . .	Tyler Gardner
12:00 - 17:59	Ham Radio Exams	
13:30 - 14:30	Amateur Radio Digital Modes Primer	Jon Marler
15:00 - 15:30	How to Contact the ISS with a $30 Radio	Gregg Horton
16:00 - 16:30	Getting started with low power & long distance com . . .	Eric Escobar
17:00 - 18:59	Remote Ham Radio Exams	
Sunday		
11:00 - 13:59	Ham Radio Exams	
11:00 - 12:30	An Introduction to RF Test Equipment	Kurits Kopf
14:00 - 14:15	Ham Radio Village Closing Commentary	

Return to Index

HTSV - Hack the Sea Village

Home Page: https://hackthesea.org/
DC Discord Chan: https://discord.com/channels/708208267699945503/732733427823935589

PDT Times	Title	speaker
Friday		
10:00 - 11:50	AIS Tools Demo (DEF CON)	Gary Kessler
12:00 - 12:55	Intro to SeaTF, Salty Sensor, and Tin Foil Competi . . .	
13:00 - 13:55	AIS Protocol Internals (Abridged)	Gary Kessler
14:00 - 15:50	In-person broadcast via demolabs	Constantine Macris
Saturday		
10:00 - 10:55	OSINT Tales: What the Public Knows About Russia' . . .	H I Sutton
11:00 - 11:55	Cyber-SHIP Lab Talk and Demo	Kevin Jones,Kimberley Tam
12:00 - 14:59	Hack the Sea Cabana Party	
12:00 - 12:55	Cyber in the Under Sea	David Strachan
13:00 - 13:55	Sea Pods	Grant Romundt
14:00 - 14:55	Cyber Operations and Operational Wargames on Port . . .	Tom Mouatt,Ed McGrady,Joh . . .
15:00 - 15:55	US Coast Guard 2021 Cyber Strategic Outlook	Michael Chien
Sunday		
10:00 - 10:55	Less Jaw Work, More Paw Work: Why We Need to Start . . .	Cliff Neve
11:00 - 11:55	Hack the Wind	Mary Ann Hoppa
12:00 - 12:55	Cyber Risk Management in the MTS	Josie Long,Kelley Edwards
13:00 - 13:55	SeaTF, Pirate Hat, and Salty Sensor Results, Closi . . .	Brian Satira

Return to Index

ICSV - IndustrialControlSystems Village

Home Page: https://www.icsvillage.com/
DC Discord Chan: https://discord.com/channels/708208267699945503/735938018514567178

PDT Times	Title	speaker
Friday		
07:00 - 07:59	Tabletop Exercise - GRIMM	
10:00 - 10:59	Keynote - PW Singer	PW Singer
10:30 - 11:30	Tabletop Exercise - GRIMM	
11:30 - 12:30	Your Infrastructure is Encrypted: Protecting Criti . . .	David Etue,Ernie Bio,Jami . . .
12:30 - 12:59	Do We Really Want to Live in the Cyberpunk World?	Mert Can Kilic
13:00 - 13:59	Tabletop Exercise - GRIMM	
13:00 - 13:30	Beetlejuice: The Lessons We Should Have Learned Fo . . .	Tim Yardley
13:30 - 13:59	Scripts and Tools to Help Your ICS InfoSec Journey	Don C. Weber
14:00 - 14:59	Consider the (Data) Source	Dan Gunter
15:00 - 15:30	Approaches to Attract, Develop, and Retain an Indu . . .	John Ellis,Julia Atkinson
15:30 - 15:59	It Takes a Village (and a generous grant): Student . . .	Alexander Vigovskiy,Chris . . .
Saturday		
10:00 - 11:59	CybatiWorks Mission Station Workshop	Matthew Luallen
12:00 - 12:59	Fireside Chat - August Cole	August Cole
13:00 - 13:30	Toward a Collaborative Cyber Defense and Enhanced . . .	Lauren Zabierek
13:30 - 13:59	Fortifying ICS - Hardening and Testing	Dieter Sarrazyn
14:00 - 14:30	Crippling the Grid: Examination of Dependencies an . . .	Joe Slowik
14:30 - 14:59	Leveraging SBOMs to Enhance ICS Security	Thomas Pace
15:00 - 15:30	Smart Meters: I'm Hacking Infrastructure and So Sh . . .	Hash Salehi
Sunday		
10:00 - 10:30	Bottom-Up and Top-Down: Exploiting Vulnerabilities . . .	Sharon Brizinov,Uri Katz
10:30 - 10:59	Detecting Attackers Using Your Own Sensors with St . . .	Stefan Stephenson-Moe
11:00 - 11:59	Top 20 Secure PLC Coding Practices	Sarah Fluchs,Vivek Ponnad . . .
12:00 - 12:59	ICS Cyber Threat Intelligence (CTI) Information Sh . . .	Helio Sant'ana,John Felke . . .
13:00 - 13:30	ICS Intrusion KillChain explained with real simula . . .	Javier Perez,Juan Escobar
13:30 - 13:59	Building an ICS Firing Range (in our kitchen): Sha . . .	Moritz Thomas,Nico Leidec . . .
14:00 - 14:59	ICS Jeopardy	Chris Sistrunk,Maggie Mor . . .

Return to Index

IOTV - InternetOfThings Village

Hours: Fri: 10:00 - 21:15 - Sat: 10:00 - 21:00
Home Page: https://www.iotvillage.org/
Sched Page: https://www.iotvillage.org/defcon.html
DC Discord Chan: https://discord.com/channels/708208267699945503/732734565604655114

PDT Times	Title	speaker
Friday		
10:00 - 18:30	Pentesting 101	
10:00 - 10:30	When Penetration Testing Isn’t Penetration Testi . . .	Ted Harrington
10:45 - 11:30	Representation Matters	Camille Eddy,Chloe Messda . . .
10:00 - 18:30	UART to UBOOT to ROOT	
10:00 - 18:30	IoT Village Capture the Flag (CTF)	
10:00 - 18:30	IoT Village Labs	
10:00 - 18:30	Black Box Challenges	
11:45 - 12:30	1.21 Gigawatts! Vulnerabilities in Solar Panel Con . . .	Waylon Grange
12:45 - 13:15	LED Light Lunacy!	Victor Hanna
13:30 - 14:15	5 years of IoT vulnerability research and countles . . .	Alex "Jay" Balan
14:30 - 15:15	BLUEMONDAY Series – Exploitation & Mapping of vu . . .	Ken Pyle
15:30 - 16:15	“Alexa, have you been compromised?” — Exploi . . .	Hutch (Justin Hutchens)
16:30 - 17:15	IoT Testing Crash Course	Tim Jensen (EapolSniper)
17:30 - 18:15	Defending IoT in the Future of High-Tech Warfare	Harshit Agrawal
Saturday		
10:00 - 18:30	Pentesting 101	
10:00 - 10:45	I used AppSec skills to hack IoT, and so can you	Alexei Kojenov
10:00 - 18:30	UART to UBOOT to ROOT	
10:00 - 18:30	IoT Village Capture the Flag (CTF)	
10:00 - 18:30	IoT Village Labs	
10:00 - 18:30	Black Box Challenges	
11:00 - 11:45	You're Doing IoT RNG	Allan Cecil - dwangoAC,Da . . .
12:00 - 12:30	Strategic Trust and Deception in the Internet of T . . .	Juneau Jones
12:45 - 13:30	MIPS-X - The next IoT Frontier	Patrick Ross,Zoltán Bal. . .
13:45 - 14:30	Mind the Gap - Managing Insecurity in Enterprise I . . .	Cheryl Biswas
14:45 - 15:30	Reverse Supply Chain Attack - A Dangerous Pathway . . .	Barak Hadad,Gal Kaufman
15:45 - 16:15	Ethics at the Edge: IoT as the Embodiment of AI fo . . .	Ria Cheruvu
16:30 - 16:59	IoT devices as government witnesses: Can IoT devic . . .	Anthony Hendricks,Jordan . . .
17:15 - 17:59	The Journey of Establishing IoT Trustworthiness an . . .	Amit Elazari,Anahit Tarkh . . .
Sunday		
06:00 - 10:59	IoT Village Labs	

PDT Times	Title	speaker
10:00 - 11:59	IoT Village Capture the Flag (CTF)	

Return to Index

LBV - Lock Bypass Village

Hours: Fri: 09:00 - 19:00 - Sat: 09:00 - 19:00 - Sun: 09:00 - 17:00
Home Page: https://bypassvillage.org/
Sched Page: https://www.bypassvillage.org/#schedule
DC Discord Chan: https://discord.com/channels/708208267699945503/732732893830447175

PDT Times	Title	speaker
Friday		
09:30 - 10:30	Bypass 101	
10:30 - 11:30	Tools 101	
11:30 - 12:30	Intro to RFID Hacking	
13:30 - 14:30	Alarm Bypass	
16:00 - 17:59	Expoiting Retail Security with Tiktok's Hacker Com . . .	
Saturday		
10:00 - 10:30	Bypass 101	
11:00 - 11:59	Bypassing Retail Security Tags	
12:00 - 12:59	Tools 101 & Q&A	
13:00 - 14:30	Electronic Warfare & Q&A	
14:30 - 15:59	Alarm Bypass & Q&A	
16:30 - 16:59	Bypass 101	
Sunday		
14:00 - 14:30	Bypass 101	
14:30 - 15:59	Bypass Village Panel	

Return to Index

LPV - Lock Pick Village

Home Page: https://toool.us/
Sched Page: https://bit.ly/LPVSchedule2021
DC Discord Chan: https://discord.com/channels/708208267699945503/732734164780056708

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Intro To Lockpicking	TOOOL
11:00 - 11:50	Key Duplication - It's not just for the movies!	Tony Virelli
12:00 - 12:30	Intro To Lockpicking	TOOOL
13:00 - 13:20	Are We Still Doing it? 10 Locksport Hobbies that g . . .	Lock Noob
14:15 - 14:45	Intro To Lockpicking	TOOOL
15:00 - 15:30	Doors, Cameras, and Mantraps OH MY!	Dylan The Magician
16:15 - 16:45	Intro To Lockpicking	TOOOL
17:00 - 17:45	Law School for Lockpickers	Preston Thomas
Saturday		
10:00 - 10:30	Intro To Lockpicking	TOOOL
11:00 - 11:30	Hybrid PhySec tools - best of both worlds or just . . .	d1dymu5
12:00 - 12:30	Intro To Lockpicking	TOOOL
13:00 - 13:59	How I defeated the Western Electric 30c	N thing
14:15 - 14:45	Intro To Lockpicking	TOOOL
15:00 - 15:30	The Coat Hanger Talk: A Noob's Look Into the Thiev . . .	De
16:15 - 16:45	Intro To Lockpicking	TOOOL
Sunday		
10:00 - 10:30	Intro To Lockpicking	TOOOL
11:00 - 11:50	Safecracking for Everyone!	Jared Dygert
12:00 - 12:30	Intro To Lockpicking	TOOOL
13:00 - 13:59	Bobby Pins, More Effective Than Lockpicks?	John the Greek
14:15 - 14:45	Intro To Lockpicking	TOOOL
15:00 - 15:59	Intro to high security locks and lockpicking	N thing

Return to Index

MUS - Music

Home Page: https://defconmusic.org
Sched Page: https://defconmusic.org/sched.txt

PDT Times	Title	speaker
Thursday		
21:00 - 21:59	Music - CTRL/RSM	CTRL/rsm
21:00 - 21:59	Music - Deep Therapy	Deep Therapy
22:00 - 22:59	Music - Abstrct	Abstrct
22:00 - 22:59	Music - Tense Future	Tense Future
23:00 - 23:59	Music - Dr. McGrew	Dr. McGrew
23:00 - 23:59	Music - FuzzyNop	FuzzyNop
Friday		
00:00 - 00:59	Music - DJ St3rling	DJ St3rling
01:00 - 01:59	Music - Acid T	Acid T
21:00 - 21:59	Music - Thaad	Thaad
21:00 - 21:59	Music - Yesterday & Tomorrow	Yesterday & Tomorrow
22:00 - 22:59	Music - FuzzyNop	FuzzyNop
22:00 - 22:59	Music - Terrestrial Access Network	Terrestrial Access Networ . . .
23:00 - 23:59	Music - n0x08	n0x08
23:00 - 23:59	Music - Z3NPI	Z3NPI
Saturday		
00:00 - 00:59	Music - Scotch & Bubbles	Scotch & Bubbles
01:00 - 01:59	Music - Magik Plan	Magik Plan
21:00 - 21:59	Music - Ohm-i	Ohm-i
21:00 - 21:59	Music - mattrix	mattrix
22:00 - 22:59	Music - Krisz Klink	Krisz Klink
22:00 - 22:59	Music - Icetre Normal	Icetre Normal
23:00 - 23:59	Music - Miss Jackalope	Miss Jackalope
23:00 - 23:59	Music - Nina Lowe	Nina Lowe
Sunday		
00:00 - 00:59	Music - Zebbler Encanti Experience	Zebbler Encanti Experienc . . .
01:00 - 01:59	Music - CTRL/rsm	CTRL/rsm

Return to Index

PHV - Packet Hacking Village

Hours: Fri: 14:00 - 18:00 - Sat: 14:00 - 18:00
Home Page: https://www.wallofsheep.com/
Sched Page: https://www.wallofsheep.com/pages/dc29#talksschedule
DC Discord Chan: https://discord.com/channels/708208267699945503/708242376883306526

PDT Times	Title	speaker
Friday		
09:00 - 10:59	Web App Penetration Testing Workshop	Sunny Wear
09:00 - 09:59	The War for Control of DNS Encryption	Paul Vixie
10:00 - 10:59	Internet Protocol (IP)	Roy Feng
11:00 - 11:59	MITRE Engage: A Framework for Adversary Engagement . . .	Stan Bar,Gabby Raymond,Ma . . .
12:00 - 13:59	Hunting Evil with Wireshark	Michael Wylie
12:00 - 12:59	Seeing Through The Windows: Centralizing Windows L . . .	Matthew Gracie
Saturday		
09:00 - 10:59	APT Hunting with Splunk	John Stoner
09:00 - 09:59	Seeing the Forest Through the Trees – Foundation . . .	Jake Williams
10:00 - 10:59	*nix Processes. Starting, Stopping, and Everything . . .	Nick Roy
11:00 - 11:59	Linux Binary Analysis w/ Strace	Jared Stroud
12:00 - 13:59	Security Investigations with Splunk	Robert Wagner
12:00 - 12:59	RCE via Meow Variant along with an Example 0day	Özkan Mustafa AKKUŞ
Sunday		
09:00 - 10:59	Intrusion Analysis and Threat Hunting with Suricat . . .	Peter Manev,Josh Strosche . . .
12:00 - 13:59	Hands-On TCP Deep Dive with Wireshark	Chris Greer

Return to Index

PYV - Payment Village

Home Page: https://www.paymentvillage.org/
Sched Page: https://www.paymentvillage.org/schedule
DC Discord Chan: https://discord.com/channels/708208267699945503/732733473558626314

PDT Times	Title	speaker
Thursday		
10:00 - 10:59	Welcome to the Payment Village	
Friday		
10:00 - 10:59	ATM Transaction Reversal Frauds (And how to fight . . .	Hector Cuevas Cruz
11:00 - 11:59	Racing cryptoexchanges or how I manipulated the ba . . .	Vahagan Vardanyan
12:00 - 12:59	Automated Tear Machines	Meadow Ellis
13:00 - 13:59	What happens when businesses decide to enroll cryp . . .	Timur Yunusov

Return to Index

RCV - Recon Village

Hours: Fri: 10:00 - 16:45 - Sat: 10:00 - 16:05
Home Page: https://www.reconvillage.org/
Sched Page: https://www.reconvillage.org/recon-village-defcon-29-talks
DC Discord Chan: https://discord.com/channels/708208267699945503/732733566051418193

PDT Times	Title	speaker
Friday		
10:00 - 10:45	Recon Village Keynote	Ben S
10:55 - 11:25	Using Passive DNS for gathering Business Intellige . . .	Andy Dennis
11:35 - 12:05	So You Want to OPSEC, Eh?	Ritu Gill
12:15 - 12:59	OSINT and the Hermit Kingdom. Leveraging online so . . .	Nick Roy
14:00 - 14:30	Finding Hidden Gems via URL Shortener Services	Utku Sen
14:40 - 15:10	Using OSINT to Aid in Human Trafficking and Smuggl . . .	Rae
15:20 - 16:05	Venator: Hunting & Smashing Trolls on Twitter	Mauro Cáseres Rozanowski
16:15 - 16:45	People Hunting: A Pentesters Perspective	Mishaal Khan
Saturday		
10:00 - 10:30	Adversary Infrastructure Tracking with Mihari	Manabu Niseki
10:40 - 11:10	The Bug Hunter's Recon Methodology	Tushar Verma
11:20 - 11:50	Can I Make My Own Social Threat Score?	MasterChen
12:00 - 12:45	Let the bugs come to me - how to build cloud-based . . .	Ryan Elkins
14:00 - 14:30	How vigilant researchers can uncover APT attacks f . . .	Ladislav Baco
14:40 - 15:10	.GOV Doppelgänger: Your Häx Dollars at Work	Anthony Kava
15:20 - 16:05	OSINT for Sex Workers	Kala Kinyon

Return to Index

RFV - RF Village

Home Page: https://rfhackers.com/
Sched Page: https://rfhackers.com/calendar
DC Discord Chan: https://discord.com/channels/708208267699945503/732732595493666826

PDT Times	Title	speaker
Thursday		
12:00 - 11:59	Frag, You’re it - Hacking Laser Tag	Eric Escobar
12:00 - 11:59	ESP8266, do you know what's inside your IoT?	JoshInGeneral
12:00 - 11:59	Using UAV in Military Zone Areas by GPS Spoofing w . . .	Mehmet Onder Key
12:00 - 11:59	Assless Chaps: a novel combination of prior work t . . .	singe,cablethief
12:00 - 11:59	RF Propagation and Visualization with DragonOS	cemaxecuter
Saturday		
08:00 - 07:59	The Basics of Breaking BLE - Part 2: Doing More Wi . . .	freqy

Return to Index

RGV - Rogues Village

Hours: Fri: 10:00 - 18:00 - Sat: 10:00 - 18:00 - Sun: 10:00 - 14:00
Home Page: https://foursuits.co/roguesvillage
DC Discord Chan: https://discord.com/channels/708208267699945503/732732701144121434

PDT Times	Title	speaker
Friday		
10:00 - 10:59	Top 10 BOGUS Biometrics!	Vic Harkness
14:00 - 14:30	The Neuroscience of Magic (Registration required)	Daniel Roy
Saturday		
12:00 - 12:59	Twitter Q&A regarding Top 10 BOGUS Biometrics!	Vic Harkness

Return to Index

SEV - Social Engineering Village

Home Page: https://www.social-engineer.org/
DC Discord Chan: https://discord.com/channels/708208267699945503/732733952867172382

PDT Times	Title	speaker
Friday		
10:00 - 11:59	SECTF4Kids (Pre-Registration Required)	Ryan M,Colin H
12:30 - 13:30	Judging by the Cover: Profiling & Targeting Throug . . .	Christina Lekati
13:30 - 14:30	SE Team vs. Red Team	Ryan MacDougall
Saturday		
10:00 - 11:59	SECTF4Teens	Chris Silvers,Kris Silver . . .
12:30 - 13:30	Using SE to create insider threats and win all the . . .	Lisa Forte
13:30 - 14:30	The Innocent Lives Foundation: A Beacon of Light i . . .	John McCombs
14:30 - 15:30	Make Them Want To Tell You: The Science of Elicita . . .	Christopher Hadnagy

Return to Index

SOC - Social Activities: Parties/Meetups

PDT Times	Title	speaker
Thursday		
12:00 - 12:59	Friends of Bill W.	
13:00 - 23:59	A&E Pool Party!	
16:00 - 21:59	Toxic BBQ	
16:00 - 17:59	QueerCon Party	
17:00 - 17:59	Friends of Bill W.	
18:00 - 18:59	QueerCon Virtual Mixer	
Friday		
12:00 - 12:59	Friends of Bill W.	
13:00 - 23:59	A&E Pool Party!	
14:00 - 15:59	BADASS Meetup (Virtual)	
16:00 - 17:59	QueerCon Virtual Pool Party	
16:00 - 17:59	QueerCon Party	
17:00 - 17:59	Friends of Bill W.	
18:00 - 19:59	Lawyers Meet	
18:00 - 23:59	Hacker Karaoke (Virtual)	
20:00 - 01:59	Vampire the Masquerade (Party)	
20:00 - 21:59	War Story Bunker	
21:00 - 01:59	Gothcon 2021 (Virtual)	
Saturday		
12:00 - 12:59	Friends of Bill W.	
13:00 - 23:59	A&E Pool Party!	
16:00 - 17:59	QueerCon Party	
17:00 - 18:59	DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup	
17:00 - 17:59	Friends of Bill W.	
18:00 - 18:59	QueerCon Virtual Chat Mixer	
18:00 - 23:59	Hacker Karaoke (Virtual)	
20:00 - 22:59	Hacker Flairgrounds	
20:00 - 01:59	Gothcon 2021	
21:00 - 01:59	Vetcon Meetup (Hybrid)	
Sunday		
11:30 - 12:30	QueerCon End-of-Con Chat	
12:00 - 12:59	Friends of Bill W.	
13:00 - 23:59	A&E Pool Party!	

VMV - Voting Machine Village

Sched Page: https://docs.google.com/document/d/123a7PYCkxzR6U2eW0C_YjYNRXIXqSHBKebb4b830J1I/edit
DC Discord Chan: https://discord.com/channels/708208267699945503/732733881148506164

PDT Times	Title	speaker
Friday		
10:00 - 10:30	Voting Village Logistical Information Broadcast (D . . .	
10:30 - 10:59	Hacking to Save Democracy: What Technologists Need . . .	Eddie Perez
11:00 - 11:30	A Deep Dive on Vulnerability Disclosure for Electi . . .	Tod Beardsley
11:30 - 11:59	Wireless Odyssey or why is the federal government . . .	Susan Greenhalgh
12:00 - 12:10	A Journalist’s Perspective on Fake News	Bob Sullivan
12:30 - 12:59	Are Barcodes on Ballots Bad?	Kevin Skoglund
13:00 - 13:30	Hack the Conspiracies	Barb Byrum
13:30 - 13:59	Kickoff Remarks (recorded in-person in Las Vegas)	Harri Hursti
Saturday		
10:30 - 10:59	Secrets of Social Media PsyOps	BiaSciLab
10:00 - 10:30	Voting Village Keynote Remarks	Thomas Hicks
11:00 - 11:30	How to Weaponize RLAs to Discredit an Election	Carsten Schürmann
11:30 - 11:59	High Turnout, Wide Margins	Brianna Lennon,Eric Fey
12:00 - 12:30	Keeping Your Information Security Policy Up to Dat . . .	Sang-Oun Lee
12:30 - 12:59	Social Media Security = Election Security	Sebastian Bay
13:00 - 13:30	New Hampshire SB43 Forensic Audit	Harri Hursti
13:30 - 13:59	Why Hacking Voters Is Easier Than Hacking Ballots	Maurice Turner

Return to Index

WS - DEF CON Workshops

Home Page: https://defcon.org/html/defcon-29/dc-29-workshops.html

PDT Times	Title	speaker
Friday		
10:00 - 13:59	The Joy of Reverse Engineering: Learning With Ghid . . .	Wesley McGrew
10:00 - 13:59	Inspecting Signals from Satellites to Shock Collar . . .	Eric Escobar,Trenton Ivey
10:00 - 13:59	Analysis 101 and 102 for the Incident Responder	Kristy Westphal
10:00 - 13:59	House of Heap Exploitation	James Dolan,Maxwell Dulin . . .
15:00 - 18:59	Windows Internals	Sam Bowne,Elizabeth Biddl . . .
15:00 - 18:59	Secure messaging over unsecured transports	Ash
15:00 - 18:59	Learning to Hack Bluetooth Low Energy with BLE CTF	Ryan Holeman
15:00 - 18:59	Writing Golang Malware	Benjamin Kurtz
Saturday		
10:00 - 13:59	From Zero to Hero in Web Security Research	Dikla Barda,Oded Vanunu,R . . .
10:00 - 13:59	Bug bounty Hunting Workshop	David Patten,Philippe Del . . .
10:00 - 13:59	Hacking the Metal: An Introduction to Assembly Lan . . .	eigentourist
10:00 - 13:59	Digital Forensics and Incident Response Against th . . .	Michael Register,Michael . . .
15:00 - 18:59	Network Analysis with Wireshark	Sam Bowne,Elizabeth Biddl . . .
15:00 - 18:59	Analysis 101 and 102 for the Incident Responder	Kristy Westphal
15:00 - 18:59	Evading Detection a Beginner's Guide to Obfuscatio . . .	Anthony "Cx01N" Rose,Jake . . .
15:00 - 18:59	Advanced Wireless Attacks Against Enterprise Netwo . . .	Solstice
Sunday		
10:00 - 13:59	Windows Internals	Sam Bowne,Elizabeth Biddl . . .
10:00 - 13:59	From Zero to Hero in Web Security Research	Dikla Barda,Oded Vanunu,R . . .
10:00 - 13:59	Modern Malware Analysis for Threat Hunters	Aaron Rosenmund,Ryan Chap . . .
10:00 - 13:59	Hacking the Metal: An Introduction to Assembly Lan . . .	eigentourist

Return to Index

RCV - Saturday - 14:40-15:10 PDT

Title: .GOV Doppelgänger: Your Häx Dollars at Work
When: Saturday, Aug 7, 14:40 - 15:10 PDT
Where: Recon Village (Virtual)

SpeakerBio: Anthony Kava
No BIO available
Twitter: @anthonykava

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Friday - 11:00-11:30 PDT

Title: "Ask a Ham" Q&A
When: Friday, Aug 6, 11:00 - 11:30 PDT
Where: Ham Radio Village (Virtual Talks)

Description:

Got a question about anything ham radio? Come ask us in this open forum of all things ham radio!

All Ham Radio Village talks will be streamed to Twitch, with discussion in Discord.

For more information, see https://hamvillage.org/dc29.html

Twitch: https://www.twitch.tv/hamradiovillage

#hrv-presentation-text: https://discord.com/channels/708208267699945503/736674835413073991

Return to Index - Add to Google Calendar - ics Calendar file

APV - Sunday - 09:05-09:45 PDT

Title: "The Poisoned Diary": Supply Chain Attacks on Install scripts
When: Sunday, Aug 8, 09:05 - 09:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Yakov Shafranovich
No BIO available

Description:
The "curl | bash" pattern is in use everywhere but is it safe? How common is it and how can we make it safer? Join this talk to a discussion on install script security, Harry Potter and more!

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Friday - 13:00-13:30 PDT

Title: "Who Bears the Risk?" Why a Market Incentives Perspective is Critical to Protecting Patients from Cyber Threats
When: Friday, Aug 6, 13:00 - 13:30 PDT
Where: Biohacking Village (Talk - Virtual)
Speakers: Matt McMahon,Shannon Lantzky

SpeakerBio: Matt McMahon , Senior Product Manager - Cybersecurity at Philips
Matt is currently a Program Manager for IoMT with Booz Allen, Grad Adj Professor, teaching coursework in Cyber and Healthcare at Salve Regina University and a Cyber & IOT SME with MIT

SpeakerBio: Shannon Lantzky , Chief Scientist, Secure Connected Health, Strategic Innovation Group at Booz Allen Hamilton
Dr. Shannon Lantzy is a leader in Booz Allen's regulatory science practice, focused on efficient regulatory decisions to promote public health. Based out of our Bethesda, Maryland office, Shannon oversees innovation projects in the areas of secure connected health, medical device premarket review program assessment, digital health, simulation modeling, and decision science support services. Her team includes biologists, economists, operations researchers, engineers, chemists, epidemiologists, technologists, and data scientists.

Shannon has a background in data science, strategy, and mission integration. Prior to joining Booz Allen, she supported NASA's science and human space flight mission directorates for close to a decade. After NASA, she took a 5-year academic hiatus to conduct research in consumer decision making using econometrics, predictive modeling, and experimental methods.

Shannon has three degrees from the University of Maryland, College Park, including a Ph.D. in business information systems from the Robert H. Smith School of Business; a master's degree in information management from the College of Information Studies; and a bachelor's degree in mathematics and philosophy.

Description:

Cyberattacks in healthcare abound. Sensitive health data is stolen, and patients' lives are put at risk by the fleet of outdated, legacy medical devices in our hospitals that are vulnerable to attackers. As the market for internet of medical things (IoMT) rapidly expands, these trends will only increase. While we have the technology to fix this problem, traditional market incentives have not been able to induce a more secure healthcare environment. This talk will discuss those market failures from an economics perspective and suggest new strategies for properly incentivizing medical device manufacturers to make more cyber secure and resilient devices.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 15:00-15:59 PDT

Title: (CANCELED) Discord Closing Ceremonies
When: Sunday, Aug 8, 15:00 - 15:59 PDT
Where: See Description

SpeakerBio: Dark Tangent
No BIO available

Description:
There will be no Discord Closing Ceremony. Please view the live closing ceremony at 16:00 PDT instead.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 19:00-19:30 PDT

Title: (Replay) Racketeer Toolkit. Prototyping Controlled Ransomware Operations
When: Saturday, Aug 7, 19:00 - 19:30 PDT
Where: Track 2 CLOSED; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Dimitry "Op_Nomad" Snezhkov
Dimitry Snezhkov is an Associate Director at Protiviti. In this role he hacks code, tools, networks, apps and sometimes subverts human behavior too. Dimitry has spoken at DEF CON, BlackHat, THOTCON conferences, and presented tools at BlackHat Arsenal.
Twitter: @Op_Nomad

Description:
*** SPECIAL NOTE: Technical difficulties prevented this talk from being shown at the correct time slot on DCTV/Twitch. This entry is for the replay. You may also watch this talk on-demand, by following the links at the bottom of this message. ***

Offensive testing in organizations has shown a tremendous value for simulating controlled attacks. While cyber extortion may be one of the main high ROI end goals for the attacker, surprisingly few tools exist to simulate ransomware operations.

Racketeer is one such tool. It is an offensive agent coupled with a C2 base, built to help teams to prototype and exercise a tightly controlled ransomware campaign.

We walk through the design considerations and implementation of a ransomware implant which emulates logical steps taken to manage connectivity and asset encryption and decryption capabilities. We showcase flexible and actionable ways to prototype components of fully remote ransomware operation including key and data management, as well as data communication that is used in ransomware campaigns.

Racketeer is equipped with practical safeguards for lights out operations, and can address the goals of keeping strict control of data and key management in its deployment, including target containment policy, safe credential management, and implementing operational security in simulated operations.

Racketeer can help gain better optics into IoCs, and is helpful in providing detailed logs that can be used to study the behavior and execution artifacts of a ransomware agent.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=VJ8aqReB118

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20D

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will only be broadcast to DCTV2, in local hotels and on Twitch. This talk is not being presented in Track 2.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

Title: (Replay) UFOs: Misinformation, Disinformation, and the Basic Truth
When: Saturday, Aug 7, 19:00 - 19:59 PDT
Where: Track 1 CLOSED; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Richard Thieme AKA neuralcowboy
Richard Thieme, https://thiemeworks.com has addressed security and intelligence issues for 28 years. He has keynoted security conferences in 15 countries and given presentations for the NSA, FBI, Secret Service, Pentagon Security Forum, U.S. Department of the Treasury, and Los Alamos National Laboratory. He has been speaking at Def Con since Def Con 4. His sixth book, a novel, Mobius: A Memoir, about an intelligence professional looking back on his career and how it led down unexpected paths, is receiving rave reviews. He has explored UFO phenomena seriously for 43 years.
Twitter: @neuralcowboy

Description:

** SPECIAL NOTE: This is a replay on DCTV/Twitch only, because a technical issue prevented part of the talk from airing during its previously scheduled slot. **

The talk, "UFOs and Government: A Historical Inquiry" given at Def Con 21 has been viewed thousands of times. It was a serious well-documented exploration of the UFO subject based on Thieme's participation in research into the subject with colleagues. The book of that name is the gold standard for historical research into the subject and is in 100+ university libraries.

This update was necessitated by recent UFO incidents and the diverse conversations triggered by them. Contextual understanding is needed to evaluate current reports from pilots and naval personnel, statements from senators and Pentagon personnel, and indeed, all the input from journalists who are often unfamiliar with the field and the real history of documented UFOs over the past 70 years.

Thieme was privileged to participate with scholars and lifelong researchers into the massive trove of reports. We estimate that 95% can be explained by mundane phenomena but the remainder suggest prolonged interaction with our planetary society over a long period. Thieme also knows that when you know you don't know something, don't suggest that you do. Stay with the facts, stay with the data. Sensible conclusions, when we do that, are astonishing enough.

Reality, as Philip K. Dick said, will not go away just because we refuse to believe in it.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=mExktWB0qz4

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20R

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will only be broadcast to DCTV1, in local hotels and on Twitch. This talk is not being presented in Track 1.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Title: (Tool Demo) ImproHound - Identify AD tiering violations
When: Sunday, Aug 8, 12:30 - 13:15 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Jonas Bülow Knudsen , Security Advisor, Improsec A/S
Jonas Bülow Knudsen is an Active Directory (AD) security advisor. Jonas have spent the past two years helping organizations implement technical countermeasures and remediate vulnerabilities in and around AD, including implementation of the AD tier model. Working closely together with penetration testers and having a strong interest in offensive security enable Jonas to focus on security measures that matters and not just best practice.

Jonas has recently developed a FOSS tool called ImproHound to identify the attack paths in BloodHound breaking AD tiering: https://github.com/improsec/ImproHound.

At least _wald0 (co-creator of BloodHound) thinks it is cool: https://twitter.com/_wald0/status/1403441218495807495

Twitter: @Jonas_B_K
https://www.linkedin.com/in/jonas-bülow-knudsen-950957b7/

Description:

It is not viable for system administrators and defenders in a large Active Directory (AD) environment to ensure all AD objects have only the exact permissions they need. Microsoft also realised that, why they recommended organizations to implement the AD tier model: Split the AD into three tiers and focus on preventing attack paths leading from one tier to a more business critical tier.

The concept is great, as it in theory prevents adversaries from gaining access to the server tiers (Tier 1 and 0) when they have obtained a shell on a workstation (Tier 2) i.e. through phishing, and it prevents adversaries from gaining access to the Domain Admins, Domain Controllers, etc. in Tier 0 when they have got a shell on a web server i.e. through an RCE vulnerability. But it turns out to be rather difficult to implement the tiering concept in AD, why most organizations fail it and end up leaving security gaps.

It doesn't help on the organization's motivation to make sure their tiering is sound, when Microsoft now call it the AD tier model "legacy" and have replaced it with the more cloud-focused enterprise access model:
https://docs.microsoft.com/en-us/security/compass/privileged-access-access-model#evolution-from-the-legacy-ad-tier-model

As a person hired to help identify the vulnerabilities in an organization, you want to find and report the attack paths of their AD. BloodHound is well-known and great tool for revealing some of the hidden and often unintended relationships within an AD environment and can be used to identify highly complex chained attack paths that would otherwise be almost impossible to identify. It is great for finding the shortest attack path from a compromised user or computer to a desired target, but it is not built to find and report attack paths between tiers..

I will in my presentation explain and demonstrate a tool I have created called ImproHound, which take advantage of BloodHound's graph database to identify and report the misconfigurations and security flaws that breaks the tiering of an AD environment.

ImproHound is a FOSS tool and available on GitHub: https://github.com/improsec/ImproHound

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 19:45-20:30 PDT

Title: (Tool Demo) New generation of PEAS
When: Saturday, Aug 7, 19:45 - 20:30 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Carlos Polop , Senior Security Engineer, Mettle
Carlos is a Spanish Telecommunications Engineer with a Master in Cybersecurity.He had worked hard to pass some important certifications like OSCP, OSWE, CRTP, eMAPT, and eWPTXv2. He has worked mainly as penetration tester/red teamer but also as programmer and system administrator. Since he started learning cybersecurity he has been trying to share his knowledge and help improving the infosec world with his tools (the most remarkable ones are https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite and https://github.com/carlospolop/legion) and with his free hacking tricks online book: https://book.hacktricks.xyz
Twitter: @carlospolopm
https://es.linkedin.com/in/carlos-polop-martin

Description:

Local privilege escalation techniques are far beyond checking the Windows/Kernel version, looking for unquoted service paths or checking SUID binaries. Moreover, a local privilege escalation could make a huge difference when trying to comprise a domain. Several tools have been created to find possible privilege escalation paths, but most of the tools for Red Team and Pentesting just check for a few possible ways, so pentesters need to use several tools and do some manual recon to check for everything.

PEASS is a compilation of a bash script for Linux/MacOS/*nix and a .Net project and a batch script for Windows that I have created some time ago which aims to check and highlight every possible privescpath so professionals don't need to execute several different tools for this purpose and can very easily find vulnerabilities.

During this talk I would like to present PEASS-ng. The architecture of these scripts has evolved and improved so much that I would like to present how they work at the moment and how the difficulty to collaborate with the project has been reduced significantly. Moreover, I would also like to present the 2 new PEAS that haven't been present anywhere yet: BotPEAS and WebPEAS (the latest one will be released the day of the talk). During the talk I will also present my local privilege escalation resources (https://book.hacktricks.xyz/linux-unix/privilege-escalation , https://book.hacktricks.xyz/windows/windows-local-privilege-escalation) so the attended will be able to continue learning about the topic after the talk.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

Title: (Tool Demo) Prelude Operator
When: Sunday, Aug 8, 11:00 - 11:45 PDT
Where: Adversary Village (Virtual)
Speakers: David Hunt,Alex Manners

SpeakerBio: David Hunt , CTO, Prelude Research
David Hunt is the CTO of Prelude. David specializes in building teams which bridge cybersecurity with best-practice technology. Before coming to Prelude, David spent two years at MITRE Corporation in a dual-role as head developer and project lead for the CALDERA adversary emulation framework. David designed CALDERA v2 from the ground up and instrumented a plan which made it the industry leader in open-source breach and simulation. Prior to this work, David spent 15 years in offensive security and management roles, ranging organizations like Rockwell Collins, John Deere, Kenna Security and FireEye.

While at FireEye, David personally oversaw the storage and access of Mandiant's threat intelligence data, as the leader of the (then secretive) Nucleus team. Over the years, David has also worked as a contractor for several U.S. intelligence agencies, working domestically and internationally, as a principal security specialist.

Twitter: @privateducky
https://www.linkedin.com/in/david-hunt-b72864200

SpeakerBio: Alex Manners , Principal Cyber Security Engineer, Prelude Research
Alex Manners is a Principal Cyber Security Engineer at Prelude. Alex blends military cyber operations with a deep infrastructure and software engineering background. Prior to joining Prelude, Alex spent almost two years at The MITRE Corporation as a lead Adversary Emulation engineer and software development manager for the CALDERA adversary emulation framework. He led R&D for the CALDERA framework, designing multiple plugins and the current planning engine, as well as pushing the latest in offensive security tooling into the project. Earlier in Alex's career, he served as a Cyber Warfare Operations officer in the United State Air Force (USAF) where he led large operational support teams and integrated all aspects of offensive and defensive cyber operations into USAF Air Operations Center (AOC) operations. His cybersecurity experience spans the intelligence community, the U.S. military, non-military government, federal contracting, and the private sector.
Twitter: @khyberspache
https://linkedin.com/in/alexander-manners-87281a30

Description:
Prelude Operator is the new kid to the adversary emulation block party. Built by the same people who designed and built the MITRE Caldera framework, Operator is a free and largely open-source desktop platform that aims to make adversary emulation accessible to smaller organizations.

The app includes a library of RATs (agents) which can deploy into the field and supports a modular architecture of plugins and network protocols, including hundreds of TTPs mapped to ATT&CK. In this tool demonstration, we will highlight the key features of Operator and empower people to walk away with a developer-first adversary emulation desktop platform that is end-to-end free & open-source.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 15:00-15:45 PDT

Title: (Tool Demo) PurpleSharp: Automated Adversary Simulation
When: Saturday, Aug 7, 15:00 - 15:45 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Mauricio Velazco , Principal Threat Research Engineer, Splunk
Mauricio Velazco (@mvelazco) is a Peruvian, information security professionalwith more than a decade of work experience across different roles on both offensive and defensive security. In his current role as a Principal Threat Researcher on Splunk’s Threat Research Team, Mauricio focuses on adversary simulation and threat detection. Prior to Splunk, he led the Threat Management team at a Fortune 500 organization. Mauricio has presented/hosted workshops at conferences like Defcon, BlackHat, Derbycon, BSides, SANS, etc.
Twitter: @mvelazco
https://www.linkedin.com/in/mauricio-velazco-4314b51a/

Description:

Defending enterprise networks against attackers continues to present a difficult challenge for blue teams. Prevention has fallen short; improving detection & response capabilities has proven to be a step in the right direction. However, without the telemetry produced by adversary behavior, building new and testing existing detection capabilities will be constrained. PurpleSharp is an open source adversary simulation tool written in C# that executes adversary techniques within Windows Active Directory environments. The resulting telemetry can be leveraged to measure and improve the efficacy of a detection engineering program. PurpleSharp leverages the MITRE ATT&CK Framework and executes different techniques across the attack life cycle: execution, persistence, privilege escalation, credential access, lateral movement, etc

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 13:15-13:59 PDT

Title: (Tool Demo) Red Team Credentials Reconnaissance (OLD with a TWIST)
When: Saturday, Aug 7, 13:15 - 13:59 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Shantanu Khandelwal , Manager, KPMG Singapore
Shantanu is a Manager in the Cybersecurity Consulting practice in KPMG. He has experience in leading and performing Adversary Simulation exercises, Security Testing, and IT Security consultancy. He has worked in the Banking and Financial sectors, the Power and Utility sector, and the FMCG sector. He has led and performed various technical assessments, including Red/Purple Teaming, Security Architecture reviews, Application penetration tests, Network penetration tests, and source code reviews for many global multi-national companies. He has experience working in various world regions, including the Middle East, India, Hong Kong, and Singapore.
https://sg.linkedin.com/in/khandelwalshantanu

Description:

This talk covers the basics of credentials reconnaissance performed for a red team. Mostly covers the reconnaissance performed on GitHub to search for leaked passwords by developers. The current toolset and the Shiny new GitHub Credentials Stroller which dives into each repository and performs a deep scan.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 16:30-17:15 PDT

Title: (Tool Demo) Tenacity: An Adversary Emulation Tool for Persistence
When: Saturday, Aug 7, 16:30 - 17:15 PDT
Where: Adversary Village (Virtual)
Speakers: Atul Nair,Harshal Tupsamudre

SpeakerBio: Atul Nair , Malware Researcher, Qualys
Atul is a Malware Researcher at Qualys. His name has been listed in Google, Microsoft,Olx, Twitter Hall of fame for finding critical security vulnerabilities. Before joining Qualys he worked as a Cybersecurity consultant at Ernst & Young. Atul has extensive experience in MITRE ATT&CK framework and Adversary emulation. He is currently researching on Android adversary emulation techniques.
https://in.linkedin.com/in/atul-nair-3932a2141/

SpeakerBio: Harshal Tupsamudre , Senior Threat Research Engineer, Qualys
Harshal Tupsamudre is a senior threat researcher at Qualys. He has 8 years of research experience in the areas of cryptanalysis and usable security. He has published 15+ research articles in top-tier international conferences. He has contributed techniques, threat groups and tools to MITRE ATT&CK framework. Currently, he is researching on detection methodologies for MITRE ATT&CK techniques.
https://in.linkedin.com/in/harshal-tupsamudre-28a58735

Description:
Persistence consists of techniques that adversaries use to maintain their foothold on systems across restarts. Techniques used for persistence include any access, action, or configuration changes that allow attackers retain access on systems. Persistence is one of the more sought-after techniques of an attacker. Every 3 techniques out of top 10 usedby Adversaries belong to Persistence. We leveraged data from MITRE ATT&CK and open source cyber threat intelligence to understand how adversary achieves persistence. We created Tenacity, a light-weight adversary emulation tool that emulates over 30+ persistence techniques using 100+ procedures employed by attackers in the wild. Using this tool the organizations and individuals can quickly validate the risk posture and exposure of their business as well as the performance of the existing security solutions.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 12:00-14:30 PDT

Title: (Workshop) - Integrating DAST tools into developers' test process
When: Saturday, Aug 7, 12:00 - 14:30 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Joe Schottman
No BIO available

Description:

API testing is now vital to AppSec but presents some challenges that conventional DAST testing did not face. This session will show how running developers’ non-security tests for the APIs they develop through an interception proxy such as OWASP ZAP can enable easier, faster, and more accurate DAST testing.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 11:00-13:15 PDT

Title: (Workshop) From zero to hero: creating a reflective loader in C#
When: Saturday, Aug 7, 11:00 - 13:15 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Jean Francois Maes , Senior Red Teamer, NVISO
Jean-Franãois Maes is the technical red team lead at NVISO security and a SANS instructor for the SEC699:Adversary Emulation for Breach Prevention & Detection course. Jean-Franãois wants to help people level up in their careers and make people want to join the infosec community. This is why he's the host of the voices of infosec podcast and the creator of redteamer.tips. Both tailored to inspire people to join in on the fun. Next to his job at NVISO and SANS, he is also very engaged with the infosec community on social media and is a strong believer of open source tooling. He has authored several C# tools such as SharpNukeEventLog, SharpZipRunner and Trustjack.
Twitter: @Jean_Maes_1994

Description:

Have you ever heard of reflective loading before? Ever worked with tools like donut and sRDI? Ever wanted to execute an assembly over Cobalt-Strike but it was bigger than a megabyte? Reflection is awesome, adversaries use it frequently, and in C# it is easier than ever. In this workshop, we will explorer how to create our own reflective loader starting from scratch, adding functionality as we go, in total we will create 6 to 7 loaders. In the end, you will have a better understanding of how reflection works, what appdomains are and do, and how you can leverage reflection in red team operations. In order to attend this workshop, you will need a Windows computer (or VM) and visual studio 2019.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 17:45-19:59 PDT

Title: (Workshop) Tradecraft Development in Adversary Simulations
When: Friday, Aug 6, 17:45 - 19:59 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Fatih Ozavci , Managing Security Consultant, The Missing Link (Australia)
Fatih Ozavci is a multidisciplinary security manager, engineer and researcher with two decades of experience on offensive and defensive security technologies. He has managed several international security assessment and research projects focused on various technologies including service provider networks, unified communications, application security and embedded systems. He shared his researches, tools, advisories and vulnerabilities in major security conferences such as Black Hat USA, DEF CON and HITB. Nowadays, he combines his skillsets to perform realistic adversary simulations and defence exercises for larger organisations. Fatih is also studying Master of Cyber Security (Advanced Tradecraft) at University of New South Wales at Australian Defence Force Academy.
https://au.linkedin.com/in/fozavci

Description:

Threat actors build their tradecraft for each campaign, they need to select the right tactics, techniques. Most of the time they use open source or commercial, but publicly available tools. They even re-purpose or pack existing malware acquired from other threat actors. The reason behind of this decision is tool development takes time, and if the known/current tools already work well, they don't need upgrades either. However, the adversary simulation specialists need to operate in safer environments, therefore, they're not allowed to use malicious tradecraft or unknown tools in general. Tradecraft development is an essential skills for an adversary simulation specialist as it needs custom C2 protocols, implants, safer but realistic Mitre Att&ck TTPs, and finally cutting-edge evasions for the modern security controls including EDRs and Cyber Analytics. In this workshop, we'll walk through reasons and ways of Tradecraft development, talk about where to start, and to go, finding example source codes, walking through the source code of existing C2s, implants, and draft tools. We'll also discuss about weaponization techniques such as offensive pipelines, modern evasions techniques and tool integrations. Duringthe exercises, we'll prefer C# for programming, but you can replicate what you learn in various languages after this workshop (e.g. Python, Go, Rust). During the workshop, the participants will be able to develop their own implants, C2s, evasions and more using examples and active tools such as Petaq Purple Team C2 and Malware, TA505+ Adversary Simulation Pack and Tehsat Malware Traffic Generator

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Saturday - 10:00-10:59 PDT

Title: *nix Processes. Starting, Stopping, and Everything In Between
When: Saturday, Aug 7, 10:00 - 10:59 PDT
Where: Packet Hacking Village - Talks (Virtual)

SpeakerBio: Nick Roy
Nick Roy (Twitter: @superducktoes) currently works for a global security vendor creating training content and researching new attacker patterns and techniques. Previously he worked at an automation platform startup teaching people about the joys and benefits of automation. While not working he lives in Boston with his wife and two cats hunting out the best dive bars in Boston and solving math problems on college chalkboards overnight.
Twitter: @superducktoes

Description:

Recording discusses Linux and Unix processes, starting with a high level overview of what a process is and what the key components are. We then take a look at how the operating system manages multiple processes, what are the main components of a running process, and finally some common syscalls used in Linux when creating processes. Finally, we look at a few code samples to show how these calls are used with a simple shell. All code can be found here to compliment the video:
https://github.com/superducktoes/syscall_processes

All Packet Hacking Village talks will stream on YouTube, Twitch, Facebook, and Periscope.

YouTube: https://youtube.com/wallofsheep

Twitch: https://twitch.tv/wallofsheep

Facebook: https://www.facebook.com/wallofsheep/

Periscope: https://www.periscope.tv/wallofsheep

Return to Index - Add to Google Calendar - ics Calendar file

APV - Sunday - 13:00-13:45 PDT

Title: 0-Days & Nat 20's - CVSSv3 Through the Lens of Dungeons & Dragons
When: Sunday, Aug 8, 13:00 - 13:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Alex "RedWedgeX" Hoffman
No BIO available

Description:

What do the Critical Vulnerability Scoring System and Dungeons & Dragons have in common? As a pentester, security professional, network defender, developer, or an RPG gamer, it's vital to know how to read your character sheet in order figure out how much the BBEG (big bad evil guy) is going to mess you up and what you can do to prevent it. We'll take a brief glance at the CVSSv3 Calculator and walk through a dungeon encounter in order to better understand how to translate the ancient, often-misunderstood language of vulnerability scoring metrics.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 11:45-12:30 PDT

Title: 1.21 Gigawatts! Vulnerabilities in Solar Panel Controllers
When: Friday, Aug 6, 11:45 - 12:30 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Waylon Grange
Waylon Grange is an experienced vulnerability researcher, reverse engineer, and developer. Prior to Stage 2, he worked for Symantec and the NSA. Waylon has been a speaker at Black Hat, DefCon, RSA, CanSecWest, and DerbyCon and is credited with a US patient, multiple CVEs, and exposing APT groups. His in-depth knowledge of embedded systems is utilized to evaluate the security of IoT systems and develop electronic badges for conferences.

Description:

Embedded device security has come a long way since the days of telnet and default passwords. Product vendors are now doing more to secure their devices but how effective are they? This presentation will outline many of the software and hardware-based attacks used to compromise embedded systems. It also discusses some of the mitigations used to prevent these attacks. Many previous IoT talks show the simplicity of hacking devices that have weak security or no hardening. In contrast, this presentation shows how even secured devices have attack surfaces that still need to be addressed. It demonstrates the need for embedded devices to incorporate a security lifecycle plan and hardware designs must be audited for security weakness before production. Topics to be covered include firmware image encryption, disabling UART console access, hardening JTAG development access, securing e.MMC storage, NOR Flash protection, processor glitching, update lifecycle attacks, avoiding custom crypto, dealing with reverse engineers, and initial device setup vs authentication. None of these topics will be a deep dive. The intent is to show how they are attacked or utilized to mitigate specific attacks. To illustrate these topics the presentation will use a recent security audit of a US solar equipment manufacturer as a case study. The vendor incorporated many best practices for securing embedded devices but made some architecture decisions in the guise of security that ended up weakening their security posture rather than helping it. Finally, we'll show the ramifications of an attack against solar systems and how it could be used for racketeering. Attacks in this talk are beneficial to system designers, hobbyists, and researchers.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: 2021 - Our Journey Back To The Future Of Windows Vulnerabilities and the 0-days we brought back with us
When: Friday, Aug 6, 11:00 - 11:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded
Speakers: Eran Segal,Tomer Bar

SpeakerBio: Eran Segal
Eran Segal is a security researcher, having 7+ years experience in cyber security research. He is working on security research projects in SafeBreach Labs in the last 2 years after serving in various sec positions at the IDF.

His experience involves research on Windows and embedded devices

SpeakerBio: Tomer Bar
Tomer Bar is hands-on security researcher and head of research manager with ~20 years of unique experience in the cyber security. In the Past, he ran research groups for the Israeli government and then lead the endpoint malware research for Palo Alto Networks. Currently, he leads the SafeBreach Labs research which is the research and development arm of SafeBreach.

His main interest is focused on Windows vulnerability research, reverse engineering and APT research.

His recent discoveries are vulnerabilities in the Windows Spooler mechansim and a research on the most persistent Iranian APT campaign. He is a contributor to Mitre Attack framework and a Speaker at BlackHat, Defcon and Sector conferences.

Description:
In 2020, security researchers reported a record number of Windows vulnerabilities. We were curious what superpowers will we get from researching this huge number of vulnerabilities? Can we leverage our findings to discover 0-days?

We decided to go back in time to 2016 to search for patterns and automatically classify all the public vulnerabilities since then. We believed that only by connecting the dots to a bigger picture, we will be able to come back 2021 with the success of achieving our goal.

We adopted a new approach, in terms of both the goal and how to get there. Until now, the main goal of patch-diff was focused on the root cause of the vulnerability and building a 1-day to exploit it Usually patch-diff was done manually on a single patch.

We reached higher for the holy grail. We understood that in order to find 0-days we needed to build an automated process that would gather all the insights from all the patches in a single, searchable db.

It worked! We discovered the root causes of multiple classes of vulnerabilities. We used these discoveries on a fully patched Windows 10 host in order to highlight opportunities for exploitation. As a consequence, we found and reported (1) 6 information disclosure vulnerabilities to Microsoft, (2) 2 post exploitation techniques allowing covert exfiltration of private user data, and (3) an additional surprise.

In this presentation, we'll describe our research process, demonstrate a live exploitation of the vulnerabilities we found, share the tools we developed, and explain how other researchers can use it to discover 0-days.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=VxNi5pVDZU0

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20T

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

BICV - Saturday - 14:30-14:30 PDT

Title: 40 cores and a CPU
When: Saturday, Aug 7, 14:30 - 14:30 PDT
Where: Blacks in Cyber

SpeakerBio: Nico "Socks" Smith
Nico Smith is a technology hobbyist with over 15 years in Information Technology and 10years focused on developing defensive and offensive teams, privately and collegiately. He also is Captain in the US Army National Guard and previously a Cyber Network Defense Manager for a US Army National Guard Cyber Protection Team. In his spare time Nico Smith volunteers 30hrs a month to mentor and support college and high school students interested in entering the cyber career field. He also created the only functioning cyber challenge coin in the DOD. He also created the BIC Village Badge for DEFCON29. He has committed to improving cybersecurity and changing the way cyber is understood, leveraged, and cultivated.
Twitter: @nicolaismith1

Description:

The talk 40 Cores and a CPU will speak to the importance of participating in the cybersecurity field at every level for Black Technologists. I will demonstrate the benefits and struggles that can be both met and overcome through owning physical infrastructure and providing services to the community, with this question in mind: “If the goal is to own and secure your data, wouldn’t be easier if you owned the IP’s and the Bare Metal Infrastructure that supports it?” While the scale will always be dwarfed by larger companies that are Cloud Service Providers, the capabilities to grow and develop at a grassroots level, future engineers, and cybersecurity professionals of color is much easier, which in turn prepares better candidates for larger enterprises. This talk should start the discussion, is it possible for the black community to own spaces of the internet from the BareMetal to the code on the front-end server? And what economic impact would that have, or would it become a security issue, a new cyber target ?

Blacks in Cyber talks will be streamed on YouTube.

YouTube: https://www.youtube.com/c/BlacksInCybersecurity

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 13:30-14:15 PDT

Title: 5 years of IoT vulnerability research and countless 0days - A retrospective
When: Friday, Aug 6, 13:30 - 14:15 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Alex "Jay" Balan
Alex "Jay" Balan is the Security Research Director and Spokesperson for Bitdefender. His career is focused on Information Security and Innovation, fields in which he has so far accumulated over 20 years of experience. He is now furthering security and privacy research and has been actively involved in creating awareness by speaking at a number of conferences including DEFCON , Derbycon, RSA, BSides, ISC China, and many others

Description:
How many 0days can a research team discover in 4 years of vulnerability research in IoT? How many of them are relevant and can be used even today? How to get started (or advance further) with IoT vulnerability research? This talk will answer all these questions and show you some hands-on shell-popping and authentication bypasses as well as some new 0days published this year

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 16:45-16:59 PDT

Title: A Cohort of Pirate Ships
When: Saturday, Aug 7, 16:45 - 16:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Alex Pearlman , Science and Health Policy + Emerging Issues in Bioethics
No BIO available

Description:

A presentation on our newly published research on ethics attitudes and preferences in biomedical citizen science, biohacker, and community bio groups. As biomedical citizen science initiatives become more prevalent, the unique ethical issues that they raise are attracting policy attention. One issue identified as a significant concern is the ethical oversight of bottom-up biomedical citizen science projects that are designed and executed primarily or solely by members of the public. That is because the federal rules that require ethical oversight of research by institutional review boards generally do not apply to such projects, creating what has been called an ethics gap. Working to close this gap, practitioners and scholars have considered new mechanisms of ethical oversight for biomedical citizen science. To date, however, participants' attitudes about ethics and oversight preferences have not been systematically examined. This information is useful to efforts to develop ethical oversight mechanisms because it provides a basis for evaluating the likely effectiveness of specific features of such mechanisms and their acceptability from the perspective of biomedical citizen scientists. Here, we report data from qualitative interviews with 35 stakeholders (some from BHV!) in bottom-up biomedical citizen science about their general ethics attitudes and preferences regarding ethical oversight. Interviewees described ten ethical priorities and endorsed oversight mechanisms that are voluntary, community-driven, and offer guidance. Conversely, interviewees rejected mechanisms that are mandatory, hierarchical, and inflexible. Applying these findings, we conclude that expert consultation and community review models appear to align well with ethical priorities and oversight preferences of many biomedical citizen scientists, although local conditions should guide the development and use of mechanisms in specific communities.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 15:00-15:45 PDT

Title: A Deep Dive Into Supply Chain Vulnerabilities: And How SecDevOps Can Save the Day
When: Saturday, Aug 7, 15:00 - 15:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Adam Schaal
No BIO available

Description:

These are dangerous times. From left-pad to event-stream to the Node Security Platform shutdown - nowhere are supply chain vulnerabilities more prevalent than modern-day javascript applications. Join us as we discuss how investing in the DevOps cycle now can help save your assets in the long run.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Friday - 11:00-11:30 PDT

Title: A Deep Dive on Vulnerability Disclosure for Election Systems
When: Friday, Aug 6, 11:00 - 11:30 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Tod Beardsley
Tod Beardsley is the Director of Research at Rapid7. He has over 30 years of hands-on security experience, stretching from in-band telephony switching to modern IoT implementations. He has held IT Ops and Security positions in large organizations such as 3Com, Dell, and Westinghouse, as both an offensive and defensive practitioner. Today, Tod directs the security research program at Rapid7, is a zealous advocate for coordinated vulnerability disclosure, is a CVE Board member, is a contributing author to a number of research papers produced by Rapid7, and is often a Travis County Election Judge in Texas. Because of this last qualifier, it is permissible to address him as “Your Honor.”

Description:

The norms and practices of vulnerability disclosure among voting machine manufacturers and election infrastructure providers have radically changed since the first Voting Machine Hacking Village of DEFCON 25. In just a few short years, private companies in the election services sector have matured from recalcitrant, close-lipped antagonists to active and willing participants in coordinated vulnerability disclosure (CVD) with published vulnerability disclosure programs (VDPs). And yet, truly unbelievable claims about voting security have risen to the fore, and as a result, the public imagination around how cybersecurity works and what are realistic threats to election integrity seems more fanciful than ever. In this short presentation, we will explore how CVD works for voting machines and other election systems, provide guidance on how well-meaning, virtuous hackers can best interface with this niche but crucial industry, and how we can all do our part to bring some reason and rigor to the practice of information security when it comes to one of our most important institutions.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 10:00-10:45 PDT

Title: A Discussion with Agent X
When: Sunday, Aug 8, 10:00 - 10:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Agent X
No BIO available

Description:
This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=U2-8MNx8nsg

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20A

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Friday - 12:00-12:10 PDT

Title: A Journalist’s Perspective on Fake News
When: Friday, Aug 6, 12:00 - 12:10 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Bob Sullivan
Bob Sullivan is a veteran journalist and the author of five books, including New York Times Best-Sellers, Gotcha Capitalism and Stop Getting Ripped Off! He has won the Society of Professional Journalists Public Service Award, a Peabody award, a Carnegie Mellon University CyLab Cybersecurity Journalism Award, and the Consumer Federation of America Betty Furness Consumer Media Service Award. He spent nearly two decades working at MSNBC.com and NBC News, and he still appears on TODAY, NBC Nightly News, and CNBC. He’s now a syndicated columnist and frequent TV guest. He is also host of AARP’s The Perfect Scam podcast, co-host of the podcast / audio documentary “Breach“, which examines history’s biggest hacking stories, and co-host of the podcast “So, Bob,” which tackles stories about the unintended consequences of technology. His latest podcast is called Debugger, exploring issues at the intersection of technology and democracy, produced in cooperation with Duke University’s Sanford School of Public Policy and the Kenan Institute for Ethics.

He holds a master’s degree in journalism from the University of Missouri and degrees in history and mathematics from Fairfield University. He is on the advisory board of the University of Georgia journalism school’s Cox Institute for Media Innovation and is a mentor/editor at the Op-Ed Project.

Description:
Why pseudo-events led to fake news.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 13:30-14:30 PDT

Title: A Lazy r2 Solve of @mediumrehr Challenge 6

When: Friday, Aug 6, 13:30 - 14:30 PDT

Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Ben Gardiner

Mr. Gardiner is an independent consultant at Yellow Flag Security, Inc. presently working to secure heavy vehicles at the NMFTA. With more than ten years of professional experience in embedded systems design and a lifetime of hacking experience, Gardiner has a deep knowledge of the low-level functions of operating systems and the hardware with which they interface. Prior YFS Inc. and joining the NMFTA team in 2019, Mr. Gardiner held security assurance and reversing roles at a global corporation, as well as worked in embedded software and systems engineering roles at several organizations. He holds a M.Sc. Eng. in Applied Math & Stats from Queen's University. He is a DEF CON Hardware Hacking Village (DC HHV) and Car Hacking Village (CHV) volunteer.
Twitter: @BenLGardiner

Description:

Join Ben for an informal let's play of @mediumrehr's Hardware Hacking Village challenge 6. Some topics we will cover include: radare2 , AVR assembly, 7 segment displays, and sigrok. It should be fun and relaxed with plenty of time to stop and re-do some steps if something needs more deliberation. See you there.

#hhv-challenge-text https://discord.com/channels/708208267699945503/739567199647301702

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 12:00-12:59 PDT

Title: A Lazy r2 Solve of @mediumrehr Challenge 6
When: Saturday, Aug 7, 12:00 - 12:59 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Ben Gardiner
Mr. Gardiner is an independent consultant at Yellow Flag Security, Inc. presently working to secure heavy vehicles at the NMFTA. With more than ten years of professional experience in embedded systems design and a lifetime of hacking experience, Gardiner has a deep knowledge of the low-level functions of operating systems and the hardware with which they interface. Prior YFS Inc. and joining the NMFTA team in 2019, Mr. Gardiner held security assurance and reversing roles at a global corporation, as well as worked in embedded software and systems engineering roles at several organizations. He holds a M.Sc. Eng. in Applied Math & Stats from Queen's University. He is a DEF CON Hardware Hacking Village (DC HHV) and Car Hacking Village (CHV) volunteer.
Twitter: @BenLGardiner

Description:
Join Ben for an informal let's play of @mediumrehr's Hardware Hacking Village challenge 6. Some topics we will cover include: radare2 , AVR assembly, 7 segment displays, and sigrok. It should be fun and relaxed with plenty of time to stop and re-do some steps if something needs more deliberation. See you there.

#hhv-challenge-text https://discord.com/channels/708208267699945503/739567199647301702

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Sunday - 10:00-10:59 PDT

Title: A Lazy r2 Solve of @mediumrehr Challenge 6
When: Sunday, Aug 8, 10:00 - 10:59 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Ben Gardiner
Mr. Gardiner is an independent consultant at Yellow Flag Security, Inc. presently working to secure heavy vehicles at the NMFTA. With more than ten years of professional experience in embedded systems design and a lifetime of hacking experience, Gardiner has a deep knowledge of the low-level functions of operating systems and the hardware with which they interface. Prior YFS Inc. and joining the NMFTA team in 2019, Mr. Gardiner held security assurance and reversing roles at a global corporation, as well as worked in embedded software and systems engineering roles at several organizations. He holds a M.Sc. Eng. in Applied Math & Stats from Queen's University. He is a DEF CON Hardware Hacking Village (DC HHV) and Car Hacking Village (CHV) volunteer.
Twitter: @BenLGardiner

Description:

Join Ben for an informal let's play of @mediumrehr's Hardware Hacking Village challenge 6. Some topics we will cover include: radare2 , AVR assembly, 7 segment displays, and sigrok. It should be fun and relaxed with plenty of time to stop and re-do some steps if something needs more deliberation. See you there.

#hhv-challenge-text https://discord.com/channels/708208267699945503/739567199647301702

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 12:30-12:50 PDT

Title: A new class of DNS vulnerabilities affecting many DNS-as-Service platforms
When: Saturday, Aug 7, 12:30 - 12:50 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded
Speakers: Ami Luttwak,Shir Tamari

SpeakerBio: Ami Luttwak
Ami Luttwak is a serial entrepreneur, an experienced cyber security CTO and a hacker by heart. Mainly interested in cloud security and cloud exploits, understanding how the cloud is built to uncover its weaknesses. Currently CTO of Wiz, the fastest growing unicorn in cloud security, prior to that led research as CTO of Microsoft cloud security and prior to that founded Adallom, a pioneering cloud security startup acquired by Microsoft in 2015.
Twitter: @amiluttwak

SpeakerBio: Shir Tamari
Shir Tamari is a security and technology researcher, specializing in vulnerability research and practical hacking. Works as Head of Research at the cloud security company Wiz. In the past, he served in the Israeli intelligence unit, and in recent years has led a variety of research and security products in the industry. Shir's interests include Android, Linux Kernel, Web hacking and Blockchain.
Twitter: @shirtamari

Description:

We present a novel class of DNS vulnerabilities that affects multiple DNS-as-a-Service (DNSaaS) providers. The vulnerabilities have been proven and successfully exploited on three major cloud providers including AWS Route 53 and may affect many others. Successful exploitation of the vulnerabilities may allow exfiltration of sensitive information from service customers' corporate networks. The leaked information contains internal and external IP addresses, computer names, and sometimes NTLM hashes. The number of organizations vulnerable to this weakness is shocking. Over a few hours of DNS sniffing, we received sensitive information carried by DNS update queries from ~1M Windows endpoints from around 15,000 potentially vulnerable companies, including 15 Fortune 500 companies. In some organizations, there were more than 20,000 endpoints that actively leaked their information out of the organization. We will review possible mitigations to this problem and solutions for both DNSaaS providers and managed networks.

REFERENCES

I. Microsoft Windows DNS Update algorithm explained - https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/configure-dns-dynamic-updates-windows-serve

II. An excellent blog post by Matthew Bryant on hijacking DNS Updates abusing a dangling domain issue on Guatemala State's Top Level Domain - https://thehackerblog.com/hacking-guatemalas-dns-spying-on-active-directory-users-by-exploiting-a-tld-misconfiguration/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=72uzIZPyVjI

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20S

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Friday - 16:45-17:15 PDT

Title: A SERVERLESS SIEM: DETECTING ALL BADDIES ON A BUDGET
When: Friday, Aug 6, 16:45 - 17:15 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Chen Cao
A security engineer at Cloudflare focuses on Detection and Response. Chen holds a Master of Science degree in Security Informatics from Johns Hopkins University and has been in the security industry for about 4 years now. He enjoys sharing & learning good practices in the industry and currently working on finding a reliable, scalable and cheap way for log collection and alerting.
Twitter: @chencao_cc

Description:

Commercial SIEMs are expensive, inflexible and risk a vendor lock-in. At Cloudflare, we built a SIEM using a Serverless architecture that provides scalability and flexibility to perform various Detection and Response functions. We will discuss this architecture and how it can be built upon to solve many Security problems, in a true pay-as-you-use model after 2 years of use handling Cloudflare’s data.

A SIEM is pivotal to a Threat Detection and Incident Response function. But, commercial SIEMs are expensive both in terms of cost of usage and maintenance, and risk a vendor lock-in. At Cloudflare, we build a SIEM to manage logs from 200+ data centers, 2000s endpoints and our corporate networks. The SIEM is built using a Serverless architecture in GCP that scales up and down based on usage, for a true pay-as-you-go model. It provides multiple data processing and analyzing paradigms that enable various D&R workflows. In this talk, we will discuss the motivation, constraints and the SIEM architecture. We’ll also dive into our logging pipeline, detection, automation and notification workflows using this SIEM.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 09:00-17:59 PDT

Title: A-ISAC CTF -- Pre-registration Required
When: Friday, Aug 6, 09:00 - 17:59 PDT
Where: Aerospace Village (Virtual CTF)

Description:
A-ISAC, ERAU with support from IntelliGenesis (CybatiWorks)

Day 1: Aug. 6th, 2021 9:00AM – 6:00PM PDT (UTC-7) Day 2: Aug. 7th, 2021 9:00AM – 6:00PM PDT (UTC-7)

Registration available at https://aisac.cyberskyline.com/defcon

Aviation ISAC is hosting a competition at DC29 Aerospace Village! This competition represents a simulated airport hosted on the Cyber Skyline platform and is developed by the Department of Cyber Intelligence and Security at Embry-Riddle Aeronautical University (Prescott) and Matthew E. Luallen, Chief Executive Inventor at CybatiWorks powered by IntelliGenesis. The ethical design of the competition is achieved through investigative themes that provides a focus in blue team while still offering red team aspects.

Storyline for CTF: On 8/6, an employee from ERAU Airline noticed a USB stick inside one of their kiosks. After further investigation, airport security suspects someone is carrying out an attack against the airport. You have been brought in to retrace the steps of the attackers, determine where security needs to be hardened, regain control of compromised systems, and prevent a successful attack at the airport. Identify the criminals by retracing their steps and utilizing OSINT to identify which suspects need to be arrested. Investigators have not ruled out insider threats which means you must remain undetected by airport staff while you attempt to regain control of the airport's infrastructure. Good Luck and remember to register ahead of time!

CybatiWorks part of the CTF Stage 7: Runway Lighting System: The Runway Lighting System (RLS) was taken over by the attackers and the lights are operating erratically. Identify what the attackers have changed causing the RLS HMI systems to work improperly and regain access to the remote logic controller operating the runway lights. Update the logic on the HMI system, regain control of the remote logic controller and successfully operate the RLS.

Architecture Design: The competitors are provided with a CybatiWorks custom docker image that they use to gain access to the operator and maintenance HMI logic. The competitors will review and update the logic to match the documentation provided in stage 4. Once the local components are successfully completed the competitors will request access to the remote RLS logic controller (i.e. a Raspberry PI with a 3d printed/LED runway lighting system accessible via a VPN). The competitors will complete additional challenges to confirm the logic program and then remotely control the RLS. All remote RLS stations will be visible

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 09:00-17:59 PDT

Title: A-ISAC CTF -- Pre-registration Required
When: Saturday, Aug 7, 09:00 - 17:59 PDT
Where: Aerospace Village (Virtual CTF)

Description:

A-ISAC, ERAU with support from IntelliGenesis (CybatiWorks)

Day 1: Aug. 6th, 2021 9:00AM – 6:00PM PDT (UTC-7) Day 2: Aug. 7th, 2021 9:00AM – 6:00PM PDT (UTC-7)

Registration available at https://aisac.cyberskyline.com/defcon

Aviation ISAC is hosting a competition at DC29 Aerospace Village! This competition represents a simulated airport hosted on the Cyber Skyline platform and is developed by the Department of Cyber Intelligence and Security at Embry-Riddle Aeronautical University (Prescott) and Matthew E. Luallen, Chief Executive Inventor at CybatiWorks powered by IntelliGenesis. The ethical design of the competition is achieved through investigative themes that provides a focus in blue team while still offering red team aspects.

Storyline for CTF: On 8/6, an employee from ERAU Airline noticed a USB stick inside one of their kiosks. After further investigation, airport security suspects someone is carrying out an attack against the airport. You have been brought in to retrace the steps of the attackers, determine where security needs to be hardened, regain control of compromised systems, and prevent a successful attack at the airport. Identify the criminals by retracing their steps and utilizing OSINT to identify which suspects need to be arrested. Investigators have not ruled out insider threats which means you must remain undetected by airport staff while you attempt to regain control of the airport's infrastructure. Good Luck and remember to register ahead of time!

CybatiWorks part of the CTF Stage 7: Runway Lighting System: The Runway Lighting System (RLS) was taken over by the attackers and the lights are operating erratically. Identify what the attackers have changed causing the RLS HMI systems to work improperly and regain access to the remote logic controller operating the runway lights. Update the logic on the HMI system, regain control of the remote logic controller and successfully operate the RLS.

Architecture Design: The competitors are provided with a CybatiWorks custom docker image that they use to gain access to the operator and maintenance HMI logic. The competitors will review and update the logic to match the documentation provided in stage 4. Once the local components are successfully completed the competitors will request access to the remote RLS logic controller (i.e. a Raspberry PI with a 3d printed/LED runway lighting system accessible via a VPN). The competitors will complete additional challenges to confirm the logic program and then remotely control the RLS. All remote RLS stations will be visible

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Thursday - 13:00-23:59 PDT

Title: A&E Pool Party!
When: Thursday, Aug 5, 13:00 - 23:59 PDT
Where: Bally's Pool

Description:
Pool Party Schedule is listed here: https://forum.defcon.org/node/238025

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 13:00-23:59 PDT

Title: A&E Pool Party!
When: Friday, Aug 6, 13:00 - 23:59 PDT
Where: Bally's Pool

Description:
Pool Party Schedule is listed here: https://forum.defcon.org/node/238025

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 13:00-23:59 PDT

Title: A&E Pool Party!

When: Saturday, Aug 7, 13:00 - 23:59 PDT

Where: Bally's Pool

Description:

Pool Party Schedule is listed here: https://forum.defcon.org/node/238025

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Sunday - 13:00-23:59 PDT

Title: A&E Pool Party!
When: Sunday, Aug 8, 13:00 - 23:59 PDT
Where: Bally's Pool

Description:
Pool Party Schedule is listed here: https://forum.defcon.org/node/238025

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 15:30-16:15 PDT

Title: “Alexa, have you been compromised?” — Exploitation of Voice Assistants in Healthcare (and other business contexts)

When: Friday, Aug 6, 15:30 - 16:15 PDT

Where: IoT Village (Talk - Virtual)

SpeakerBio: Hutch (Justin Hutchens)

Justin Hutchens (“Hutch”) is the Assessments Services Practice Lead at Set Solutions and manages TVM, IR, and GRC services. He is the co-host of the "Ready, Set, Secure" InfoSec podcast. He is also the creator of Sociosploit, a research blog which examines exploitation opportunities on the social web – a confluence of his interests in both hacking and social psychology. Hutch has spoken at multiple conferences to include HouSecCon, ToorCon, and DEF CON.

Description:

As voice assistant technologies (such as Amazon Alexa and Google Assistant) become increasingly sophisticated, we are beginning to see adoption of these technologies in the workplace. Whether supporting conference room communications, or even supporting interactions between an organization and its customers — these technologies are becoming increasingly integrated into the ways that we do business. While implementations of these solutions can streamline operations, they are not always without risk. During this talk, the speaker will discuss lessons learned during a recent penetration test of a large-scale “Alexa for Business” implementation in a hospital environment where voice assistants were implemented to assist with patient interactions during the peak of the COVID-19 pandemic. The speaker will provide a live demonstration of how a cyber-criminal could potentially use pre-staged AWS Lambda functions to compromise an “Alexa for Business” device with less than one-minute of physical access. Multiple attack scenarios will be discussed to include making Alexa verbally abuse her users (resulting in possible reputation damage), remote eavesdropping on user interactions, and even active “vishing” (voice phishing) attacks to obtain sensitive information. Finally, the talk will conclude with a discussion of best-practice hardening measures that can be taken to prevent your “Alexa for Business” devices from being transformed into foul-mouthed miscreants with malicious intent.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Abusing SAST tools! When scanners do more than just scanning
When: Friday, Aug 6, 15:00 - 15:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Rotem Bar
Rotem Bar has over a decade of experience in the security field including penetration testing both application and network, design reviews, code reviews, architecture reviews, tech management, and of course development.

Over the years Rotem has gained experience in a diversity of industries from the financial services, to insurance, through high-tech & the automotive industry, along with other complex environments.

In the last couple of years Rotem has been working in concept design and development, pen testing and working with hardware in Cymotive, which is a company that focuses on end to end cyber security for the automotive industry, and after that he served as an application security expert at AppsFlyer.

Today Rotem is the Head of Marketplace Integrations at Cider Security, that is focusing on revolutionizing CI/CD security.

During his free time, Rotem plays with robotics, bug-bounty and and enjoys traveling with his family.

Twitter: @rotembar
www.rotem-bar.com

Description:
When we write code, we often run many scanners for different purposes on our code - from linters, to testing, security scanning, secret scanning, and more.

Scanning the code occurs on developers' machines and in CI/CD pipelines, which assumes the code is untrusted and unverified and based on this assumption scanners shouldn't have the ability to dynamically run code.

Our research focuses on the many static analyzers out there if this is really the case. Many of the scanners allow different ways of interaction - From requesting external resources, overriding the configuration and to remote code execution as part of the process.This talk will be technical and show examples of well-known scanning tools and how we created code that attacks them.

TLDR -
When integrating and using new tools in our CI systems and especially when running on unverified code, Which tools can we trust and how can we scan safe untrusted code in a secure way?

REFERENCES

https://github.com/jonase/kibit/issues/235 - Issue I raised in the past in one of the tools

Hiroki Suezawa in a thread in cloud security forum talked about exploiting terraform plan
https://cloudsecurityforum.slack.com/archives/CNJKBFXMH/p1584035704035800

This reference was released after I've started my research but nevertheless a good resource and has interesting perspectives and I will reference it: https://alex.kaskaso.li/post/terraform-plan-rce

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=Jl-CU6G4Ofc

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20R

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:00-15:59 PDT

Title: ADSB Demo and Paper Airplanes

When: Friday, Aug 6, 10:00 - 15:59 PDT

Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:

Interactive ADS-B demonstration and paper airplane activity. Educational and fun

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 10:00-15:59 PDT

Title: ADSB Demo and Paper Airplanes
When: Saturday, Aug 7, 10:00 - 15:59 PDT
Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:
Interactive ADS-B demonstration and paper airplane activity. Educational and fun

Return to Index - Add to Google Calendar - ics Calendar file

WS - Saturday - 15:00-18:59 PDT

Title: Advanced Wireless Attacks Against Enterprise Networks
When: Saturday, Aug 7, 15:00 - 18:59 PDT
Where: Workshops - Las Vegas 5+6 (Onsite Only)

SpeakerBio: Solstice , Offensive Security Engineer
Solstice is an offensive security engineer at a major cloud provider. He currently specializes in kinetic threats, identifying attack vectors against "edge" devices deployed in hostile environments. Previously, he worked as a red team operator at companies such as SpecterOps, specializing in SIGINT and Windows-focused adversarial tradecraft. He is the author of EAPHammer, SilentBridge, DropEngine, and has contributed to high-profile projects such as hostapd-wpe and Empire.

Description:

This workshop will instruct attendees on how to carry out sophisticated wireless attacks against corporate infrastructure. Attendees will learn how to attack and gain access to WPA2-Enterprise networks using relay attacks, how to abuse MSCHAPv2 and GTC to efficiently capture network credentials, perform effective target selection with zero prior knowledge, leverage rogue access point attacks to deliver malware and harvest keystrokes, and abuse Opportunistic Wireless Encryption (OWE) to perform PITM attacks. All material discussed in the lectures will be practiced within a realistic lab environment.

Registration Link:
https://www.eventbrite.com/e/advanced-wireless-attacks-against-enterprise-networks-las-vegas-5-6-tickets-162214769743

Prerequisites

A previous wireless security background is helpful but certainly not required.

Materials needed:
- Students will be required to provide their own laptops, which must meet the following requirements:

- must be capable of running virtualization software such as VMWare or VirtualBox
- must have at least 100gb of free disk space OR have a free USB port and supplementary external hard drive with at least 100gb of free disk space available
- must be provisioned with a 64-bit operating system

Corporate / managed laptops are not recommended due to software restrictions.

Return to Index - Add to Google Calendar - ics Calendar file

Title: Adventures in MitM-land: Using Machine-in-the-Middle to Attack Active Directory Authentication Schemes
When: Saturday, Aug 7, 16:00 - 16:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Eyal Karni,Sagi Sheinfeld,Yaron Zinar

SpeakerBio: Eyal Karni
Eyal Karni is a Sr. Engineer at CrowdStrike working on Identity Protection products (previously Preempt). Eyal spent over 11 years researching cyber security projects. Previously, he served 5 years in an elite unit of the IDF in Cyber Security Research and Development. Eyal is an expert on Windows Internals and has previously found numerous vulnerabilities. Eyal holds a B.Sc in Mathematics and Physics.
Twitter: @eyal_karni

SpeakerBio: Sagi Sheinfeld
Sagi Sheinfeld is a Sr. Engineer at CrowdStrike working on Identity Protection products (previously Preempt). Sagi spent over 14 years researching cyber security projects. Previously, he served 8 years in an elite unit of the IDF in Cyber Security Research and Development and in IBM Security. Sagi is an expert on Windows internals. Sagi holds a B.Sc in Computer Science.
Twitter: @sagish1233

SpeakerBio: Yaron Zinar
Yaron Zinar is a Sr. Manager at CrowdStrike working on Identity Protection products (previously Preempt). Previously, Yaron spent over 16 years at leading companies such as Google where he held various positions researching and leading big data, machine learning and cyber security projects. Yaron is an expert on Windows Authentication protocols and has previously presented his research at top conferences such as Black Hat and DEFCON. Yaron holds an M.Sc. in Computer Science with focus on statistical analysis.
Twitter: @YaronZi

Description:
Over the years, researchers were able to break many secure protocols using MitM attacks. A common theme in this family of vulnerabilities is the lack of proper validation for any of the communicating parties. We will review previous MitM attacks found on AD authentication protocols and the mitigation strategies previously implemented. We will show that the relay attack technique is not limited to NTLM alone and can be used to attack the newer Kerberos authentication protocol. In addition, we will show several injection attacks compromising client systems. We'll show how the lack of validation can lead to devastating issues ranging from authentication bypass to remote code execution on various critical infrastructure systems. However, the issues do not stop on Windows on-premises networks but span to other infrastructure such as domain-joined unix machines, virtualization infrastructure, open-source security audit tools and even cloud directories. The talk will deep-dive into multiple vulnerabilities we have discovered along with several demos. Demos include a MitM attack which allows an attacker to inject user passwords in a hybrid AD environment allowing the attacker to authenticate as any user in the network. We will also show how to use a similar technique to compromise many other IT infrastructure.

REFERENCES

https://www.crowdstrike.com/blog/cve-2021-1678-printer-spooler-relay-security-advisory/
https://labs.f-secure.com/archive/practically-exploiting-ms15-014-and-ms15-011/
https://www.securityfocus.com/bid/1616/info

--

This talk has been released to the DEF CON Media server.

Media:

https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20S

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Friday - 14:15-15:15 PDT

Title: Adventures in Pro Bono Digital Forensics Work
When: Friday, Aug 6, 14:15 - 15:15 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: John Bambenek
John Bambenek is President of Bambenek Labs, a threat intelligence firm, and a PhD student studying cyber security machine learning at the University of Illinois at Urbana-Champaign. He has 20 years experience investigating cyber crime and has participated in large investigations in ransomware, the 2016 election-related hacking, and extremist fundraising in cryptocurrency.
Twitter: @bambenek

Description:

Most of DFIR work never makes it to a courtroom and even when it does it is often unchallenged. This talk will cover cases of doing pro bono digital forensics for public defenders and journalists and the shoddy work that often passes for science.

One of the major problems with our justice system is how the power dynamics work when one side of a legal dispute has resources and the other does not. This plays out in digital forensics too. Most of our work never ends up in court and is rarely challenged. While most of us are honest, there is far more work that needs to be done and not enough qualified people doing it. In short, not every analyst is qualified or experienced but their testimony is accepted unquestioned.

This talk will cover cases that were performed pro bono for clients who would not normally have access to an expert to challenge the government’s experts. Cautionary tales of bad analysis will be shown to emphasize the importance of sound forensic techniques and the risks of sloppy work.

The talk will end with a call to action for more professionals to contribute their time on similar pro bono efforts.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Saturday - 10:00-10:30 PDT

Title: Adversary Infrastructure Tracking with Mihari
When: Saturday, Aug 7, 10:00 - 10:30 PDT
Where: Recon Village (Virtual)

SpeakerBio: Manabu Niseki
No BIO available
Twitter: @ninoseki

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Sunday - 16:00-16:59 PDT

Title: Adversary Village Closing Ceremony
When: Sunday, Aug 8, 16:00 - 16:59 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Adversary Village Team
No BIO available

Description: No Description available

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 12:15-12:59 PDT

Title: Adversary Village Keynote
When: Friday, Aug 6, 12:15 - 12:59 PDT
Where: Adversary Village (Virtual)

SpeakerBio: David Kennedy , CEO, TrustedSec
David is a cybersecurity authority whose mission is to drive the industry forward and make the world a more secure place. In addition to creating two large-scale cybersecurity firms, David has testified before Congress on issues of national security and has appeared as a subject matter expert on hundreds of national news and TV shows.

Prior to creating TrustedSec, David was a Chief Security Officer (CSO) for Diebold Incorporated, a Fortune 1000 company. As a forward thinker in the security field, David has had the privilege of speaking at some of the nation's largest conferences, including Microsoft's BlueHat, DEF CON, Black Hat, and DerbyCon, which he co-created in 2011 and expanded into DerbyCon Communities.

Twitter: @HackingDave
https://www.linkedin.com/in/davidkennedy4

Description: No Description available

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 12:00-12:15 PDT

Title: Adversary Village Kick-off
When: Friday, Aug 6, 12:00 - 12:15 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Abhijith B R
No BIO available

Description: No Description available

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 14:30-14:59 PDT

Title: AI Policy Talk: "An AI Security ISAC" and "An AI Playbook"
When: Friday, Aug 6, 14:30 - 14:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Sagar Samtani
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 11:30-12:59 PDT

Title: AIAA CubeSat Hacking Workshop - Virtual Lab #1
When: Friday, Aug 6, 11:30 - 12:59 PDT
Where: See Description

Description:
DEF CON participants will be able to interact with CubeSat hardware and ground equipment in cybersecurity sandbox environment.

For more information, please see
https://aerospacevillage.org/events/upcoming-events/def-con-29/aiaa-cubesat-hacking-workshop/

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 14:00-15:59 PDT

Title: AIAA CubeSat Hacking Workshop - Virtual Lab #2
When: Friday, Aug 6, 14:00 - 15:59 PDT
Where: See Description

Description:

DEF CON participants will be able to interact with CubeSat hardware and ground equipment in cybersecurity sandbox environment.

For more information, please see https://aerospacevillage.org/events/upcoming-events/def-con-29/aiaa-cubesat-hacking-workshop/

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 11:30-12:59 PDT

Title: AIAA CubeSat Hacking Workshop - Virtual Lab #3
When: Saturday, Aug 7, 11:30 - 12:59 PDT
Where: See Description

Description:

DEF CON participants will be able to interact with CubeSat hardware and ground equipment in cybersecurity sandbox environment.

For more information, please see
https://aerospacevillage.org/events/upcoming-events/def-con-29/aiaa-cubesat-hacking-workshop/

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 14:00-15:59 PDT

Title: AIAA CubeSat Hacking Workshop - Virtual Lab #4
When: Saturday, Aug 7, 14:00 - 15:59 PDT
Where: See Description

Description:

DEF CON participants will be able to interact with CubeSat hardware and ground equipment in cybersecurity sandbox environment.

For more information, please see
https://aerospacevillage.org/events/upcoming-events/def-con-29/aiaa-cubesat-hacking-workshop/

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:00-11:30 PDT

Title: AIAA CubeSat Hacking Workshop - World Premier of the videos
When: Friday, Aug 6, 10:00 - 11:30 PDT
Where: See Description

Description:

DEF CON participants will be able to interact with CubeSat hardware and ground equipment in cybersecurity sandbox environment.

For more information, please see
https://aerospacevillage.org/events/upcoming-events/def-con-29/aiaa-cubesat-hacking-workshop/

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Friday - 13:00-13:55 PDT

Title: AIS Protocol Internals (Abridged)
When: Friday, Aug 6, 13:00 - 13:55 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: Gary Kessler
Gary Kessler, Ph.D., CISSP is a principal consultant at Fathom5, a retired professor of cybersecurity, and co-author of "Maritime Cybersecurity: A Guide for Leaders and Managers." He is a past speaker at DEFCON, where he has presented on AIS cybersecurity vulnerabilities and an encryption-based demonstration-of-capability method to mitigate some of those vulnerabilities. Gary's background is in mathematics and computer science, and he has spent several decades teaching about network protocols, data communications, digital forensics, and information security. He holds a leadership position in USCG Auxiliary cybersecurity efforts, is a Master SCUBA Diver Trainer, and holds a 50GT captain license.

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Friday - 10:00-11:50 PDT

Title: AIS Tools Demo (DEF CON)
When: Friday, Aug 6, 10:00 - 11:50 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: Gary Kessler
Gary Kessler, Ph.D., CISSP is a principal consultant at Fathom5, a retired professor of cybersecurity, and co-author of "Maritime Cybersecurity: A Guide for Leaders and Managers." He is a past speaker at DEFCON, where he has presented on AIS cybersecurity vulnerabilities and an encryption-based demonstration-of-capability method to mitigate some of those vulnerabilities. Gary's background is in mathematics and computer science, and he has spent several decades teaching about network protocols, data communications, digital forensics, and information security. He holds a leadership position in USCG Auxiliary cybersecurity efforts, is a Master SCUBA Diver Trainer, and holds a 50GT captain license.

Description:
This is a placeholder event.

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

Title: AIS Tools
When: Friday, Aug 6, 10:00 - 11:50 PDT
Where: DemoLab Video Channel 1

SpeakerBio: Gary Kessler
Gary Kessler, Ph.D., CISSP is a principal consultant at Fathom5, a retired professor of cybersecurity, and co-author of "Maritime Cybersecurity: A Guide for Leaders and Managers." He is a past speaker at DEFCON, where he has presented on AIS cybersecurity vulnerabilities and an encryption-based demonstration-of-capability method to mitigate some of those vulnerabilities. Gary's background is in mathematics and computer science, and he has spent several decades teaching about network protocols, data communications, digital forensics, and information security. He holds a leadership position in USCG Auxiliary cybersecurity efforts, is a Master SCUBA Diver Trainer, and holds a 50GT captain license.

Description:

Tool or Project Name: AIS Tools

Short Abstract: AIS Tools is a suite of Perl-based scripts to create, capture, interpret, and play NMEA 0183 Automatic Identification System (AIS) messages.

Short Developer Bio: Gary Kessler, Ph.D., CISSP is a principal consultant at Fathom5, a retired professor of cybersecurity, and co-author of "Maritime Cybersecurity: A Guide for Leaders and Managers." He is a past speaker at DEFCON, where he has presented on AIS cybersecurity vulnerabilities and an encryption-based demonstration-of-capability method to mitigate some of those vulnerabilities. Gary's background is in mathematics and computer science, and he has spent several decades teaching about network protocols, data communications, digital forensics, and information security. He holds a leadership position in USCG Auxiliary cybersecurity efforts, is a Master SCUBA Diver Trainer, and holds a 50GT captain license.

URL to any additional information:
https://www.garykessler.net/library/ais_pi.html https://www.garykessler.net/software/AIS_README.TXT
https://gpsd.gitlab.io/gpsd/AIVDM.html
https://github.com/trendmicro/ais/

Detailed Explanation of Tool:
AIS Tools is a suite of Perl scripts that allow a user to customize and parse National Marine Electronics Association (NMEA) 0183 standard AIS messages (seen in over-the-air broadcasts per ITU Recommendation M.1371). It is conceptually based upon the TrendMicro AIS Blacktoolkit, but is an extension intended for research and development purposes by incorporating more message types and standard default values.

The suite includes the following programs and functions: AIS_menu: Allows the user to create a custom NMEA 0183 AIS message by entering parameters specific to a requested message type. (At this time, the tools supports 22 of the 27 message types.) The output of the program is a properly formatted command line with all appropriate switches for the AIS_ping program. AIS_ping: AIS_ping allows a user to define an AIS message that will be properly formatted but could, in fact, contain invalid parameter values (a la hping3). The output is a binary string representing the AIS message. The binary string could be directed to a radio transmission (using Blacktoolkit software for GNU Radio) or formatted into one or more AIS sentences using AIS_NMEA. AIS_NMEA: This program accepts an AIS message binary string and produces a set of one or more AIS sentences. AIS_parser: Decodes an NMEA binary string or AIS sentence, displaying the contents field by field. parser2html: Produces HTML formatting of parsed messages. timestamp_data: Capture live AIS data from over-the-air transmissions and store the sentences in a file with a timestamp. play_ais: Replay timestamped AIS data from a file. This is code that was used for research and development purposes, gathering input from, and directing output to, OpenCPN. Data can also be received and broadcast via software-defined radio.

More detail can be found in https://www.garykessler.net/software/AIS_README.TXT

Supporting Files, Code, etc: https://www.garykessler.net/software/index.html#ais

Target Audience:
Defense, students, researchers, product developers (but, like any good tool, can be used for offense)

This tool is specifically directed at those interested in maritime cybersecurity, particularly with respect to navigation systems, but applies to anyone interested in a deep understanding of the AIS protocol as observed in over-the-air transmissions. It will aid researchers in capturing and analyzing AIS data, and designing scenarios with which to prepare exercises and test products.

This content will be presented on a Discord video channel.

#dl-video1-voice: https://discord.com/channels/708208267699945503/734027693250576505

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 12:00-12:30 PDT

Title: Algorithmic Ethics Bug Bounty Contest Announcement
When: Friday, Aug 6, 12:00 - 12:30 PDT
Where: AI Village (Virtual)

SpeakerBio: Rumman Chowdhury
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Saturday - 13:30-14:30 PDT

Title: Amateur Radio Digital Modes Primer
When: Saturday, Aug 7, 13:30 - 14:30 PDT
Where: Ham Radio Village (Virtual Talks)

SpeakerBio: Jon Marler
Jon is a product manager at SecureTrust with a true passion for information security. Jon is an amateur radio operator, lockpicker, phreaker, repairer of all things, and maker. As a result of his long-standing commitment to open source software, Jon has offered his expertise as a package manager for the Debian GNU/Linux OS distribution since 1998.

Description:
Amateur radio operator Jon Marler, callsign K4CHN, presents an introduction to many of the digital modes available to amateur radio operators. Jon will be discussing the modes available for voice and data, as well as many of the hardware options available. Jon will also be presenting a very simple design for a way to connect a Raspberry Pi to your radio safely. A demonstration of slow scan television (SSTV) will be made to end the presentation before Q&A.

All Ham Radio Village talks will be streamed to Twitch, with discussion in Discord.

For more information, see https://hamvillage.org/dc29.html

Twitch: https://www.twitch.tv/hamradiovillage

#hrv-presentation-text: https://discord.com/channels/708208267699945503/736674835413073991

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Saturday - 11:00-11:59 PDT

Title: Amateur Radio Mesh Networking: Enabling Higher Data-rate Communications

When: Saturday, Aug 7, 11:00 - 11:59 PDT

Where: Ham Radio Village (Virtual Talks)

SpeakerBio: Tyler Gardner

Tyler Gardner holds a General class U.S. amateur radio license. He received his first license in 2017 and enjoys participating in ARES, contesting, public service events, and digital modes. While attending college in Logan, Utah, Tyler was a member of the Bridgerland Amateur Radio Club. He now participates in amateur radio organizations in Dayton, Ohio, including the Miami Valley Mesh Alliance. Professionally, Tyler holds a master's degree in Aerospace Engineering and works as a research engineer.

Description:

Amateur radio encompasses a broad range of activities and applications. From contests and events to emergency communications and public service, hams have many different interests they can explore. One area that is being enabled by modern wireless technologies is mesh networking. Typical digital radio modes, such as those based on AX.25, offer low data rates. While fairly robust and widely used, the low data rates of these modes limits their capabilities. Mesh networking, such as AREDN, can supplement and empower many aspects of your amateur radio operations - and the entry cost is quite low! This presentation will talk about what mesh networking is, how it is being used by amateur radio operators, and how you can get started with mesh networking yourself!

All Ham Radio Village talks will be streamed to Twitch, with discussion in Discord.

For more information, see https://hamvillage.org/dc29.html

Twitch: https://www.twitch.tv/hamradiovillage

#hrv-presentation-text: https://discord.com/channels/708208267699945503/736674835413073991

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Sunday - 11:00-12:30 PDT

Title: An Introduction to RF Test Equipment
When: Sunday, Aug 8, 11:00 - 12:30 PDT
Where: Ham Radio Village (Virtual Talks)

SpeakerBio: Kurits Kopf
Kurits Kopf is a software engineer, technology enthusiast, and perpetual hobby collector. He is a video game industry veteran, working in Los Angeles. When he's not building games or playing them with his kids, he's in the garage tinkering. He has been taking interesting things apart to see how they work since childhood, and sometimes has even managed to put them back together.

Description:

An overview covering several common pieces of equipment used in RF and Ham Radio testing, focusing on oscilloscopes, spectrum analyzers, and vector network analyzers. I cover the basics of each and demonstrate common uses of the equipment for RF testing on both homebrew and commercial equipment. I also introduce other testing tools, including temperature controlled oscillators, dummy loads, and attenuators.

All Ham Radio Village talks will be streamed to Twitch, with discussion in Discord.

For more information, see https://hamvillage.org/dc29.html

Twitch: https://www.twitch.tv/hamradiovillage

#hrv-presentation-text: https://discord.com/channels/708208267699945503/736674835413073991

Return to Index - Add to Google Calendar - ics Calendar file

WS - Saturday - 15:00-18:59 PDT

Title: Analysis 101 and 102 for the Incident Responder
When: Saturday, Aug 7, 15:00 - 18:59 PDT
Where: Workshops - Las Vegas 1+2 (Onsite Only)

SpeakerBio: Kristy Westphal , Vice President, Security Operations
Kristy Westphal is a versatile information technology professional with specific experience in providing advisory and management services in the area of information security and risk is currently employed as the Vice President, Security Operations at a financial services company. Specializing in leadership and program development, specific expertise in security areas includes: process analysis, risk assessments, security awareness programs, operating system security, network security, incident handling, vulnerability analysis and policy development.

Description:

You have a theory about something you have found while roaming the network or conducting your own hackfest, but how do you go about proving it? This workshop will be a hands-on journey deep into the world of analysis. While analysis is a bit of an art form, there are methods that can be applied to make it less of a gut feeling and more of a scientific approach to support your hypothesis. From network forensics to log analysis to endpoint forensics and cloud log analysis, we will review numerous quick methods to gain context over the data you have gathered and apply critical thinking in an attempt to find the answers. Sometimes, the answers weren’t meant to be found, but we’ll also discuss how to make the best of any conclusion that you reach.

Registration Link:
https://www.eventbrite.com/e/analysis-101-and-102-for-the-incident-responder-las-vegas-1-2-tickets-162220226063

Prerequisites
None

Materials needed:
Laptop with Wireshark installed

Return to Index - Add to Google Calendar - ics Calendar file

WS - Friday - 10:00-13:59 PDT

Title: Analysis 101 and 102 for the Incident Responder

When: Friday, Aug 6, 10:00 - 13:59 PDT

Where: Workshops - Las Vegas 3+4 (Onsite Only)

SpeakerBio: Kristy Westphal , Vice President, Security Operations

Kristy Westphal is a versatile information technology professional with specific experience in providing advisory and management services in the area of information security and risk is currently employed as the Vice President, Security Operations at a financial services company. Specializing in leadership and program development, specific expertise in security areas includes: process analysis, risk assessments, security awareness programs, operating system security, network security, incident handling, vulnerability analysis and policy development.

Description:

You have a theory about something you have found while roaming the network or conducting your own hackfest, but how do you go about proving it? This workshop will be a hands-on journey deep into the world of analysis. While analysis is a bit of an art form, there are methods that can be applied to make it less of a gut feeling and more of a scientific approach to support your hypothesis. From network forensics to log analysis to endpoint forensics and cloud log analysis, we will review numerous quick methods to gain context over the data you have gathered and apply critical thinking in an attempt to find the answers. Sometimes, the answers weren’t meant to be found, but we’ll also discuss how to make the best of any conclusion that you reach.

Registration Link:
https://www.eventbrite.com/e/analysis-101-and-102-for-the-incident-responder-las-vegas-3-4-tickets-162216976343

Prerequisites

None

Materials needed:
Laptop with Wireshark installed

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:00-15:59 PDT

Title: Antenny

When: Friday, Aug 6, 10:00 - 15:59 PDT

Where: Aerospace Village (Virtual Workshop)

Description:

Come together to build on Antenny boards. Make things that can talk to the sky with very very very affordable hardware. What becomes possible when we have 1000 ground stations? I have a few ideas, I'm sure participants will have many others. Let's build it and find out together!

Return to Index - Add to Google Calendar - ics Calendar file

Title: Antenny

When: Saturday, Aug 7, 10:00 - 15:59 PDT

Where: Aerospace Village (Virtual Workshop)

Description:

Come together to build on Antenny boards. Make things that can talk to the sky with very very very affordable hardware. What becomes possible when we have 1000 ground stations? I have a few ideas, I’m sure participants will have many others. Let’s build it and find out together!

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Friday - 15:00-15:30 PDT

Title: Approaches to Attract, Develop, and Retain an Industrial Cybersecurity Workforce
When: Friday, Aug 6, 15:00 - 15:30 PDT
Where: ICS Village (Virtual)
Speakers: John Ellis,Julia Atkinson

SpeakerBio: John Ellis , Siemens Energy
John Ellis has 10 years of experience in global customer-centric strategic and business roles with a focus on relationship building, commercial intelligence, strategic advisory, and transforming technological innovation into business success. In his current role as the Global Head of Industrial Cyber Alliances at Siemens Energy, he works to develop partnerships between industry, academia, and government to solve some of the most challenging critical infrastructure cybersecurity challenges. John holds a BS in Mechanical Engineering and an MS in Engineering Management from the University of Maryland Baltimore County, an MBA from Johns Hopkins Carey Business School, and an MPS in Cybersecurity and Information Assurance from Penn State.

SpeakerBio: Julia Atkinson , Siemens Energy
Julia Atkinson has 10 years of relationship building experience across multiple sectors including business, government, NGO, and journalism. As a Global Cyber Program Alliance Manager at Siemens Energy, Julia believes in the power of diverse partnerships in solving today’s cybersecurity challenges. Julia graduated with her Master’s Degree in International Economics and Strategic Studies from The Johns Hopkins School of Advanced International Studies and holds a Bachelor’s in Political Science from Yale University.

Description:

Gaps in the industrial cybersecurity workforce leave critical infrastructure assets vulnerable to attack. In a 2020 ICS2 report, 64% of companies reported a significant or slight shortage of cybersecurity professionals. At the same time, 56% of companies reported that their organization is extremely or moderately at risk due to the cyber workforce shortage. A National Initiative for Cybersecurity Education (NICE) report found that industry-wide there was only one qualified worker to fill every 10 cybersecurity jobs in 2020. To protect the cyber-physical systems that form the lifeblood of the economy, something needs to be done to develop the ICS/OT cybersecurity workforce pipeline. This session will present models to attract, develop, and retain talent in industrial cybersecurity.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

APV - Sunday - 11:00-11:45 PDT

Title: AppSec 101: A Journey from Engineer to Hacker
When: Sunday, Aug 8, 11:00 - 11:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Arjun Gopalakrishna
No BIO available

Description:
Join this session to appreciate the role of Application Security in the context of software development, by examining them side by side. We will walk through an insecure application to find (and exploit) a few security issues, and examine - from an AppSec lens - the issue classes and ways to unearth them. This is an introductory level talk, especially for hackers new to AppSec.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 17:30-17:35 PDT

Title: AppSec Quiz Time!
When: Friday, Aug 6, 17:30 - 17:35 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Eden Stroet
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 17:45-17:50 PDT

Title: AppSec Quiz Time!
When: Saturday, Aug 7, 17:45 - 17:50 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Eden Stroet
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Sunday - 15:00-15:15 PDT

Title: AppSec Quiz Time!
When: Sunday, Aug 8, 15:00 - 15:15 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Eden Stroet
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Sunday - 13:00-12:59 PDT

Title: AppSec Village Capture the Flag Ends
When: Sunday, Aug 8, 13:00 - 12:59 PDT
Where: AppSec Village (Virtual)

Description:

For more information, see https://www.appsecvillage.com/ctf

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 11:00-10:59 PDT

Title: AppSec Village Capture the Flag Starts
When: Friday, Aug 6, 11:00 - 10:59 PDT
Where: AppSec Village (Virtual)

Description:

For more information, see https://www.appsecvillage.com/ctf

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Saturday - 09:00-10:59 PDT

Title: APT Hunting with Splunk
When: Saturday, Aug 7, 09:00 - 10:59 PDT
Where: Packet Hacking Village - Workshops (Virtual)

SpeakerBio: John Stoner , PRINCIPAL SECURITY STRATEGIST AT SPLUNK
John Stoner (Twitter: @stonerpsu) is a Principal Security Strategist at Splunk where he enjoys writing, problem solving and building stuff, including APT Scenarios. When not doing cyber things, you can find him watching his boys play hockey, reading or binge-watching TV series that everyone else has already seen.
Twitter: @stonerpsu

Description:

Interested in practicing your hunting skills? If so, this is the workshop for you. Using a real-worldish dataset, this workshop will teach you how to hunt the “fictional” APT group Violent Memmes. We discuss the Diamond model, building hypotheses, LM Kill Chain, and MITRE ATT&CK and how these concepts can frame your hunting. Using Splunk, we will hunt for APT activity riddling a small startup's environment. During the event, we will be presented with a "notable event" and pull on that string to conduct our own hunts based on indicators that we uncover or are identified. Depending on the hunt, we will uncover persistence, exfiltration, c2 and other adversary tactics. We may even find some PowerShell scripts. We will regroup and review the specific hunt conducted and discuss the timeline of events, a narrative that could be shared with others on your team, the artifacts that were uncovered to better identify potential future hunts, ATT&CK techniques referenced as well as what could be operationalized. At the end, we will highlight some additional datasets and content that you can take with you and try newly learned techniques yourself.

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Sunday - 11:45-12:30 PDT

Title: APT: A Short History and An Example Attack
When: Sunday, Aug 8, 11:45 - 12:30 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Mark Loveless , Researcher, Gitlab
Mark Loveless - aka Simple Nomad - is a security researcher, hacker, and explorer.He has worked in startups, large companies, hardware and software vendors. He's spoken at numerous security and hacker conferences worldwide on security and privacy topics, including Blackhat, DEF CON, ShmooCon, RSA, AusCERT, among others. He has been quoted in television, online, and print media outlets as a security expert, including CNN, Washington Post, and the New York Times. He's paranoid (justified), has done ghost hunting, been mugged four times, storm chased, and seen UFOs. He is currently a Sr Security Researcher at GitLab.
Twitter: @simplenomad
https://linkedin.com/in/markloveless

Description:

Advanced Persistent Threat. Where did this term come from? What does it really mean? Exactly how can you determine that it is a "nation state" as opposed to a run-of-the-mill attack? All of this will be explained in detail. As an example, I will use an actual attempt against my home system, with a review of collected data to illustrate the whole APT thing.

There are differences in how APT actors approach things, and this will be discussed from the perspective of someone who attacked plenty of systems in their youth - me. We'll talk about how APT differs from Red Teaming and Penetration Testing, and if you are trying to simulate it you need to throw the rulebook out of the window to do it right.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Friday - 12:30-12:59 PDT

Title: Are Barcodes on Ballots Bad?
When: Friday, Aug 6, 12:30 - 12:59 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Kevin Skoglund
Keããvin Skoglund is a digital security and election technology expert, and the President and Chief Technologist for Citizens for Better Elections, a non-profit, non-partisan group advocating for evidence-based elections. Kevin serves on the Board of Advisors for Verified Voting, participates in the NIST Voting System Cybersecurity Working Group which develops national guidelines for U.S. voting systems, and is a designated speaker on election security for the U.S. Department of State. His past work includes advising nonprofits, counties, cities, and members of the U.S. Congress on voting system technology and election legislation, researching security vulnerabilities, and identifying voting systems connected to the internet. Kevin is also a Judge of Election (chief poll worker) in Pennsylvania. Outside of his election work, Kevin has been a programmer, consultant, and teacher for over 20 years.

Description:

This presentation focuses on the use of barcodes on ballots, specifically barcodes on ballots that store vote selections. Skoglund teaches us how voting systems store votes and barcodes, explains how to decode them, and explores their attack surface from a security perspective. Through close examination of three examples (ES&S ExpressVote, Dominion ImageCast X, Unisyn Freedom Vote Tablet), the presentation explains potential attacks, and highlights detection and mitigation strategies.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Friday - 13:00-13:20 PDT

Title: Are We Still Doing it? 10 Locksport Hobbies that go Beyond Lock Picking
When: Friday, Aug 6, 13:00 - 13:20 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio: Lock Noob
No BIO available

Description:
There is so much more to locksport than just lock picking. In this presentation I look at 10 inspiring locksport hobbies that every lock picker should try! From key casting to tool making, from impressioning to making jewellery and many more, you will be surprised by the range and depth of the skills you can choose from.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:00-15:59 PDT

Title: ARINC 429 Lab
When: Friday, Aug 6, 10:00 - 15:59 PDT
Where: Aerospace Village (Workshop - Virtual + Paris Rivoli B)

Description:

Sessions will be held for small audience 15-20 users to demonstrate the structure and use of avionic-specific communication protocol (ARINC 429). This is an opportunity for hands-on experience in a controlled setting.

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 10:00-15:59 PDT

Title: ARINC 429 Lab

When: Saturday, Aug 7, 10:00 - 15:59 PDT

Where: Aerospace Village (Workshop - Virtual + Paris Rivoli B)

Description:

Sessions will be held for small audience 15-20 users to demonstrate the structure and use of avionic-specific communication protocol (ARINC 429). This is an opportunity for hands-on experience in a controlled setting.

Return to Index - Add to Google Calendar - ics Calendar file

Title: Assless Chaps: a novel combination of prior work to crack MSCHAPv2, fast (or why MSCHAPv2 is so broken, it's showing it's whole ass)

When: Thursday, Aug 5, 12:00 - 11:59 PDT

Where: Radio Frequency Village (Virtual)

Speakers:singe,cablethief

SpeakerBio:singe
No BIO available

SpeakerBio:cablethief
No BIO available

Description:
"Cracking intercepted MSCHAPv2 challenge/response pairs from Wi-Fi or VPN attacks has long been known to be possible. However, unless the underlying cleartext password was common, this can take frustratingly long. Especially, for at-the-same-time attacks like the auto-crack-and-add we proposed in 2014 [1]. We'll combine some prior work and release tooling to show how even extremely large hashlists can be run through in seconds.

MSCHAPv2 has several weaknesses, the first is that one doesn't need the clear-text password, as merely having the MD4 hash (aka NT hash) of the password is good enough to prove to either a client or authenticator you know the password. This means we can use a technique proposed in 2020 by Sam Croley called hash shucking [2] to use large NT hash lists such as the Have I Been Pwned set [3] to determine the NT hash used in the exchange. We'll go through the theory of MSCHAPv2, why the NT hash is useful and how to use it, as well as how hashcat modes for cracking it were developed.

The second weakness relates to the work done by Moxie Marlinspike and David Hulton in 2012 [4] where they found that because MSCHAPv2 breaks the NT hash into three parts, and pads the last two bytes with NULLs, its trivially easy to brute force this part (the ass). Then a brute force of the first two parts is performed using only a single DES round by iterating the entire DES keyspace with an FPGA. However, most of us still don't have our own MSCHAPv2 cracking FPGA rigs, and this attack isn't widely available or practical. Instead, if we limit our input hashlist to only those with the matching last two bytes, we can perform a far more efficient hash shucking attack against the exchange. We'll go through the theory of MSCHAPv2 in use here and the optimisations devised with an associated tool.

Finally, we'll end on why we think MSCHAPv2 needs to finally die the death it has so deserved for so long.

[1] https://sensepost.com/blog/2015/improvements-in-rogue-ap-attacks-mana-1%2F2/ and DEF CON 22 - Dominic White and Ian de Villiers - Manna from Heaven https://youtu.be/i2-jReLBSVk?t=1380

[2] DEF CON Safe Mode: Password Village - Sam Croley: What the Shuck? Layered Hash Shucking https://www.youtube.com/watch?v=OQD3qDYMyYQ

[3] https://haveibeenpwned.com/Passwords

[4] https://web.archive.org/web/20160120152007/http://cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/"

This talk has been released on YouTube.

YouTube: https://www.youtube.com/watch?v=lm7Cuktpnb4

Radio Frequency Village will not be streaming any talks, but they will be making talks available on their YouTube channel.

YouTube: https://youtube.com/c/RFHackersSanctuary

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Friday - 13:30-14:30 PDT

Title: At least ten questions for “Bad HIPPA Takes” (@BadHIPPA), 2021’s best tweeter on privacy, pandemic, and snark.
When: Friday, Aug 6, 13:30 - 14:30 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Lucia Savage , 21st Century health care strategic expert
Lucia is a nationally recognized expert on health information privacy. She was an architect of the foundational aspects of ONC's new interoperability rules. She believes in vaccine records.
Twitter: @savagelucia

Description:

From the start of the pandemic, through the election and the insurrection on the Capitol and on into the vaccine roll-out, the nationwide health privacy law, HIPAA, has gotten more famous and more misunderstood than ever. Out of this morass of politicization and polemic emerged “Bad HIPPA Takes” (@BadHIPPA), shining a light on the absurd, funny, sad and even accurate in a must-follow for anyone interested in privacy. In this session, we’ll ask Bad HIPPA Takes some questions, check out their views based on the past year, and even see if they have any inkling about the future of privacy law in the U. S.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

PYV - Friday - 10:00-10:59 PDT

Title: ATM Transaction Reversal Frauds (And how to fight them)
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: Payment Village (Virtual)

SpeakerBio: Hector Cuevas Cruz
No BIO available

Description:
Transaction Reversal Frauds (TRF) are a type of attack that doesn't require a malware, complex physical attacks or even opening an ATM, instead they abuse some business and operational rules defined by the financial institutions to cash-out an ATM. This presentation describe what Transaction Reversal Frauds are, why this type of attacks are on rise and more important, how to detect them through an integral analysis of journaling and some other logs

Payment Village events will stream to Twitch and YouTube.

--

Twitch: https://www.twitch.tv/paymentvillage

YouTube: https://www.youtube.com/c/PaymentVillage

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Friday - 09:30-10:59 PDT

Title: Attack and Detect with Prelude Operator and Security Onion
When: Friday, Aug 6, 09:30 - 10:59 PDT
Where: Blue Team Village - Workshop Track 1 (Virtual)

SpeakerBio: Wes Lambert
Wes Lambert is the Director of Support and Professional Services at Security Onion Solutions, where he helps customers to implement enterprise security monitoring solutions and understand their computer networks. A huge fan of OSS projects, Wes loves to solve problems and enhance security using completely free and easily deployable tools.
Twitter: @therealwlambert

Description:

In this workshop, we'll leverage Prelude Operator, an easy-to-use desktop platform for autonomous red teaming. With Operator, we can generate adversary profiles, complete with TTPs and goals, then deploy an "adversary", evaluating our detection coverage against the MITRE ATT&CK framework using Security Onion, a free and open platform for intrusion detection, enterprise security monitoring, and log management. By providing network, host, and other types of data, Security Onion can provide a leg up to defenders, allowing them to track down their adversaries and make them cry.

This talk will go over the introduction of red/purple teaming, along with how individuals can emulate adversary actions, as well as track those actions across their enterprise, evaluating their detection coverage.

We'll first go over how a tool like Prelude Operator can be used to emulate these adversary actions, then learn how Security Onion can be leveraged to detect these actions and track our coverage across the MITRE attack framework.

Throughout the discussion the following tools will be introduced:

Prelude Operator - autonomous red-teaming platform, creating adversaries to test detection Zeek - Policy-neutral NIDS
Suricata - Signature-based NIDS
Stenographer – Full Packet capture
Playbook - Detection development
ATT&CK Navigator - Track detection coverage Strelka - File analysis
Osquery - Host-based monitoring
Wazuh - HIDS

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 12:05-12:50 PDT

Title: Attacking Modern Environments Series: Attack Vectors on Terraform Environments
When: Friday, Aug 6, 12:05 - 12:50 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Mazin Ahmed
Mazin Ahmed is a security engineer that specializes in AppSec and offensive security. He is passionate about information security and has previously found vulnerabilities in Facebook, Twitter, Linkedin, and Oracle to name a few. Mazin is the developer of several popular open-source security tools that have been integrated into security testing frameworks and distributions. Mazin also built FullHunt.io, the next-generation continuous attack surface security platform. He is also passionate about cloud security where he has been running dozens of experiments in the cloud security world.
Twitter: @mazen160

Description:
Ever come across an environment in an engagement that uses Terraform for IAC (infrastructure-as-code) management? Almost every modern company does now.

In this talk, I will be sharing techniques and attack vectors to exploit and compromise Terraform environments in engagements, as well as patterns that I have seen that achieve successful infrastructure takeover against companies. I will be also covering prevention methods for the discussed attack vectors in my talk. This is part of my work-in-progress research in cloud security and attacking modern environments.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

APV - Sunday - 14:00-14:45 PDT

Title: Attacking Modern Environments Series: Attack Vectors on Terraform Environments
When: Sunday, Aug 8, 14:00 - 14:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Mazin Ahmed
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

CON - Thursday - 18:00-17:59 PDT

Title: AutoDriving CTF
When: Thursday, Aug 5, 18:00 - 17:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/238185 and https://autodrivingctf.org/

Return to Index - Add to Google Calendar - ics Calendar file

PYV - Friday - 12:00-12:59 PDT

Title: Automated Tear Machines
When: Friday, Aug 6, 12:00 - 12:59 PDT
Where: Payment Village (Virtual)

SpeakerBio: Meadow Ellis
No BIO available

Description:

Short, yet packed with information talk about why ATMs are bad, why they are a literal magnet for criminals, what types of attacks do actually happen and why it is so bloody hard to do any kind of research on them, unless you are a criminal. I won't bore you with stuff you can read on Wikipedia but rather give you an overview of terms, parts and crazy things people do to either get the money out of you or out of an ATM itself. And, what can you do to try and protect yourself and what to do when you see something 'that doesn't look right'. Don't tear off the magstripe from your card, though.

Payment Village events will stream to Twitch and YouTube.

--

Twitch: https://www.twitch.tv/paymentvillage

YouTube: https://www.youtube.com/c/PaymentVillage

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Saturday - 11:30-12:15 PDT

Title: AWS cloud attack vectors and security controls
When: Saturday, Aug 7, 11:30 - 12:15 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Kavisha Sheth
Kavisha is a Security Analyst at Appsecco. She is a cloud security and machine learning enthusiast who dabbles in application and API security and is passionate about helping customers in securing their IT assets. Kavisha is a member of a number of security communities including null community, InfoSecGirls, and WiCys India group. She believes in giving back to the community and frequently finds audiences to talk about Attacking GraphQL, different techniques to bypass authentication and Attacking AWS. When not breaking apps for Appsecco, Kavisha spends time learning and researching on different areas of security . She has also been listed as one of the top security researchers of the nation by NCIIPC RVDP.
Twitter: @sheth_kavisha

Description:

In the last decade, cloud computing has been incorporated in various industries, from Health to Military, which has been meticulously guided by exploring related technologies in the industry and academia alike. The enterprise computing model have shifted from on-site infrastructure to remote data centers which is accessible via internet and managed by cloud service providers.However, Many companies breached on AWS moved sensitive data to AWS without following best practices or implementing cloud security controls correctly. Main objective of the session is to bring awareness about some of the AWS cloud attack vectors and as well as security controls that can help. You get to know discovery, identification and exploitation of security weaknesses, misconfigurations lead to complete compromise of the cloud infrastructure. As,Cloud attack vectors and security controls are different as security professional you need to be aware about attack vector and controls. So, you will also learn about what can be possible best practices, detective controls to avoid some of the misconfigurations. In this session: - Learn about how an attacker can perform reconnaissance, leverage network, AWS Lambda functions, S3 misconfiguration and implementation in weaknesses to steal credentials and data. - Learn how misconfigurations and other leading cloud vulnerabilities put you at risk to exploitation with some real world example - Learn about Security controls, possible best practices, detective controls to avoid these misconfigurations

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Saturday - 13:50-14:35 PDT

Title: Azure Active Directory Hacking Wars
When: Saturday, Aug 7, 13:50 - 14:35 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Batuhan Sancak
Hello Cloud Village. I'm Batuhan (@nullx3d). He is a cyber security researcher. He's living Turkey and studying Management Information Systems at university. He's 21 age years old. He feel like he belong in cyberspace. Web Application Security, Linux structure is very attractive for he. He work on virtual machines, live web systems and on new technology(cloud security). Batuhan gave trainings and presentations in many universities in his country. He shares his experiences and works on his personal blog (docs.rka0x.com). If you accept he for defcon cloud village, he will very happy. This is he dream. he hopes you like the CFP.
Twitter: @nullx3d

Description:

Abstract Azure is one of the most popular cloud services today. It has 15.4 million customers worldwide. 95% of Fortune 500 companies use Azure. If you look at it from the hacker point of view, that's perfect. Is Azure completely secure? No! No system is completely secure. It would be good to talk about Azure and talk about attack techniques. Check out the attack vectors. The results obtained by comparing attack vectors and defense vectors will be beneficial for everyone. In this presentation, I would like to talk about Azure Active Directory technology and attack vectors. I wrote the titles for you to review. Outline

- Azure Ad Overview Roles, terminology
- Understand Active directory with azure
- Azure AD security features Attacking
- Azure Ad (Techniques)
    - Unauth Recon
    - Password Sniper
    - MsOnline Powershell Module
    - PHS
    - Backdoor Azure
    - SSO
    - Spn scanning
    - DcShadow Attack
    - Group Policy, etc.
- Defense Azure Ad Suggestions

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 14:00-15:59 PDT

Title: BADASS Meetup (Virtual)
When: Friday, Aug 6, 14:00 - 15:59 PDT
Where: See Description

Description:

We represent the BADASS army, an organization that empowers and assists victims of revenge-porn and non-consensual images through education in privacy, operational security, and evidence collection. This'd be an event where we discuss how we fight NCI/RP, how that battlespace has changed, what we've learned and more.

BADASS is going to be from 2 PM PDT til 4 PM PDT on Discord in Fireside Lounge for a video discussion.

Fireside Lounge: https://discord.com/channels/708208267699945503/738141986476916826

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Friday - 11:30-11:59 PDT

Title: BCOS Village Contest Overview
When: Friday, Aug 6, 11:30 - 11:59 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Reddcoin
No BIO available

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Friday - 13:00-13:30 PDT

Title: Beetlejuice: The Lessons We Should Have Learned For ICS Cybersecurity
When: Friday, Aug 6, 13:00 - 13:30 PDT
Where: ICS Village (Virtual)

SpeakerBio: Tim Yardley , University of Illinois Urbana-Champaign
Tim Yardley is a Principal Research Scientist and Associate Director at the Information Trust Institute (ITI) in the University of Illinois Urbana-Champaign. He works on trustworthiness and resiliency in critical infrastructure. Much of his work has focused on experimentation frameworks, device analytics, assessments, verification and validation, intrusion detection and data fusion approaches. Enough of the boring bio's though, let's have some fun.
Twitter: @timyardley

Description:
In this talk I will present the top 15 quotes from *redacted* and how we can transform them to operational advice to improve ICS cyber security. Hold tight, this is going to be a wild ride.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-13:59 PDT

Title: Beverage Cooling Contraption Contest
When: Friday, Aug 6, 10:00 - 13:59 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/236475

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Thursday - 10:00-13:59 PDT

Title: Biohacking Village CTF: Hospital Under Siege (Pre-Qual) (Pre-registration required)
When: Thursday, Aug 5, 10:00 - 13:59 PDT
Where: Biohacking Village (CTF)

Description:
https://www.villageb.io/ctf2021

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Friday - 10:00-10:45 PDT

Title: Biohacking Village Welcome Keynote
When: Friday, Aug 6, 10:00 - 10:45 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Nina Alli , Executive Director, Biohacking Village
No BIO available

Description:
Willkommen, Bienvenue, Bienvenido, Bem-vindo, , , , kaabo.

Lets talk about the strides we, as a village and a community, have made in one year.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Sunday - 14:00-14:30 PDT

Title: Biohacking Village Wrap-Up
When: Sunday, Aug 8, 14:00 - 14:30 PDT
Where: Biohacking Village (Talk - Virtual)

Description:
Where do we go from here?

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 10:00-18:30 PDT

Title: Black Box Challenges
When: Saturday, Aug 7, 10:00 - 18:30 PDT
Where: IoT Village (Onsite)

Description:
For more information, see https://www.iotvillage.org/defcon.html

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 10:00-18:30 PDT

Title: Black Box Challenges
When: Friday, Aug 6, 10:00 - 18:30 PDT
Where: IoT Village (Onsite)

Description:
For more information, see https://www.iotvillage.org/defcon.html

Return to Index - Add to Google Calendar - ics Calendar file

BICV - Saturday - 10:30-10:30 PDT

Title: Black Cyber Exodus: The Mis-Education (Certification) of Black Cyber
When: Saturday, Aug 7, 10:30 - 10:30 PDT
Where: Blacks in Cyber

SpeakerBio: Stephen Pullum
Stephen Pullum is a Cyber Security Evangelist and Pioneer. Stephen is an entrepreneur in Accra, Ghana to his company AFRICURITY. This company brings best practices in multiple lanes of Cybersecurity, Cyber Education, Cyber Resiliency and Cyber Scalability both corporate and individual. Stephen has over 40 years in the Cybersecurity field, having began in the early '80's with the handle 'The Madhatter'. Stephen is also recognized as an Alumni of the Cult of the Dead Cow (cDc). Stephen served in the United States Air Force from 1984 to 2012, and has a unique perspective of the Cybersecurity field as he has been participating in both the culture and the proffession since it's infancy.
Twitter: @The Madhatter

Description:
In this talk I will analyze the pipeline between many Black Cyber Practitioners that were never credited or brought to the forefront and the certification plans/materials being developed for the progression of the holistic industry, as well as discuss the premise; "How much of their non-profit revenue is being invested into the Black Community which they cleverly so snared into the premise of being qualified to do a job."

In1982, CompTIA was started under another name, yet still CompTIA. In 1989, SANS/GIAC was started and in 1992, ISC2 released the CBK that would 2 years later become the CISSP. In 2001, the EC Council formed in response to the attacks on the World Trade Center. Before these so-called cybersecurity certifications, how did the founders and instructors get certified to even instruct or create these organizations? Materials such as the Rainbow Books Series were the mainstay in the Trust Computing Model environment that are still being implemented today, just rebranded. These institutions implemented disproportionate programs when they gained traction and Cyber specific programs became profitable without giving up their "non-profit" status.

Blacks in Cyber talks will be streamed on YouTube.

YouTube: https://www.youtube.com/c/BlacksInCybersecurity

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 12:00-17:59 PDT

Title: Blacks in Cybersecurity CTF
When: Friday, Aug 6, 12:00 - 17:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236493 or https://www.blacksincyberconf.com/ctf

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 21:00-20:59 PDT

Title: Blockchain as a Threat Modeling Thinking Tool
When: Thursday, Aug 5, 21:00 - 20:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Shinchul Park, Graduate Student
Shinchul Park is graduate student at the School of Cybersecurity, Korea University from 2021 and his research areas focus on security engineering, blockchain.

Description:

Threat modelling is a risk-based approach to designing secure systems. It is based on identifying threats in order to develop mitigations to them. Threat modeling is a “team sport,” because it requires the knowledge and skill set of a diverse team where all inputs can be viewed as equal in value. As the enabler of mass collaboration, blockchain is the framework that pieces everything together at a larger scale.

In this talk, we propose the first platform that combines blockchain with threat modeling. To this end, we first present a system model that combines a blockchain-based collective intelligence system with threat modeling, and then explain the role of the model, the scheme of the tool, and the operation procedure.

This talk is now available on YouTube: https://www.youtube.com/watch?v=vBGhW9gnCtU

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Friday - 14:00-14:30 PDT

Title: Blockchain Security Tools
When: Friday, Aug 6, 14:00 - 14:30 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Mila Paul , Blockchain Security Researcher
Mila Paul is a researcher in cybersecurity and blockchain startup technology. Her background includes systems, network and storage in a secure and virtual infrastructure. She recently earned a Ph.D in Cyber Operations and enjoys teaching.

Description:

Blockchain was originally created by cypherpunks to integrate privacy and integrity in cash transactions. Since the inception of Bitcoin and its blockhain back-end, research and development in blockchain has revealed its strength in providing security through cryptology. This lecture inspires an exploration into finding blockchain based solution for common cybersecurity issues.

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

Title: BLUEMONDAY Series – Exploitation & Mapping of vulnerable devices at scale through self-registration services (DATTO/ EGNYTE/ SYNOLOGY/ MERAKI/ GEOVISION)
When: Friday, Aug 6, 14:30 - 15:15 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Ken Pyle
Ken Pyle is a partner of CYBIR, specializing in Information Security, exploit development, penetration testing and enterprise risk management. Ken is a graduate professor of CyberSecurity at Chestnut Hill College. He has published academic works on a wide range of topics and has presented at industry events such as ShmooCon, Secureworld, HTCIA International.

Description:

Vendors like DATTO, MERAKI, GEOVISION, SYNOLOGY, EGNYTE and others are which leverage or depend on these services are imperiling data, networks, and businesses through insecure design, intentional design decisions, and web application flaws.

These devices frequently self-provision services which leak critical data or through insecure network design and installation practices which are easily mapped, attacked, and discovered via insecure vendor, software, and integrator practices (ex. PKI, Dynamic DNS, “Finder” service registrations, DNS leakage, Layer 2 Attacks / DHCP network attacks, DNS passive hijacking through domain purchases & active record injection)

Some concepts and new attacks may be obliquely referenced or held private by the researcher. Essential PoC is contained in this document and is easily reproduced using supplied narrative and screenshots.

The affected devices are easily discoverable either through insecure practices (ex. insecure Zones, algorithmic FQDN generation, lack of local network controls, public metadata leakage) or vendor provided interfaces and access methods. (DATTOWEB, DATTOLOCAL, SYNOLOGY.ME, DYNAMIC-M, GVDIP.COM, EGNYTE-APPLIANCE.COM)

Many issues develop due to these problems. For example, nearly all of these devices and appliances provide easily discoverable portals / content / metadata with which to craft extremely convincing social engineering campaigns, even in the absence of technical exploit vectors.

Host Header Attacks & 302 redirects used in concert with malicious DNS records / spoofed or squatted domains can be abused in this manner. An attacker can identify the MERAKI device a victim uses through registration, abuse the API to obtain sensitive metadata, and send the victim to a spoofed site or malicious content purported to be a Meraki Dashboard alert. An attacker can change the dynamic DNS record through a number of vectors (ex. Third party service attacks, local vectors) and effectively “hijack” the user or content being accessed.

Through our DNS harvesting and our undisclosed 0-days, we can establish a complex exploit network and botnet via poor vendor controls (ex. MIRAI) We can also hide exploit code in APIs, persist across multiple appliance types, and abuse multiple dynamic DNS networks.

The DNS zones we have provided are intentionally designed, demonstrably insecure, provide detailed information, and can be abused easily. Registrations can be abused for data exfiltration or beaconing over the vendor’s DNS network. These DYNAMIC DNS services allow for efficient, mass exploitation and recon. The poor controls and “spoofability” of these networks (will demonstrate at another time) allow an attacker to not only FIND vulnerable devices.. but automate mass exploitation via attacks such as those we provided or other common attacks.

The author wishes for this to be noted as responsible disclosure and ethical considerations for the attacks / exploits seriously impacted disclosure dates and continues to.

Some initial work can be found here:

https://cybir.com/2021/cyber-security/bluemonday-series-part-1-exploitation-mapping-of-vulnerable-devices-at-scale-through-self-

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Sunday - 13:00-13:59 PDT

Title: Bobby Pins, More Effective Than Lockpicks?

When: Sunday, Aug 8, 13:00 - 13:59 PDT

Where: Lock Pick Village (Virtual)

SpeakerBio: John the Greek
No BIO available

Description:

When should you not have picks in your pocket? Answer, never... but This course will present to the novice and the less prepared suggestions for improvising lockpicks when the proper tools are not on hand as well as techniques of bypass that are more effective than trying to pick a lock especially when you don't have the proper tools on hand. This class is ideal for our current situation! Those interested should look around their locations for the following:

Bobby pins
Paper clips (big ones)
Pocket clips from ink pens (Pilot rollerball) Old Wind Shield Wipers
Spark Plug Gappers
Bra Underwire

... and my favorite
Street cleaner bristles

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Sunday - 10:00-10:30 PDT

Title: Bottom-Up and Top-Down: Exploiting Vulnerabilities In the OT Cloud Era
When: Sunday, Aug 8, 10:00 - 10:30 PDT
Where: ICS Village (Virtual)
Speakers: Sharon Brizinov,Uri Katz

SpeakerBio: Sharon Brizinov , Claroty
Sharon Brizinov is the vulnerability research team lead at Claroty. He specializes in vulnerability research, malware analysis, network forensics, and ICS/SCADA security. In addition, Brizinov participated in well-known hacking competitions such as Pwn2Own, and he holds a DEFCON black-badge for winning the ICS CTF.

SpeakerBio: Uri Katz , Claroty
Uri is a security researcher at Claroty specializes in reverse engineering and vulnerability research across both embedded and Windows systems.

Description:
We researched the exploitability of cloud-based management platforms responsible for monitoring industrial control systems (ICS), and developed techniques to exploit vulnerabilities in automation vendor CODESYS' Automation Server and vulnerabilities in the WAGO PLC platform. Our research mimics the top-down and bottom-up paths an attacker would take to either control a Level 1 device in order to eventually compromise the cloud-based management console, or the reverse, commandeer the cloud in order to manipulate all networked field devices.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Sunday - 11:30-12:30 PDT

Title: Breaking Future Crypto Custody
When: Sunday, Aug 8, 11:30 - 12:30 PDT
Where: Blockchain Village / Paris Vendome B
Speakers: Mehow Powers,Chris Odom

SpeakerBio: Mehow Powers
No BIO available

SpeakerBio: Chris Odom
No BIO available

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Saturday - 11:30-12:30 PDT

Title: Breaking Historical Ciphers with Modern Algorithms
When: Saturday, Aug 7, 11:30 - 12:30 PDT
Where: Crypto & Privacy Village (Virtual)
Speakers: Elonka Dunin,Klaus Schmeh

SpeakerBio: Elonka Dunin
Elonka Dunin is co-founder of a group working to crack the Kryptos sculpture at CIA Headquarters, and a member of the National Cryptologic Foundation’s Board of Directors. Bestselling author Dan Brown named a character after her in one of his novels. She maintains popular websites about the world's most famous unsolved codes, and her publications include the book with Klaus Schmeh, "Codebreaking: A Practical Guide”, as well as a Cryptologia paper on Playfair cipher world records. She has also developed award-winning games at companies such as Simutronics.

SpeakerBio: Klaus Schmeh
Klaus Schmeh is the most-published cryptology author in the world. He has written 15 books about the subject, as well as over 200 articles, 25 scientific papers, and 1,400 blog posts. His blog "Cipherbrain" covers codebreaking and crypto history, and he is a member of the editorial board of the scientific magazine Cryptologia. He co-published his latest book "Codebreaking: A Practical Guide" with Elonka Dunin. He is known for his entertaining presentation style involving self-drawn cartoons and Lego models, and he has lectured at hundreds of conferences, including the NSA Cryptologic History Symposium and the RSA Conference. In his day job, Klaus works for a German cryptology company.

Description:
Many old encryption methods are still hard to break today. For instance, cryptanalyzing a short 19th century Playfair cipher is far from trivial. WW2 Enigma messages, spy ciphers from the Cold War, and manual methods used by criminals such as the Zodiac Killer can also be challenging, especially when the ciphertexts are short. On the other hand, techniques for breaking historical ciphers have recently made considerable progress. Computer-based cryptanalysis methods such as hill climbing and simulated annealing have been successfully applied to break original WWII Enigma messages, as well as one of the world's most famous unsolved codes, a 1970 ciphertext sent by the Zodiac Killer. The record in solving short Playfair messages has improved: whereas many years ago the shortest Playfair ciphertext that could be cracked required a minimum of 60 letters, now messages as short as 26 letters have been solved. However, many other historical ciphertexts are still unbroken to date. This presentation will introduce the most important historical ciphers, and modern techniques to break them - based on the 2020 book "Codebreaking: A Practical Guide" authored by the presenters. Many real-world examples will be provided, with slides that use an entertaining style including Lego brick models, self-drawn cartoons, and animations.

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 15:00-15:59 PDT

Title: Breaking Secure Bootloaders
When: Saturday, Aug 7, 15:00 - 15:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Christopher Wade
Christopher is a seasoned security researcher and consultant. His main focuses are in reverse engineering hardware, fingerprinting USB vulnerabilities and playing with Software Defined Radios, with his key strength lying in firmware analysis, which he utilizes as part of the hardware testing team at Pen Test Partners.
Twitter: @Iskuri1
https://github.com/Iskuri

Description:

Bootloaders often use signature verification mechanisms in order to protect a device from executing malicious software. This talk aims to outline actionable weaknesses in modern bootloaders which allow attackers to deploy unsigned code, despite these protection mechanisms.

In the first phase of this talk, we will discuss exploitation of the bootloaders in modern Android smartphones, demonstrating weaknesses which allow for bypassing bootloader unlocking restrictions, decryption of protected user data, and deployment of malicious software to devices using full disk encryption.

In the second phase, we will discuss bootloader weaknesses in the secondary hardware used by smartphones. Using an embedded RF chip as a target, we will demonstrate reverse engineering techniques which identified weaknesses in the signature verification mechanisms of the firmware update protocols used by the bootloader, allowing for deployment of custom firmware to the chip.

REFERENCES

> Travis Goodspeed - Great Ideas in Reversing the Tytera MD380:
> https://nullcon.net/website/archives/ppt/goa-16/Great-Ideas-in-Reversing-the-Tytera-MD380-by-Travis-Goodspeed.pdf
> Roee Hay - fastboot oem vuln: Android Bootloader Vulnerabilities in Vendor Customizations:
> https://www.usenix.org/system/files/conference/woot17/woot17-paper-hay.pdf

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=z4gIxdFfJDg

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20C

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

Title: Breaking TrustZone-M: Privilege Escalation on LPC55S69
When: Sunday, Aug 8, 12:00 - 12:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Laura Abbott,Rick Altherr

SpeakerBio: Laura Abbott
Laura Abbott is a software engineer who focuses on low level software. Her background includes Linux kernel development with work in the memory management and security areas as well as ARM enablement.
Twitter: @openlabbott

SpeakerBio: Rick Altherr
Rick Altherr has a career ranging from ASICs to UX with a focus on the intersection of hardware and software, especially in server systems. His past work includes USBAnywhere, leading the unification of OpenBMC as a project under Linux Foundation, co-authoring a whitepaper on Google's Titan, and reverse engineering Xilinx 7 Series FPGA bitstreams as part of prjxray.
Twitter: @kc8apf

Description:

The concept of Trusted Execution Environments has been broadly introduced to microcontrollers with ARM's TrustZone-M. While much experience with TrustZone-A can be applied, architectural differences with ARMv8-M lead to a very different approach to configuration and transitions between secure and non-secure worlds. This talk will deep dive into how TrustZone-M works, where to look for weaknesses in implementations, and a detailed look into NXP LPC55S69's implementation including discovering an undocumented peripheral that leads to a priviledge escalation vulnerability exploitable with TrustedFirmware-M. Finally, NXP PSIRT will be used as a case study in how not to respond to a vulnerability report.

REFERENCES

> TrustZone technology for the ARMv8-M architecture Version 2.0; ARM;
> https://developer.arm.com/documentation/100690/0200

Your Peripheral Has Planted Malware -- An Exploit of NXP SOCs Vulnerability; Yuwei Zheng, Shaokun Cao, Yunding Jian, Mingchuang Qin; DEFCON 26; https://media.defcon.org/DEF CON 26/DEF CON 26 presentations/DEFCON-26-Yuwei-Zheng-Shaokun-Cao-Bypass-the-SecureBoot-and-etc-on-NXP-SOCs-Updated.pdf

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=eKKgaGbcq4o

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20L

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 12:00-12:59 PDT

Title: Bring Your Own Print Driver Vulnerability
When: Saturday, Aug 7, 12:00 - 12:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Jacob Baines
Jacob is a vulnerability researcher at Dragos. He enjoys focusing much of his research time on routers and other embedded devices. Occasionally, he finds himself looking at Windows internals. Sometimes he even finds vulnerabilities.

Description:

What can you do, as an attacker, when you find yourself as a low privileged Windows user with no path to SYSTEM? Install a vulnerable print driver! In this talk, you'll learn how to introduce vulnerable print drivers to a fully patched system. Then, using three examples, you'll learn how to use the vulnerable drivers to escalate to SYSTEM.

REFERENCES

> - Yarden Shafir and Alex Ionescu, PrintDemon: Print Spooler Privilege Escalation, Persistence & Stealth (CVE-2020-1048 & more) - https://windows-internals.com/printdemon-cve-2020-1048/ - voidsec, CVE-2020-1337 – PrintDemon is dead, long live PrintDemon! - https://voidsec.com/cve-2020-1337-printdemon-is-dead-long-live-printdemon/ - Zhipeng Huo and Chuanda Ding, Evil Printer: How to Hack Windows Machines with Printing Protocol - https://media.defcon.org/DEF CON 28/DEF CON Safe Mode presentations/DEF CON Safe Mode - Zhipeng-Huo and Chuanda-Ding - Evil Printer How to Hack Windows Machines with Printing Protocol.pdf - Pentagrid AG, Local Privilege Escalation in many Ricoh Printer Drivers for Windows (CVE-2019-19363) - https://www.pentagrid.ch/en/blog/local-privilege-escalation-in-ricoh-printer-drivers-for-windows-cve-2019-19363/ - space-r7, Add module for CVE-2019-19363 - https://github.com/rapid7/metasploit-framework/pull/12906 - Microsoft, Point and Print with Packages - https://docs.microsoft.com/en-us/windows-hardware/drivers/print/point-and-print-with-packages - Microsoft, Driver Store - https://docs.microsoft.com/en-us/windows-hardware/drivers/install/driver-store - Microsoft, Printer INF Files - https://docs.microsoft.com/en-us/windows-hardware/drivers/print/printer-inf-files - Microsoft, Use Group Policy settings to control printers in Active Directory - https://docs.microsoft.com/en-us/troubleshoot/windows-server/printing/use-group-policy-to-control-ad-printer

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=vdesswZYz-8

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20J

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 14:00-15:30 PDT

Title: BTV Presents: Forensics Station - Workshop 1
When: Saturday, Aug 7, 14:00 - 15:30 PDT
Where: Blue Team Village - Workshop Track 2 (Virtual)

SpeakerBio: Omenscan
I do stuff. Sometimes it works.

Description:

Forensics Station - Workshop 1
A walkthrough of triaging "compromised" Capstone servers.

In this workshop we will walk through a quick forensic triage of the "compromised" BTV Capstone servers.

Capstone is a Blue Team Village initiative to build and attack servers (and workstations) in a controlled environment, using common attacker techniques and tools in a safe way. We then use common Blue Team defender tools to gather information and review those machines, in order to train defenders on detecting, handling, and understanding common attacks.

This is the forensics workshop, and it will cover forensic triage. It's goal is to quickly answer some basic questions like:

Did Something Happen?
If So, When Did it Happen?
What Artifacts Can Help Us?
What Forensic Tools Can Help Us?
What Should We Look at Next?

The Capstone Project will provide the Telemetry and Artifacts to the community so they can use their own tools to explore the data and share findings. We encourage everyone at every level to participate and share findings - so everyone can learn and collaborate.

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 11:00-12:30 PDT

Title: BTV Presents: Malware Station - Maldoc Workshop
When: Saturday, Aug 7, 11:00 - 12:30 PDT
Where: Blue Team Village - Workshop Track 2 (Virtual)

SpeakerBio: Clay (ttheveii0x)
Clay is a cyber threat intelligence and malware analysis manager at a consulting company.
Twitter: @ttheveii0x

Description:

This workshop covers an overview of maldoc analysis, a demo, and a hands-on section that takes a deep dive into a malicious Excel document. VM, artifact, and guide will be available for attendees to download and follow along. Breaks will be taken after each section to give attendees time to work through the section and ask questions.

Attendees will be exposed to a number of different tools including...

REMnux
DnSpy
oletools
CyberChef
xlmdeobfuscator
shell2exe
EXCELntDonut
Invoke-Obfuscation

Target audience

SOC analysts
Forensic investigators and junior malware analysts Red team/pen testers
Anyone interested in the topic

Return to Index - Add to Google Calendar - ics Calendar file

Title: BTV Presents: Threat Report Roulette

When: Sunday, Aug 8, 10:00 - 10:59 PDT

Where: Blue Team Village - Main Track (Virtual)

Speakers: Blind Hacker JoeB,Will Thomas,Ricky Banda,Karan Aditya Ghoshal,Danny D. Henderson Jr,Christopher Russell,Jorge Orchilles,Ch33r10

SpeakerBio: Blind Hacker JoeB
The Blind Hacker is an InfoSec enthusiast, mentor, coach, pentester, hacker, and more. He regularly mentors online through streams and online communities. He frequently volunteers time on workplace development for others, gives resume reviews, job advice, and coaches people into the roles they want with mock interviews. As a person with a disability, or who is differently-abled, he has never let it slow him down.
Twitter: @TheBlindHacker

SpeakerBio: Will Thomas
Will Thomas is a security researcher at Cyjax, a UK-based Cyber Threat Intelligence vendor. In his spare time, he offers his OSINT skills to work missing persons cases with the NCPTF and is a board member of the Curated Intelligence trust group. Will graduated with a BSc (Hons) in Computer and Information Security from the University of Plymouth.
Twitter: @BushidoToken

SpeakerBio: Ricky Banda
Ricky Banda is a Incident Commander for the Amazon Security Incident Response Team. He is a SANS MSISE Graduate Student, with over a dozen industry certifications and featured author in Tribe of Hackers: Blue Team Edition. He has over a decade of experience in Security Operations and Incident Response working in both Public and Private sectors.
Twitter: @teck923

SpeakerBio: Karan Aditya Ghoshal
Karan Aditya Ghoshal is a CTI Analyst at a Big Four cybersecurity firm. He is currently pursuing his Bachelors in Computer Science Engineering at Manav Rachna University.
Twitter: @0xDISREL

SpeakerBio: Danny D. Henderson Jr
Danny Henderson Jr. is a USAF veteran who is now an expat working as a Senior Cybersecurity Analyst at SecureWorks in Romania. He is a graduate of Capitol Technology University with MSc in Cyber and Information Security, six GIAC certifications in DFIR and Offensive Security.
Twitter: @B4nd1t0_

SpeakerBio: Christopher Russell
Christopher Russell is the Head of Information Security for tZERO Group Inc. He has a Masters Degree in Cybersecurity and numerous certifications and experience in cloud security, endpoint detection and response, SIEM and blockchain. He is a combat Veteran of the US Army, where he was a human intelligence (HUMINT) collector who graduated from the Defense Language Institute, for Arabic.
Twitter: @cr00ster

SpeakerBio: Jorge Orchilles
Jorge Orchilles is the Chief Technology Officer of SCYTHE, co-creator of the C2 Matrix project, and author of the Purple Team Exercise Framework. He is a SANS Certified Instructor and the author of Security 564: Red Team Exercises and Adversary Emulation.
Twitter: @jorgeorchilles

SpeakerBio: Ch33r10
Xena Olsen, @ch33r10, is a Senior Cybersecurity Analyst at a Fortune 500 Company. She is a graduate of SANS Women's Academy with eight GIAC certifications, an MBA in IT management, and a doctoral student in cybersecurity at Marymount University.
Twitter: @ch33r10

Description:

Follow along as we spin the Threat Report Roulette Wheel and provide rapid fire responses to how we would create actionable takeaways from the publicly available, TLP: White Threat Reports. Pick up some tips and tricks to up your game! Check out our Github with links to the reports: https://github.com/ch33r10/DEFCON29-BTV-ThreatReportRoulette
https://bit.ly/DC29Roulette

Threat Report Roulette will not discuss normal (BAU) CTI actions, such as searching the logs for hits on the IOCs or entering the IOCs into a Threat Intelligence Platform (TIP) or other alerting platform. Instead, the participants will focus on pivoting, TTPs, and how they would take the contents in the Threat Report to the NEXT LEVEL! When the Panelists respond to the threat reports, they are operating under the assumption that they performed the preliminary analysis and deemed the threat report relevant to their environment. The purpose of this assumption is to decrease the amount of debate on whether or not something is relevant to get to the part of the analysis that involves extracting actionable takeaways.

Spin the Threat Report Roulette Wheel - Link Moderator calls on Participant.
Participant is in the Hot Seat:

```
        15 seconds to organize their thoughts.
        1-5 minutes to share their thoughts on how they would get value out of the report.
    Panelists' input:
        3-5 minutes to share their insights as a group. Quick commentary that is short, sweet, rapid
```

Rinse & Repeat!
Check out our Github with links to the reports: https://github.com/ch33r10/DEFCON29-BTV-ThreatReportRoulette
https://bit.ly/DC29Roulette

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: BTV Presents: Welcome to #IRLIFE. A live IR TableTop Panel
When: Sunday, Aug 8, 11:15 - 12:15 PDT
Where: Blue Team Village - Main Track (Virtual)
Speakers: Clay (ttheveii0x),plug,Ch33r10,Bassem Helmy,Wayland,O'Shea (sirmudbl00d),Ben (Innismir),Tino aka Paladin316,Neumann (aka scsideath)

SpeakerBio: Clay (ttheveii0x)
Clay is a cyber threat intelligence and malware analysis manager at a consulting company.
Twitter: @ttheveii0x

SpeakerBio:plug
Plug started his journey in computer security back in 1996 when he discovered a 2600 magazine that eventually lead him to his first LA2600 meeting in 1998. From that point forward, he has been involved in computer security. Plug currently leads the Threat Hunting Program for a Fortune 20 organization. In his free time he enjoys building Legos, playing with synthesizers, and when possible, he volunteers his time to computer security events.

SpeakerBio: Ch33r10
Xena Olsen, @ch33r10, is a Senior Cybersecurity Analyst at a Fortune 500 Company. She is a graduate of SANS Women's Academy with eight GIAC certifications, an MBA in IT management, and a doctoral student in cybersecurity at Marymount University.
Twitter: @ch33r10

SpeakerBio: Bassem Helmy
Cyber Security Professional with over eleven (11) years of experience with corporates and multinational organizations throughout the Middle East. Awarded Penetration Tester of the Year 2016 from EC-Council Foundation InfoSec Tech & Exec. Area of Expertise:

- Penetration Testing, Red Teaming, and Covert Operations • ICS / SCADA Security Assessment
- Threat Hunting Operations
- Incident Response
- Vulnerability Management and Security Assessment

Twitter: @bh3lmy

SpeakerBio: Wayland
Wayland is a cyber security practitioner with more than a decade of experience performing incident response in a variety of organizational environments. He has contributed to response efforts for multiple significant matters over the years and of late is focused on mentoring and leading the next wave of incident response professionals.
Twitter: @notx11

SpeakerBio:O'Shea (sirmudbl00d)
O'Shea Bowens is a cyber security enthusiast with 12years of experience. He is the founder and CEO of Null Hat Security which offers consulting services and addresses the cyber workforce shortage with skills and gap assessments in a custom built cyber arena. He is knowledgeable in the areas of digital forensics & incident response, threat hunting, cloud security, security analytics, security program management and architecture.
Twitter: @SirMuDbl00d

SpeakerBio: Ben (Innismir)
Ben is a security practitioner with over 15 years of hands on cyber security experience. Since 2011, Ben has been a CSIRT lead for a Fortune 500 company. In his spare time, he enjoys being a husband and dad, messing around with computers, VoIP,

analog telephones, amateur radio, and generally pressing anything with a button on it. Ben was the lead author for Asterisk Hacking from Syngress Publishing, has spoken at various industry conferences, and has been featured on the BBC, New York Times, and CNET. Ben also strongly dislikes writing about himself in the third person.
Twitter: @innismir

SpeakerBio:Tino aka Paladin316

Tino has over 25 years experience in Cyber Security. His work experience spans diverse industries, a world-renowned children's hospital, a world leading Energy Company, an enterprise application service provider, a fortune 100 global manufacturing company, and a Global Financial Services Institution. His primary experience involves developing and implementing processes for Cyber Threat Hunting, Malware Analysis/Reverse Engineering, Digital Forensics/Incident Response (DFIR), and Purple Teaming. In addition, his favorite hobby is doing Cyber Security Research. He says he would do this job for free, but don't tell anyone.
Twitter: @Paladin3161

SpeakerBio:Neumann (aka scsideath)

Neumann Lim is a senior manager at Deloitte where he leads the development of the services, strategies and methodologies on cyber detection and incident response. With more than 14 years of infosec experience, he has coordinated national incident responses across multiple industries. Prior to this role, Neumann spent several years working with large enterprises and governments specializing in incident response.
Twitter: @cybersyrupblog

Description:

In this live table top, a group of panelist will be asked for their opinion on how to deal with a fictitious security incident as it unfolds. Live audience will be encourage to submit questions. Regardless of your skill level, this fun panel will take you in a day in IRLIFE!

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Bug bounty Hunting Workshop
When: Saturday, Aug 7, 10:00 - 13:59 PDT
Where: Workshops - Las Vegas 1+2 (Onsite Only)
Speakers: David Patten,Philippe Delteil

SpeakerBio: David Patten
No BIO available

SpeakerBio: Philippe Delteil , Computer Science Engineer
Philippe Delteil is Computer Science Engineer from the University of Chile, he gave his first talk at Defcon 26 Skytalks, called "Macabre stories of a hacker in the public health sector", his country's government sent 3 officials to record the talk, they did. He's been reporting bugs for a year. He's an annoying github issue opener of some opensource tools like axiom, nuclei, dalfox and bbrf; also makes small contributions to 'Can I take Over XYZ?'

Description:

Bug bounty hunting is (probably) the most hype topic in the hacking subworld, some people read amazing stories of how a 18 years old won 1 million dollars only doing legal hacking. Many hit a wall when they realize that after two months they only won points, thanks or cheap swag. Where's the money?, they ask. What should I learn and how? How many books should I read? How many minutes of Youtube tutorials? What if I lose some weight? [always recommended] How can I be the next bug bounty millionare? In this workshop I will show you a path to be a bug bounty hunter, from my experience starting by chance and from scratch. I will teach you how to use the tools I use everyday to find bugs, but most importantly how to see bug bounty hunting as a complex business process .

What to know before
- Basic idea of bugs (and bounty hunting) - Basic Linux commands (sed, awk, grep) - Shell scripting basics
- Have some practice doing recon

What you will learn
- How bug bounty programs/platforms work - What tools hunters use and how do they work - How to hunt for bugs (hopefully for profit) - Automatization of your hunting process

How technical is the class
- 30% theory and concepts
- 70% Installing, configuring and using tools to find bugs. Send some reports if we are lucky.

What tools are we going to use
- Scanners/automated tools: nuclei, axiom, bbrf, dalfox, Burp. - Recon tools (subfinder, amass, assetfinder, waybackurls, httpx and more)

What to read/watch in advance
- Books

- The Web Application Hacker's Handbook, 2nd Edition
- Hands-On Bug Hunting for Penetration Testers (Joseph E. Marshall)
- Web Hacking 101 (Peter Yaworski) - Videos
- Live Recon and Distributed Recon Automation Using Axiom with @pry0cc (https://bit.ly/3gPsonz) The Bug Hunter's Methodology Full 2-hour Training by Jason Haddix (https://bit.ly/2PzHUsr)
- Finding Your First Bug: Choosing Your Target by InsiderPhD (https://bit.ly/3uiF3n7)
- HOW TO GET STARTED IN BUG BOUNTY (9x PRO TIPS) by STÖK (https://bit.ly/3u81U4m)

Registration Link: https://www.eventbrite.com/e/bug-bounty-hunting-workshop-tickets-162219297285

Prerequisites

Basic knowledge about Bug bounty programs Basic Linux Commands

Materials needed:
Laptop with Kali Linux (native or virtual machine).

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Friday - 14:00-14:59 PDT

Title: Bug Hunter's Guide to Bashing for a Car Hacking Bug Bash or Contest
When: Friday, Aug 6, 14:00 - 14:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Jay Turla , Manager, Security Operations at Bugcrowd
Jay Turla is a Manager, Security operations at Bugcrowd Inc., and one of the goons of ROOTCON. He has been acknowledged and rewarded by Facebook, Adobe, Yahoo, Microsoft, Mozilla, etc. for his responsible disclosures. He has also contributed auxiliary and exploit modules to the Metasploit Framework: Host Header Injection Detection, BisonWare BisonFTP Server Buffer Overflow, Zemra Botnet CnC Web Panel Remote Code Execution, Simple Backdoor Shell Remote Code Execution, w3tw0rk / Pitbul IRC Bot Remote Code Execution, etc. He used to work for HP Fortify where he performs Vulnerability Assessment, Remediation and Advance Testing.

Description:

Bug Bounty Programs and Bug Bashes geared towards vehicles or automobiles are getting attention now. A lot of our brethren have also been wining some of these competitions. What is their secret to their success? How do you prepare for one? This talk will summarize some techniques and methodologies the speaker observed during his stint as a triager for automotive security bugs and a common car hacker. This talk will also be an eye opener for other bug hunters who wants to dive into car hacking so that they may be able to participate car hacking bug bashes soon.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=5-JM1QRGUYc

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Saturday - 14:00-14:59 PDT

Title: Build Automotive Gateways with Ease
When: Saturday, Aug 7, 14:00 - 14:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Don Hatfield
No BIO available

Description:
Vehicle network architectures within modern vehicles have been transformed by the introduction of automotive gateways. These gateways enable seamless communication between different vehicle networks and are central to the success of modern architectures. In this presentation, we are going to cover some of the challenges that automotive engineers face when tasked with converting data between old and new network protocols. We’ll also detail how this process is made much easier.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=3elYcORppls

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Sunday - 13:30-13:59 PDT

Title: Building an ICS Firing Range (in our kitchen): Sharing Our Journey & Lessons Learned (so you don’t have to)
When: Sunday, Aug 8, 13:30 - 13:59 PDT
Where: ICS Village (Virtual)
Speakers: Moritz Thomas,Nico Leidecker

SpeakerBio: Moritz Thomas , NVISO
Moritz is a security consultant working in the NVISO Software and Security assessment team. He is an ICS and IoT enthusiast, getting into the latest technologies in both fields. He loves to program and reverse engineer stuff.

SpeakerBio: Nico Leidecker , NVISO
Nico has worked in IT security for over 15 years as security consultant and penetration tester. For the past two years, his focus has been on all several aspects of OT security. At NVISO Germany, he leads the security assessment team.

Description:

Aiming to improve our own expertise in ICS security, we went to build our own ICS firing range for internal and external trainings, and hacking demos. It covers multiple technical aspects about IT infrastructure, PLC configuration and programming, ICS protocols and specific methodologies for red and blue teaming. Beginning with a bridge operation scenario we planned our approach on implementing the ICS Firing Range addressing all levels of the Purdue Model, from enterprise to physical processes. We were faced with a variety of practical challenges and challenges specific to the ICS context and prototyping: we learned how to implement ladder logic, how CAD modelling works, how to print 3D models with a 3D printer and how to combine all ICS and bridge components into a single, confined and mobile lab environment. Lastly, we designed a series of kill chains for our firing range that we use for trainings on a variety of professions such as digital forensics and incident response.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 16:00-16:45 PDT

Title: Bundles of Joy: Breaking macOS via Subverted Applications Bundles
When: Friday, Aug 6, 16:00 - 16:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Patrick Wardle
Patrick Wardle is the founder of Objective-See. Having worked at NASA and the NSA, as well as presenting at countless security conferences, he is intimately familiar with aliens, spies, and talking nerdy. Patrick is passionate about all things related to macOS security and thus spends his days finding Apple 0days, analyzing macOS malware, and writing free open-source security tools to protect Mac users.
Twitter: @patrickwardle
https://objective-see.com/

Description:
A recent vulnerability, CVE-2021-30657, neatly bypassed a myriad of foundational macOS security features such as File Quarantine, Gatekeeper, and Notarization. Armed with this capability attackers could (and were!) hacking macOS systems with a simple user (double)-click. Yikes!

In this presentation we'll dig deep into the bowels of macOS to uncover the root cause of the bug: a subtle logic flaw in the complex and undocumented policy subsystem. Moreover, we'll highlight the discovery of malware exploiting this bug as an 0day, reversing Apple's patch, and discuss novel methods of both detection and prevention.

REFERENCES

> "All Your Macs Are Belong To Us" https://objective-see.com/blog/blog_0x64.html "macOS Gatekeeper Bypass (2021 Edition)" https://cedowens.medium.com/macos-gatekeeper-bypass-2021-edition-5256a2955508 "Shlayer Malware Abusing Gatekeeper Bypass On Macos" https://www.jamf.com/blog/shlayer-malware-abusing-gatekeeper-bypass-on-macos/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=raSTgFqYaoc

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20P

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

Title: C2Centipede: APT level C2 communications for common reverse HTTP shell tools
When: Saturday, Aug 7, 17:15 - 18:15 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Jose Garduno , Senior Security Consultant, Dreamlab Technologies AG
José Garduño is a senior security consultant at Dreamlab Technologies since 2014, where he usually takes part in security audits, pentesting and red teaming engagements. He has participated as a speaker in several technical conferences like: Hackito Ergo Sum (France), Swiss Cybersecurity days (Switzerland), DSS ITSEC (Latvia), 8.8 Security Conference (Chile, Bolivia), OWASP Patagonia (Argentina), Congreso Seguridad en Computo UNAM (Mexico), DragonJar Security Conference (Colombia), where he has presented his work on privacy attacks on Latin-America (The government as your hacking partner), Hacking with open hardware platforms (revisiting hardware keyloggers, say hi to mikey: an offensive hardware keylogger) and C2 detection (RATSPOTTING: Analysis of popular Remote Administration Tools & discovery of C2 servers on the wild)

Description:

Adversaries have been continuously improving their malware to be stealthier and more resilient on both the victim's host as well as on the network.Examples of these innovations on the latter include Fast Flux networks, Domain Generation Algorithms and Domain Fronting among other techniques.

Unfortunately, open source tools for threat emulation currently have limited support for such advanced features, leaving redteams with easy to detect C2 communications. We present C2Centipede, a proxy tool that provides these features to HTTP reverse shell tools (like Metasploit or Empire) to be stealthier on the network by dynamically and transparently modifying the trojan's C2 communication routing and beaconing strategies, with the aim of evading some of the blueteam's detection strategies.

BEACONING EVASION

Detection of HTTP reverse shell beaconing activity is possible because most of the patterns on which malware sends the beacons through the network can be identified as they occur in static time intervals or are adjusted in specific increments, attributes which are possible to detect using statistical analysis.[1]

For instance, Metasploit's reverse_http meterpreter sends a message to the C2 server every 100 milliseconds and increases the interval by this same measure each time the C2 server gives no new jobs to the trojan, up to a maximum of 10 seconds.[2]

It is easy then for tools like RITA to perform statistical analysis on the number, timing and size of connections between pairs of hosts (source, destination)[3]. This IP-pair evaluation works in the most typical approach of having only one IP per C2 server. We implement a beaconing detection evasion method that works by 1) Altering the trojan's C2 communication message interval and 2) Splitting and routing the C2 communication among many C2 server addresses to hide beaconing and exfiltration.

JITTER MODIFICATION

The Achille's heel of most RAT (Remote Access Trojan) and TES (Threat Emulation Software) tools network stealthiness is fixed beaconing intervals. The time interval between each message that goes to the C2 server is usually hardcoded and just too short, making manyrequests across the network, so we have incorporated in the tool, better control of the beaconing, with the possibility of modifying the jitter on the fly or having preset configurations, like allowing C2 communication just on certain time window.

Some RAT/TES tools will fail after a specific amount of unsuccessful C2 communication attempts, so the C2Centipede proxy client cannot just drop the HTTP calls that don't fit the operator's beaconing strategy, therefore fake C2 response messages are generated in order to keep the trojan alive.

FAUX FLUX

The concept of Fast Flux networks as a technique to improve a botnet's C2 availability has been in use since 2007-2008.[4] Using this technique, an attacker can hide the real C2 server behind proxies (which are usually compromised edge servers in a botnet), and distributing said proxies IPs through DNS records with a very low TTL[5], allowing them to rapidly (and thus the name fast flux) change the resolved IP for a given domain name. This results in making the shutdown of each C2 IP so difficult as to be usually compared to a whack a mole game.[4] The weakness of this approach is the reliance on a domain name[5], which can be sinkholed by the domain name registrar, as in the case of the shutdown of the Conficker botnet.[4] Some of the common detection methods for Fast Flux networks is the low TTL (time to live) of the record and a high number of IPs resolved for that record.[3]

We have incorporated the C2 proxying technique without the DNS and botnet requirements by utilizing open reverse tcp/http tunnels found on the internet, which provide plenty of IP addresses on which we can spread our C2 comms and provide anonymity as the real C2 server is hidden behind the reverse proxy. In our most recent internet-wide survey we found more than 1.5K servers that could be abused for this purpose

MULTIFRONTING

Domain fronting (ATT&CK T1090.004) is a widely used technique for evading network detection. This technique hides the trojan's HTTP requests to the C2 as if it was directed to another domain hosted on the same Content Delivery Network (CDN) as the attacker's. Without TLS inspection, where a mismatch between TLS's SNI and the HTTP header could be detected, it becomes very hard for the defenders to detect malicious traffic using this technique, having as a last resource the detection via statistical analysis like beaconing detection.

C2Centipede has the ability to utilize multiple domain fronting configurations, which are not necessarily on the same CDN, this provides additional resilience in case one of the CDN providers blocks the redteamer's account.

DOMAIN GENERATION ALGORITHMS

We have incorporated Flubot's algorithm for Domain Generation Algorithm (ATT&CK: T1568.002). The seed, and maximum number of domains generated are easily configurable.

DYNAMIC PROXY CONFIGURATION

C2Centipede's configuration on the server and client can be modified on the fly by the operator. The original trojan's and C2 messages are wrapped in the tool's own HTTP messages along with the configuration changes of the routing, jitter and encryption settings for the c2centipede client and server. These are piggybacked on the original HTTP requests, requiring no additional "noise" in the network.

LIMITATIONS

The tool currently works with reverse HTTP shells that close the TCP connections (eg. Metasploit, Empire) and currently does not support those with long connections (eg. PoshC2, Koadic)

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

ASV - Saturday - 09:00-16:59 PDT

Title: California Cyber Innovation Challenge CTF -- Pre-registration Required
When: Saturday, Aug 7, 09:00 - 16:59 PDT
Where: Aerospace Village (Virtual CTF)

Description:

Cal Poly

Starts August 7, 2021@ 9 AM PST,
Ends Aug 8, 2021 5 PM PST

Registration available at
https://www.cognitoforms.com/CCI17/CaliforniaCyberInnovationChallengeAEROSPACEVILLAGEDEFCON2021

The CCIC promotes Gamification & Esports for Space and Cybersecurity Skills Development. This is an electronic game of clue that has characters and threat actors or the person(s) who committed the Space and Cyber crime. Find the person(s) of interest that you think committed the crime. You are Cybernauts and Cyber Sleuth Analysts. Remember, throughout the challenge, record and take notes of all information, findings, evidence, and clues regarding characters you encounter. Take note of technical skills you executed to create a digital forensics analysis report of who committed the crime and their motives.

About the Crime:

A multi-billion dollar company led by CEO, William Gecko, Moonshot Satellite's constellation of 5000 CubeSat's, located in Low Earth Orbit (LEO), provides a mesh-network of internet access to over 20 million commercial and governmental customers around the globe. Moonshot Satellite, a small cube satellite company whose constellation satellite infrastructure provides communication services that deliver Internet access to over 200 million individual commercial customers and real-time communications support for numerous government agencies.

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Saturday - 11:20-11:50 PDT

Title: Can I Make My Own Social Threat Score?
When: Saturday, Aug 7, 11:20 - 11:50 PDT
Where: Recon Village (Virtual)

SpeakerBio: MasterChen
No BIO available
Twitter: @chenb0x

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 17:00-17:45 PDT

Title: Can’t Stop the Code: Embrace the Code
When: Saturday, Aug 7, 17:00 - 17:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Alton Crossley
No BIO available

Description:
You can't stop the code. So how do you make it all secure? The answer is: you don't. Let's discuss securing your software while using proprietary third parties and Open Source without disrupting ecosystems or innovation.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Sunday - 12:00-12:45 PDT

Title: Car Hacking + Bug Hunting Field Guide for Appsec Hackers
When: Sunday, Aug 8, 12:00 - 12:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Jay Turla DELETE ME
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-23:55 PDT

Title: Car Hacking CTF
When: Friday, Aug 6, 10:00 - 23:55 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236495

Return to Index - Add to Google Calendar - ics Calendar file

CAHV - Saturday - 14:00-14:59 PDT

Title: Career Hacking: Tips and Tricks to Making the Most of your Career
When: Saturday, Aug 7, 14:00 - 14:59 PDT
Where: Career Hacking Village (Talk)

SpeakerBio: Andy Piazza
No BIO available

Description:

At some point in your infosec career, you’ll hit a point of “now what?”. You may experience this as soon as you land your first role, or you’ll experience it as a seasoned veteran of the field. There are plenty of talks out there now for “getting into infosec”, but where is the advice for managing and maintaining a career? This is my attempt to fill that gap. This talk will discuss several key areas for building an awesome career, including actionable takeaways for becoming a better analyst, teammate, and leader. Most importantly, I’ll break down the How and Why behind each concept presented and include specific examples based on real experiences.

This talk will be available on YouTube: https://www.youtube.com/watch?v=oozqj7axNYM

Career Hacking Village content will be available on YouTube.

YouTube: https://youtube.com/careerhackingvillage

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Friday - 13:00-13:59 PDT

Title: Catching (and Fixing) an Unlimited Burn Vulnerability
When: Friday, Aug 6, 13:00 - 13:59 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Nadir Akhtar , Blockchain Security Engineer, Coinbase
Blockchain security engineer @ Coinbase with deep expertise in digital asset security vulnerabilities https://blog.coinbase.com/securing-an-erc-20-token-for-launch-on-coinbase-68313652768f Former President, Blockchain @ Berkeley edX Blockchain Fundamentals curriculum developer and lecturer

Nadir Akhtar is a Blockchain Security engineer at Coinbase, where he leads security reviews of assets under consideration for Coinbase listing. Previously at Quantstamp, he audited smart contracts and contributed to a book on smart contract security fundamentals. He graduated from UC Berkeley in 2019 with a degree in Computer Science. During his time in Blockchain at Berkeley, he was President and an instructor for the UC Berkeley-endorsed blockchain fundamentals edX course series, reaching over 225,000 enrolled students to date.

Description:

Bitcoin, Ethereum, and more blockchains come with an infamous storage problem: taking up too much space on miners' hard drives. In response, protocols are implementing novel methods for reducing the size of the blockchain, often deleting accounts beneath a certain balance. DOT provides a case study of the financial consequences to exchanges of pruning account data.

In this talk, you'll learn about Polkadot's reaping mechanism and its implications for exchanges and other organizations managing DOT at scale. We'll dive into the "Existential Deposit," understanding its motivation for existing in the network as well as the implications of pruning account data below a certain threshold, namely replay attacks.

We'll discover how replay attacks can be performed, as well as their consequences through a demonstration along with some protocol-level mitigations. We'll discuss how naively reaping accounts can still expose exchanges to attacks, investigate potential but infeasible mitigations, then finally reveal the solution which Coinbase discovered for protection against replay attacks.

Finally, we'll examine some final edge cases which arose from the final solution, demonstrating that protecting against attacks may not be perfect but significantly improves our defenses.

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 11:00-11:59 PDT

Title: Caught you - reveal and exploit IPC logic bugs inside Apple
When: Friday, Aug 6, 11:00 - 11:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Chuanda Ding,Yuebin Sun,Zhipeng Huo

SpeakerBio: Chuanda Ding
Chuanda Ding is a senior security researcher on Windows platform security. He leads EcoSec team at Tencent Security Xuanwu Lab. He was a speaker at Black Hat Europe 2018, DEF CON China 2018, CanSecWest 2017, CanSecWest 2016, and QCon Beijing 2016.
Twitter: @FlowerCode_

SpeakerBio: Yuebin Sun
Yuebin Sun is a senior security researcher at Tencent Security Xuanwu Lab.
Twitter: @yuebinsun2020

SpeakerBio: Zhipeng Huo
Zhipeng Huo is a senior security researcher on macOS and Windows platform security at Tencent Security Xuanwu Lab. He was a speaker at Black Hat Europe 2018 and DEF CON 28.
Twitter: @R3dF09

Description:

Apple's iOS, macOS and other OS have existed for a long time. There are numerous interesting logic bugs hidden for many years. We demonstrated the world's first public 0day exploit running natively on Apple M1 on a MacBook Air (M1, 2020). Without any modification, we exploited an iPhone 12 Pro with the same bug.

In this talk, we will show you the advantage and beauty of the IPC logic bugs, how we rule all Apple platforms, Intel and Apple Silicon alike, even with all the latest hardware mitigations enabled, without changing one line of code. We would talk about the security features introduced by Apple M1, like Pointer Authentication Code (PAC), System Integrity, and Data Protection. How did they make exploiting much harder to provide better security and protect user's privacy. We will talk about different IPC mechanisms like Mach Message, XPC, and NSXPC. They are widely used on Apple platforms which could be abused to break the well designed security boundaries.

We will walk you through some incredibly fun logic bugs we have discovered, share the stories behind them and methods of finding them, and also talk about how to exploit these logic bugs to achieve privilege escalation.

REFERENCES

https://www.youtube.com/watch?v=Kh6sEcdGruU https://support.apple.com/en-us/HT211931
https://support.apple.com/en-us/HT211850 https://support.apple.com/en-us/HT212011
https://support.apple.com/en-us/HT212317 https://helpx.adobe.com/security/products/acrobat/apsb20-24.html
https://helpx.adobe.com/security/products/acrobat/apsb20-48.html
https://helpx.adobe.com/security/products/acrobat/apsb20-67.html

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=oAMZxKsZQp0

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20Z

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 15:00-15:45 PDT

Title: Central bank digital currency, threats and vulnerabilities
When: Saturday, Aug 7, 15:00 - 15:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Ian Vitek
Ian Vitek has a background as a pentester but has worked with information security in the Swedish financial sector the last 10 years. Currently working with security of the Swedish retail central bank digital currency prototype at the Riksbank, the Swedish central bank. Interested in web application security, network layer 2 (the writer of macof), DMA attacks and local pin bypass attacks (found some on iPhone).

Description:

What are the threats and vulnerabilities of a retail central bank digital currency (CBDC)? The central bank of Sweden has built a prototype of a retail CBDC system and I will run through the procurement requirements and design and point out where a two-tier CBDC need protection against attacks. The prototype is built on Corda Token SDK and I have during tests found reliable ways to exploit weaknesses in the design. The presentation will focus on the vulnerabilities that can crash the service that handles the tokens and permanently lock tokens rendering tokens and digital wallets useless. The presentation will also go into detail how tokens are validated and how information from all earlier transactions is needed for this. With D3.js and HTML5 I will visualize the token history (backchain) and describe how this can be a problem with GDPR and the Swedish bank secrecy regulation.

The presentation will end with a summary of identified threats and weaknesses of a two-tier retail central bank digital currency prototype and how to handle them. The goal of the presentation is to give the attendees insight of the security implications, challenges depending on the design and where an attack can be carried out and everything that cannot be missed when designing a CBDC.

REFERENCES

https://www.ingwb.com/media/3024436/solutions-for-the-corda-security-and-privacy-trade-off_-whitepaper.pdf
https://d3js.org/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=-MK0bn3Ys_M

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20I

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Saturday - 13:00-13:30 PDT

Title: Certified Ethereum Professional (CEP) Overview
When: Saturday, Aug 7, 13:00 - 13:30 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Abstrct
Abstrct has spent his quarantine bringing dirty progressive and dancey funk to your living rooms, kitchens, patios, and pools each weekend, but holy heck is he ready to bring the party back to DEF CON proper.

https://soundcloud.com/abstrct/saturday-morning-quarantoons-ep46 https://imgur.com/m5Jcql2
https://twitter.com/Abstr_ct
https://www.twitch.tv/abstr_ct

Twitter: @Abstr_ct

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 09:00-20:59 PDT

Title: Chillout Lounges
When: Sunday, Aug 8, 09:00 - 20:59 PDT
Where: See Description
Speakers:DJ Pie & Darren,Louigi Verona,Merin MC,s1gns of l1fe,Mixmaster Morris

SpeakerBio:DJ Pie & Darren
No BIO available

SpeakerBio: Louigi Verona
No BIO available

SpeakerBio: Merin MC
No BIO available

SpeakerBio:s1gns of l1fe
No BIO available

SpeakerBio: Mixmaster Morris
No BIO available

Description:
There are two onsite chillout lounges available: Bally's Silver Ballroom, and Paris Concorde A.

There will be chill music playing:

09:00-12:00 DJ Pie & Darren
12:00-12:40 s1gns of l1fe
12:40-13:30 Louigi Verona
14:30-16:10 Mixmaster Morris
16:10-Close Merin MC

You can also watch the chill room stream on Twitch.

Twitch: https://www.twitch.tv/defcon_chill

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 09:00-20:59 PDT

Title: Chillout Lounges
When: Saturday, Aug 7, 09:00 - 20:59 PDT
Where: See Description
Speakers:djdead,DJ Pie & Darren,kampf,Rusty Hodge,Merin MC,Brian Behlendorf

SpeakerBio:djdead
No BIO available

SpeakerBio:DJ Pie & Darren
No BIO available

SpeakerBio:kampf
No BIO available

SpeakerBio: Rusty Hodge
No BIO available

SpeakerBio: Merin MC
No BIO available

SpeakerBio: Brian Behlendorf
No BIO available

Description:
There are two onsite chillout lounges available: Bally's Silver Ballroom, and Paris Concorde A.

There will be chill music playing:

09:00-12:00 DJ Pie & Darren
12:00-13:30 kampf
13:30-15:00 Merin MC & Rusty
15:00-18:00 Brian Behlendorf
19:00-21:00 djdead

You can also watch the chill room stream on Twitch.

Twitch: https://www.twitch.tv/defcon_chill

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 09:00-20:59 PDT

Title: Chillout Lounges
When: Friday, Aug 6, 09:00 - 20:59 PDT
Where: See Description
Speakers:djdead,DJ Pie & Darren,kampf,Merin MC,s1gns of l1fe,Mixmaster Morris

SpeakerBio:djdead
No BIO available

SpeakerBio:DJ Pie & Darren
No BIO available

SpeakerBio:kampf
No BIO available

SpeakerBio: Merin MC
No BIO available

SpeakerBio:s1gns of l1fe
No BIO available

SpeakerBio: Mixmaster Morris
No BIO available

Description:

There are two onsite chillout lounges available: Bally's Silver Ballroom, and Paris Concorde A.

There will be chill music playing:

09:00-12:00 DJ Pi & Darren
12:00-12:40 s1gns of l1fe
12:40-14:20 Mixmaster Morris
14:30-17:00 kampf
17:00-18:30 Merin MC
18:30-21:00 djdead

You can also watch the chill room stream on Twitch.

Twitch: https://www.twitch.tv/defcon_chill

Return to Index - Add to Google Calendar - ics Calendar file

DC - Thursday - 09:00-20:59 PDT

Title: Chillout Lounges
When: Thursday, Aug 5, 09:00 - 20:59 PDT
Where: See Description
Speakers:djdead,DJ Pie & Darren,kampf,Rusty Hodge,Louigi Verona,Merin MC

SpeakerBio:djdead
No BIO available

SpeakerBio:DJ Pie & Darren
No BIO available

SpeakerBio:kampf
No BIO available

SpeakerBio: Rusty Hodge
No BIO available

SpeakerBio: Louigi Verona
No BIO available

SpeakerBio: Merin MC
No BIO available

Description:
There are two onsite chillout lounges available: Bally's Silver Ballroom, and Paris Concorde A.

There will be chill music playing:

09:00-12:00 DJ Pi & Darren
12:00-13:30 kampf
13:30-16:00 Rusty Hodge
16:00-16:51ish Louigi Verona
17:30 Merin MC
19:00-21:00 djdead

You can also watch the chill room stream on Twitch.

Twitch: https://www.twitch.tv/defcon_chill

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 11:00-11:59 PDT

Title: Chinese Military Bioweapons and Intimidation Operations: Part III
When: Saturday, Aug 7, 11:00 - 11:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: RedDragon
No BIO available

Description:

Chinese Military Bio Weapons Future State is third in a three part series examining the Chinese military use of biological reagents in a kinetic capacity. The unrestricted warfare strategy outlined in the early 1990's clearly defines this Chinese military initiative. The supply chain, Program 863 and other supporting components of his strategy will be revealed. It is TLP : RED

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 12:30-13:30 PDT

Title: Cloud security for healthcare and life sciences
When: Saturday, Aug 7, 12:30 - 13:30 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio:MIchelle Holko , Innovating at the intersection of biology technology and security at Google
Michelle Holko is a PhD scientist in genomics and bioinformatics, working at the intersection of biology, technology, and security. She currently works with at Google with the healthcare and life sciences cloud team. Prior to joining Google, she was a White House Presidential Innovation Fellow.

Description:

Cloud computing is increasingly used, across sectors, to scale data storage, compute, and services on demand. There are many recent examples of healthcare and life sciences cloud-based projects, including AnVIL for genomics data and the All of Us Research Program for precision medicine research. These cloud implementations include data and analytic workflows that pose added security concerns due to the sensitive nature of the information. This panel will discuss recent use cases highlighting best security practices for cloud computing in healthcare and life sciences.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Sunday - 12:20-13:05 PDT

Title: Cloud Security Orienteering
When: Sunday, Aug 8, 12:20 - 13:05 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Rami McCarthy
Rami McCarthy is a Staff Security Engineer at Cedar (a healthtech unicorn), and a recovering Security Consultant. He spent 3 years at NCC Group where he executed dozens of security assessments and sat on the Cloud Security working group. He was a core contributor to ScoutSuite - a multi-cloud auditing tool (and SaaS offering), and released sadcloud - a tool for Terraforming insecure AWS environments. Rami holds the CCSK, the AWS Certified Security – Specialty, and is completing an MS in information security leadership.
Twitter: @ramimacisabird

Description:
Most of us are not lucky enough to have architected the perfect cloud environment, according to this month's best practices, and without any legacy elements or ""surprise"" assets. Over the course of a career in cloud security, you'll likely find yourself walking into a new environment and needing to rapidly orient yourself to both mitigate the biggest risks and also develop a roadmap towards a sustainable, secure future. As a security consultant, I had the challenge and opportunity to enter blind into a variety of cloud environments. They were across Azure, GCP, and AWS, some well-architected and others organically sprawling, containing a single account/project and hundreds. This gave me a rapid education in how to find the information necessary to familiarize myself with the environment, dig in to identify the risks that matter, and put together remediation plans that address short, medium, and long term goals. This talk will present a cloud and environment agnostic methodology for getting your bearings if tasked with securing a novel cloud environment. We'll learn by applying this to a sample AWS environment in order to cover:

- An archeological guide for where and how to find organizational context
- How to quickly find and kill the most common attack vectors at the perimeter (both network and identity)
- Common architectural and deployment patterns, how to spot them, and their security implications
- What you need to know, what you need to prioritize, and what ""best practices"" aren't worth the squeeze when you're in a crunch.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 07:00-12:15 PDT

Title: Cloud Village CTF - Registration
When: Friday, Aug 6, 07:00 - 12:15 PDT
Where: See Description

Description:

For more information, see https://cloud-village.org/

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 11:00-12:15 PDT

Title: Cloud Village CTF
When: Friday, Aug 6, 11:00 - 12:15 PDT
Where: See Description

Description:
For more information, see https://cloud-village.org/

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-15:59 PDT

Title: CMD+CTRL

When: Friday, Aug 6, 10:00 - 15:59 PDT

Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236481

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 10:00-15:59 PDT

Title: CMD+CTRL
When: Saturday, Aug 7, 10:00 - 15:59 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/236481

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 00:00-23:59 PDT

Title: Coindroids

When: Friday, Aug 6, 00:00 - 23:59 PDT

Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236482

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 15:30-15:55 PDT

Title: Collecting CANs: a Bridge Less Traveled
When: Friday, Aug 6, 15:30 - 15:55 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Peace Barry
Having worked as a Metasploit developer and later as a manager of Metasploit development at Rapid7, Pearce currently keeps busy doing security research at Rumble, Inc. and following advances in space technologies.

Description:

We'll step back a few years to early 2017, when @zombieCraig released the Metasploit Hardware Bridge as a mechanism to allow Metasploit Framework to reach into networks beyond Ethernet. While the now-defunct HWBridge initially focused on automotive targets, some of that tech, including CAN buses and RF transceivers, has commonality in aviation targets. In this talk, we'll cover basic design and use of the HWBridge, how one can use it with CAN and RF transceivers, and what it takes to set it up.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=6nxlqh-m3Jc

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 09:05-09:59 PDT

Title: Colorful AppSec
When: Friday, Aug 6, 09:05 - 09:59 PDT
Where: AppSec Village (Virtual)
Speakers: Luis Gomes,Erez Yalon,Pedro Umbelino,Tanya Janca

SpeakerBio: Luis Gomes
No BIO available

SpeakerBio: Erez Yalon
No BIO available

SpeakerBio: Pedro Umbelino
No BIO available

SpeakerBio: Tanya Janca
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Friday - 12:00-12:59 PDT

Title: Commercial Transportation: Trucking Hacking
When: Friday, Aug 6, 12:00 - 12:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Ben Gardiner
Mr. Gardiner is an independent consultant at Yellow Flag Security, Inc. presently working to secure heavy vehicles at the NMFTA. With more than ten years of professional experience in embedded systems design and a lifetime of hacking experience, Gardiner has a deep knowledge of the low-level functions of operating systems and the hardware with which they interface. Prior YFS Inc. and joining the NMFTA team in 2019, Mr. Gardiner held security assurance and reversing roles at a global corporation, as well as worked in embedded software and systems engineering roles at several organizations. He holds a M.Sc. Eng. in Applied Math & Stats from Queen's University. He is a DEF CON Hardware Hacking Village (DC HHV) and Car Hacking Village (CHV) volunteer.
Twitter: @BenLGardiner

Description:
Join us for a technical review of the how-to of hacking big rig trucks. Included is an overview and introduction to commercial transportation, specifically trucking (tractors and trailers), and its technologies. It will cover the vehicle networks J1939, J1708/J1587 and J2497, how they operate and what they can be used for both intentionally and unintentionally. Several tools for truck hacking are presented and a survey of the public truck attacks are covered. Many tools are introduced and discussed, some are covered with examples. Attendees should leave with a good sense of what are the potentially fruitful areas of technical research into commercial transport cybersecurity and how they can equip themselves to successfully explore those areas. Some exposure to the CAN bus is assumed but no specific experience with commercial transport is needed.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=RzcpZODAJE0

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 10:00-10:59 PDT

Title: Community Roundtable - (De)Criminalizing Hacking Around the Globe
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: Policy (Virtual & SkyView 1)

Description:
In the last 12 months, the Supreme Court has weighed in on the Computer Fraud and Abuse Act, a groundswell of support has arisen in the UK to reform the Computer Misuse Act, and a proposed law in Mexico would have criminalized hacking. In all cases, members of the hacker community had a voice. And with several more upcoming in the next 12 months, our community needs to continue engaging with policymakers so they understand our value to the global security ecosystem.

For virtual access, register here: https://us02web.zoom.us/meeting/register/tZcvd-yqpzkqE9bzjZeppc0bGmvkYjHnwQZN

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 15:30-16:30 PDT

Title: Community Roundtable - 10 years after SOPA: where are we now?
When: Friday, Aug 6, 15:30 - 16:30 PDT
Where: Policy (Virtual)

Description:

Ten years ago the Internet nearly changed forever, with the passage of the SOPA/PIPA bills. Driven by copyright interests, it would have unleashed new powers for individuals and governments to censor speech online. Thanks to the public outrage by enough users, those bills didn't make it into law. But whether it comes cloaked in copyright, privacy, antitrust, or some other initiative, the appetite to control speech still continues to inform Internet policymaking discussions. Will they succeed this time in shaping new law? What happens to the Internet if they do? Come discuss these and other questions with Internet policy practitioners who interact with them daily.

Register here: https://us02web.zoom.us/meeting/register/tZAqdO2tqT0tGdRR1k_xro6MUseFIxMUAuGf

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 11:30-12:30 PDT

Title: Community Roundtable - If only you knew
When: Saturday, Aug 7, 11:30 - 12:30 PDT
Where: Policy (Virtual)

Description:

Regardless of the hat you wear – whether you are a policy person dealing with technology, a tech person reacting to policy, a legal advisor struggling to bridge the two, or a business person looking to keep the lights on in the meantime – you all confront your own challenges and issues. What are the top one or two things you know well about those challenges that you wish everyone else did? Come to this session to meet people wearing different hats than you and share those insights.

Register here: https://us02web.zoom.us/meeting/register/tZAlc-2pqT8uHNARKeSvxvivpQHj3UYH3hwV

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 16:00-16:59 PDT

Title: Community Roundtable - Implementing Cyber Solarium Commission Policy
When: Saturday, Aug 7, 16:00 - 16:59 PDT
Where: Policy (Virtual & SkyView 1)

Description:

Within a year of publication of the Cyberspace Solarium Commission report, at least 25 of its recommendations were passed into law by Congress. Solarium Commission leadership wants to know how to improve their next set of recommendations - such as the Bureau of Cyber Statistics - before they become law, and wants DEF CON's help to do so. Commission staff will present their topics and elicit feedback from you and your fellow hackers to avoid unintended consequences and to strengthen their implementation plans.

For virtual access, register here: https://us02web.zoom.us/meeting/register/tZItdOCsqDouHd3-on_4mXNeaIsDQhq7HEz1

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 13:00-14:59 PDT

Title: Community Roundtable - RANSOMWARE: Combatting Ransomware on a Global Stage / The realities of responding to ransomware

When: Saturday, Aug 7, 13:00 - 14:59 PDT

Where: Policy (Virtual & SkyView 1)

Description:

Part 1:

Ransomware has made front page headlines and taken top stage in policy conversations, with even the US President issuing a letter to CEOs, Congress grilling Colonial Pipeline's CEO, and the president of France committing 1 Billion Euro to fight ransomware in hospitals. While drafting and spreading technical "best practices" have failed to protect critical infrastructure around the world, which public policy levers are best suited to do so?

Part 2:

If it's Tuesday, it must be another ransomware attack. So what is a law-abiding company to do? If they pay, it just encourages the attacks. If they don't, then their business may suffer, or worse. Meanwhile, breach-notification regulation may have started a ticking clock forcing their hand – potentially in ways that are counter-productive to other policy efforts to stem the tide of these attacks. In this session we'll confront the practical realities and policy dilemmas these attacks provoke.

For virtual access, register here: https://us02web.zoom.us/meeting/register/tZYvduuorzgtG9MAPy9QjVRAaaC4JKIu89aq

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 10:00-10:59 PDT

Title: Community Roundtable - Supply Chain in the COVID Era
When: Saturday, Aug 7, 10:00 - 10:59 PDT
Where: Policy (Virtual & SkyView 1)

Description:

During the global COVID pandemic, accidents and adversaries revealed opaque and ignored supply chain security issues in near-catastrophic ways. With global markets, global suppliers, global networks, and global adversaries, is there space for a globally-cohesive approach to shoring up supply chain security?

For virtual access, register here: https://us02web.zoom.us/meeting/register/tZcud-Gprj8qE92RoBYuXTWhhHsakUjGvoLc

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 16:00-16:59 PDT

Title: Community Roundtable - Thinking About Election Security
When: Saturday, Aug 7, 16:00 - 16:59 PDT
Where: Policy (Virtual)

Description:

Election security has left the realm of election professionals and is now top of mind for anyone. But what does it mean? Is it just about the security of voting equipment? Or the security of the entire system of running elections? If you haven't been able to catch the Voting Village's content, or would like the opportunity for a deeper dive on some of the issues policymakers are wrestling with, this session is for you.

Register here: https://us02web.zoom.us/meeting/register/tZUlfu6hqTMoGtxIQ8TXdKvAUL4gZLj9x_o8

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 11:30-12:30 PDT

Title: Community Roundtable - Toward a Global IoT Code of Practice
When: Friday, Aug 6, 11:30 - 12:30 PDT
Where: Policy (Virtual & SkyView 1)

Description:

The UK's Code of Practice for IoT Security, developed by the UK government, has become a European standard, and countries around the world are adopting it as defacto minimum threshold for devices. This session will elicit responses to proposed Parliamentary legislation which would apply the Code to consumer IoT sold and imported in the UK. Peter Stephens, who leads the initiative, will be on hand to frame the discussion, answer questions, and take feedback.

For virtual access, register here: https://us02web.zoom.us/meeting/register/tZEqf-igrDIrG92o-NpocyyBPIMNfVEONXn7

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 16:00-16:59 PDT

Title: Community Roundtable - Volunteer Hacker Fire Department
When: Friday, Aug 6, 16:00 - 16:59 PDT
Where: Policy (Virtual & SkyView 1)

Description:

The volunteer fire department model has saved countless lives and countless economic damage across the US and around the world. Several initiatives over the past several years - and continuing today - have given us a glimpse of what a volunteer-based hacker Fire Department might look like, addressing Internet-scale incidents. What are they and how do we scale them?

For virtual access, register here: https://us02web.zoom.us/meeting/register/tZUvduytqTwsGN2k75CDTSCl23o0QDiqbkDn

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 11:30-12:30 PDT

Title: Community Roundtable - We can build it. We have the technology. So why aren't we?

When: Friday, Aug 6, 11:30 - 12:30 PDT

Where: Policy (Virtual)

Description:

Clean energy. Vaccines. We are an incredible species with an incredible capacity to innovate solutions to our biggest problems. So why are we so terrible at implementing them? Have some thoughts on this? Then come share them!

Register here: https://us02web.zoom.us/meeting/register/tZYkcumtqzsqGtzGz8976GzrMPoM3e6FEi1j

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 10:00-10:59 PDT

Title: Community Roundtable - We need to talk about Norm – Discussions on International cyber norms in diplomacy
When: Saturday, Aug 7, 10:00 - 10:59 PDT
Where: Policy (Onsite - SkyView 3)

Description:

This session will dive into the wide and wonderful world of “cyber norms” – the long-running international discussions seeking to establish rules of the road of behavior in cyberspace. After years of prolonged discussions in the United Nations but also informal groups like the Global Commission on the Stability of Cyberspace, we seem to be at an impasse – do we want to simply reinforce the already agreed upon 11 norms (like “non-interference in critical infrastructure”), do we want to expand the list of norms to include new behavior (like protecting the basic infrastructure of the Internet), or do we want to do both? And who is this “we” anyway? We'll kick off with a deeper look at the state of norm discussions and then open for a wider Q/A and discussion on what norms can and could do.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 14:30-15:30 PDT

Title: Community Roundtable - Zero Trust, Critical Software, and a Cyber Safety Review Board
When: Friday, Aug 6, 14:30 - 15:30 PDT
Where: Policy (Virtual & SkyView 1)

Description:

The recent cybersecurity Executive Order called for several new protections for US Federal networks and the nation's critical infrastructure, though some of these are undefined. While Zero Trust Architectures neatly fit into vendor buzzword bingo, what are they really? And how can you define critical software when any software on a critical system could cause harm? How would a Cyber Safety Review Board weigh in on issues where bits and bytes meet flesh and blood? Join this session to talk through some of the implications.

For virtual access, register here: https://us02web.zoom.us/meeting/register/tZAtfuqsrDgiH9y3ifQhU0Pg3bewc--OFyJ3

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Friday - 14:00-14:59 PDT

Title: Consider the (Data) Source
When: Friday, Aug 6, 14:00 - 14:59 PDT
Where: ICS Village (Virtual)

SpeakerBio: Dan Gunter , Founder and CEO of Insane Forensics
Dan Gunter is the Founder and CEO of Insane Forensics; a cybersecurity company focused on the scaled analysis of memory, disk, and network data in mission-critical networks. Before Insane Forensics, Dan was Director of R&D at Dragos and served in the US Air Force."
Twitter: @dan_gunter

Description:

Protecting industrial control systems involves a variety of challenges, from low tolerance of downtime to requiring a very deliberate combination of approaches and tools to ensure the integrity and availability of the environment. These environmental challenges can often stovepipe our thoughts around how we can respond to threats to control systems in making us think that one source of data is the only option. In this talk, we will consider the strengths and weaknesses of different data sources to include network and host sources. Using data from MITRE Engenuity's recent ICS ATT&CK evaluation, we will talk about known attacker TTPs, how to detect TTPs, and how to improve the chance of adversary detection by diversifying data sources. As collecting and processing more data is both a technical and staffing challenge, we will discuss how analysis can scale without requiring a significant resource increase.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 17:00-16:59 PDT

Title: COSTA (Coinbase Secure Trait Analyzer)
When: Thursday, Aug 5, 17:00 - 16:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Peter Kacherginsky , Founder OpenBlockSec project
No BIO available

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

Title: Cotopaxi
When: Sunday, Aug 8, 12:00 - 13:50 PDT
Where: DemoLab Video Channel 1

SpeakerBio: Jakub Botwicz
Jakub Botwicz, Ph.D. works as a security researcher in one of global investment banks. He has more than 17 years of experience in information security and previously worked in: one of the world's leading payment card service providers, Big4 consulting company and vendor of network encryption devices. Jakub holds a Ph.D. degree from Warsaw University of Technology. During the last 3 years he has reported more than 50 CVEs (security vulnerabilities) in publiccomponents - mainly IoT libraries.

Description:

Tool or Project Name: Cotopaxi

Short Abstract:
Cotopaxi is a set of tools for security testing of Internet of Things devices using specific network IoT/IIoT/M2M protocols (AMQP, CoAP, DTLS, gRPC, HTTP/2, HTCPCP, KNX, mDNS, MQTT, MQTT-SN, QUIC, RTSP, SSDP).

Short Developer Bio:
Jakub Botwicz, Ph.D. works as a security researcher in one of global investment banks. He has more than 17 years of experience in information security and previously worked in: one of the world's leading payment card service providers, Big4 consulting company and vendor of network encryption devices. Jakub holds a Ph.D. degree from Warsaw University of Technology. During the last 3 years he has reported more than 50 CVEs (security vulnerabilities) in publiccomponents - mainly IoT libraries.

URL to any additional information:
https://github.com/Samsung/cotopaxi/...aster/cotopaxi

Detailed Explanation of Tool:
Currently available tools used for security testing, like nmap or OpenVAS, do not support all new IoT protocols (e.g. CoAP, DTLS, HTCPCP, QUIC). So possibilities to test IoT products and discover such devices in tested networks are limited. We are working to fill this gap with the Cotopaxi toolkit.

New features in the release for DEF CON 2021 are: Integration with Metasploit
Extended set of corpuses for fuzzing and traffic classification Mutation-based features for server and client fuzzing New vulnerabilities in the database
Main features of our toolkit are:
Checking availability of network services for supported IoT protocols at given IPs and port ranges ("service ping")
Recognizing the software used by remote network server ("software fingerprinting") based on responses for given messages using machine learning classifier, Analysis of network traffic to identify network protocols used. Classification of IoT devices based on captured traffic samples. Discovering resources identified by given URLs ("dirbusting" of URLs or services)
Performing black-box fuzzing of IoT protocols based on corpus of packets prepared using coverage-based fuzzer. Identifying known vulnerabilities.
Detecting network traffic amplification (cases where network servers are responding with larger network messages than received requests).

Supporting Files, Code, etc:
https://pypi.org/project/cotopaxi/

Target Audience:
Offense, Defense, AppSec, IoT

This content will be presented on a Discord video channel.

#dl-video1-voice: https://discord.com/channels/708208267699945503/734027693250576505

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 14:30-14:55 PDT

Title: CPDLC: Man-in-the-middle attacks and how to defend against them
When: Friday, Aug 6, 14:30 - 14:55 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Joshua Smailes
No BIO available

Description:

The Controller Pilot Data Link Communications (CPDLC) protocol replaces voice-based air traffic control with a text-based protocol. With no real security protections, this system is open to a wide range of message injection attacks. It has long been assumed that air traffic controllers and flight crew should be able to detect such attacks, but this is not always the case.

We construct a realistic threat model for CPDLC and introduce attacks on the underlying protocol, taking advantage of automated components of the system to make attacks which are difficult for human operators to detect. We also propose a number of improvements to CPDLC to mitigate these threats.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=cl_56FUk8ps

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Saturday - 14:00-14:30 PDT

Title: Crippling the Grid: Examination of Dependencies and Cyber Vulnerabilities
When: Saturday, Aug 7, 14:00 - 14:30 PDT
Where: ICS Village (Virtual)

SpeakerBio: Joe Slowik , Gigamon
Joe Slowik currently leads threat intelligence and network detection work at Gigamon. Previously, Joe performed security research for DomainTools and hunted ICS-focused adversaries for Dragos. Joe remains fascinated by the ICS landscape and critical infrastructure intrusions, and continues to pursue such topics personally and professionally.
Twitter: @jfslowik

Description:
Typical views of cyber-focused attacks on electric utilities emphasize direct impacts to generation, transmission, or distribution assets. While some examples of this activity exist, most notably in Ukraine, such actions are relatively difficult given technical and access requirements to properly execute. Less explored, but far more dangerous, are critical dependencies in electric utility operations which are often more exposed to IT networks and require less specialized knowledge to subvert. This presentation will examine some of these dependencies and their implications to show how ICS-centric defense must include relevant IT links and functional requirements.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 12:00-12:45 PDT

Title: Cross-document messaging technology, how to hack it, and how to use it safely.
When: Friday, Aug 6, 12:00 - 12:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Chen Gour-Arie
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 10:00-10:45 PDT

Title: Crossover Episode: The Real-Life Story of the First Mainframe Container Breakout
When: Saturday, Aug 7, 10:00 - 10:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded
Speakers: Chad Rikansrud (Bigendian Smalls),Ian Coldwater

SpeakerBio: Chad Rikansrud (Bigendian Smalls)
Chad is the same, but for mainframes and mainframe security.
Twitter: @bigendiansmalls

SpeakerBio: Ian Coldwater
Ian is a leading expert on containers and container security.
Twitter: @IanColdwater

Description:

You've seen talks about container hacking. You've seen talks about mainframe hacking. But how often do you see them together? IBM decided to put containers on a mainframe, so a container hacker and a mainframe hacker decided to join forces and hack it. We became the first people on the planet to escape a container on a mainframe, and we’re going to show you how.

Containers on a mainframe? For real. IBM zCX is a Docker environment running on a custom Linux hypervisor built atop z/OS - IBM’s mainframe operating system. Building this platform introduces mainframe environments to a new generation of cloud-native developers-and introduces new attack surfaces that weren’t there before.

In this crossover episode, we’re going to talk about how two people with two very particular sets of skills went about breaking zCX in both directions, escaping containers into the mainframe host and spilling the secrets of the container implementation from the mainframe side.

When two very different technologies get combined for the first time, the result is new shells nobody’s ever popped before.

REFERENCES: Getting started with z/OS Container Extensions and Docker: https://www.redbooks.ibm.com/abstracts/sg248457.html The Path Less Traveled: Abusing Kubernetes Defaults: https://www.youtube.com/watch?v=HmoVSmTIOxM Attacking and Defending Kubernetes Clusters: A Guided Tour: https://securekubernetes.com Evil Mainframe penetration testing course :https://www.evilmainframe.com/ z/OS Unix System Services (USS): https://www.ibm.com/docs/en/zos/2.1.0?topic=system-basics-zos-unix-file z/OS Concepts: https://www.ibm.com/docs/en/zos-basic-skills?topic=zc-zos-operating-system-providing-virtual-environments-since-1960s Docker overview: https://docs.docker.com/get-started/overview/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=7DXF7YDBf-g

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20I

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Saturday - 16:30-16:59 PDT

Title: Cryptocurrency Trivia!
When: Saturday, Aug 7, 16:30 - 16:59 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Justin Ehrenhofer
No BIO available

Description:
Join us for cryptocurrency-themed trivia! Each player competes using their phone or computer on topics relating cryptocurrency news, lore, history, research, and development. This will be a super fun time!

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 12:00-12:45 PDT

Title: CSP is broken, let’s fix it
When: Saturday, Aug 7, 12:00 - 12:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Amir Shaked
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Saturday - 13:30-13:50 PDT

Title: CSPM2CloudTrail - Extending CSPM Tools with (Near) Real-Time Detection Signatures (Lightning Talk)
When: Saturday, Aug 7, 13:30 - 13:50 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Rodrigo "Sp0oKeR" Montoro
Rodrigo "Sp0oKeR" Montoro has 20 years of experience deploying open source security software (firewalls, IDS, IPS, HIDS, log management) and hardening systems. Currently, he is a Senior Researcher at Tempest Security. Before it, he worked as Cloud Researcher at Tenchi Security, Head of Research and Development at Apura Cyber Intelligence, SOC/Researcher at Clavis, Senior Security Administrator at Sucuri, Spiderlabs Researcher, where he focuses on IDS/IPS Signatures, Modsecurity rules, and new detection researches. Author of 2 patented technologies involving the discovery of malicious digital documents and analyzing malicious HTTP traffic. He is currently coordinator and Snort evangelist for the Brazilian Snort Community. Rodrigo has spoken at several open-source and security conferences (OWASP AppSec, SANS DFIR & SIEM Summit, Toorcon (USA), H2HC (São Paulo and Mexico), SecTor (Canada), CNASI, SOURCE Boston & Seattle, ZonCon (Amazon Internal Conference), Blackhat Brazil, BSides (Las Vegas e São Paulo)).
Twitter: @spookerlabs

Description:

The AWS service APIs provide around 9,400 different actions (and growing!) that, when logged, give a lot of extra info that can be correlated and used to find malicious activities. However, as with most data sources, it is very noisy. Plus, it fails to include in its events critical contextual information that threat hunters need. Working with our Threat Detection Engineering Team to create very actionable use cases that don't need much additional context and exceptions. We developed an idea to detect the creation time of events discovered by most CSPMs check when evaluating a cloud provider, particularly AWS in this case. Cloud Security Posture Management (CSPM), which works by detecting cloud service misconfigurations, is one of the most common technologies used to improve cloud security and is used heavily worldwide by thousands of companies. Despite this, CSPM tools cannot detect most of the real-time findings, need privileges to be executed and scheduled to run and analyze preferably daily to decrease windows exposure. Cloud misconfigurations typically result in second-stage attacks. Aside from some risks that make information public, attackers likely need some credentials with privileges to perform actions that could impact privilege escalation, resource exposure, crypto mining, infrastructure modification, and access to sensitive data. Starting with some CloudSploit checks, we named this research CSPM2CloudTrail, so we create misconfigured services based on their findings and analyze how these changes are logged to CloudTrail. We made many use cases that we mainly transform in cards (with CloudSploit information) and sigma rules, having information such as severity, recommendations, AWS Documentation, and more importantly, for our SOC, Splunk searches. Besides this great use of trying to detect this almost in real-time (since CloudTrail delays around 15 minutes), these queries could enrich CSPM findings, making incident responses on misconfigurations caught faster. All information and detections created will be shared in our Github repository.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Saturday - 10:00-11:59 PDT

Title: CybatiWorks Mission Station Workshop
When: Saturday, Aug 7, 10:00 - 11:59 PDT
Where: ICS Village (Virtual)

SpeakerBio: Matthew Luallen , Chief Executive Inventor, IntelliGenesis
Matthew E. Luallen is the Chief Executive Inventor of IntelliGenesis, LLC. He leads the company in further developing and expanding training services to enhance the understanding of, and provide protection from, cyber-physical threats. IntelliGenesis acquired CybatiWorks™ where Luallen served as a Co-Founder of CYBATI. He also served as a Co-Founder of Dragos Security co-developing CyberLens™ for Operational Technology device and communications discovery and analysis. He was a Co-Founder of Encari, a NERC CIP cybersecurity consulting firm helping the US and Canadian power grid defend strategic assets from cyber-physical attacks. He was an Information Security Network Engineer and Architect at Argonne National Laboratory. He is a 22-year CCIE and an 18-year Certified Instructor for the SANS Institute.
Twitter: @cybati

Description:
Introduce, demonstrate and provide an interactive overview of the CybatiWorks exploratory cyber-physical mission station workshop. Participants mission station exercises cover an introduction to cyber-physical topics of logic, sensors and actuators, OT system architecture, communication protocols and data analysis. Participant mission station access is provided on a first-serve (FIFO) basis.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Sunday - 10:00-10:30 PDT

Title: Cyber Defense Matrix in Healthcare
When: Sunday, Aug 8, 10:00 - 10:30 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Sounil Yu , Cyber Strategist
Sounil Yu is a security innovator with over 30 years of hands-on experience creating, breaking, and fixing computer and network systems. He is currently the CISO & Head of Research for the startup JupiterOne. Sounil created the Cyber Defense Matrix and the DIE Triad, which are reshaping approaches to cybersecurity. He's a Board Member of the FAIR Institute and SCVX; co-chairs Art into Science: A Conference on Defense; is a visiting fellow at GMU Scalia Law School's National Security Institute; teaches at Yeshiva University; and advises many startups. Sounil previously served as the CISO-in-Residence at YL Ventures and Chief Security Scientist at Bank of America, driving innovation to meet emerging security needs and develop alternative approaches to hard problems in security. Before Bank of America, he helped improve information security at several institutions spanning from Fortune 100 companies with three letters on the stock exchange to secretive three letter agencies that are not.

Description:

The Cyber Defense Matrix helps us understand what we need organized through a logical construct so that when we go into the security vendor marketplace, we can quickly discern what products solve what problems and be informed on what is the core function of a given product. In addition, the Cyber Defense Matrix provides a mechanism to ensure that we have capabilities across the entire spectrum of options to help secure our environments.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Saturday - 12:00-12:55 PDT

Title: Cyber in the Under Sea
When: Saturday, Aug 7, 12:00 - 12:55 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: David Strachan
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Saturday - 14:00-14:55 PDT

Title: Cyber Operations and Operational Wargames on Port Infrastructure
When: Saturday, Aug 7, 14:00 - 14:55 PDT
Where: Hack the Sea (Virtual)
Speakers: Tom Mouatt,Ed McGrady,John Curry

SpeakerBio: Tom Mouatt
No BIO available

SpeakerBio: Ed McGrady
No BIO available

SpeakerBio: John Curry
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Sunday - 12:00-12:55 PDT

Title: Cyber Risk Management in the MTS
When: Sunday, Aug 8, 12:00 - 12:55 PDT
Where: Hack the Sea (Virtual)
Speakers: Josie Long,Kelley Edwards

SpeakerBio: Josie Long , USCG Cyber
No BIO available

SpeakerBio: Kelley Edwards
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Saturday - 11:00-11:55 PDT

Title: Cyber-SHIP Lab Talk and Demo
When: Saturday, Aug 7, 11:00 - 11:55 PDT
Where: Hack the Sea (Virtual)
Speakers: Kevin Jones,Kimberley Tam

SpeakerBio: Kevin Jones
No BIO available

SpeakerBio: Kimberley Tam
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

CON - Sunday - 09:00-23:59 PDT

Title: Darknet-NG
When: Sunday, Aug 8, 09:00 - 23:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/238249

- warning, end time is suspect, must confirm *

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 09:00-15:59 PDT

Title: Darknet-NG
When: Friday, Aug 6, 09:00 - 15:59 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/238249

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 09:00-16:59 PDT

Title: Darknet-NG

When: Saturday, Aug 7, 09:00 - 16:59 PDT

Where: See Description

Description:

For more information, see https://forum.defcon.org/node/238249

Return to Index - Add to Google Calendar - ics Calendar file

DDV - Sunday - 10:00-10:59 PDT

Title: Data Duplication Village - Last Chance Pickup Only
When: Sunday, Aug 8, 10:00 - 10:59 PDT
Where: Data Duplication Village

Description:

Space permitting, last drop off is Saturday at 3:00pm.

Pick your drives full of data anytime 14-24 hours after drop off.

Last chance pickup is Sunday from 10:00 to 11:00.

Yes, 6TB and larger drives are accepted.

Any drives not picked up by Sunday at 11:00am are considered donated to the DDV.

See https://dcddv.org/dc29-schedule for more information.

Return to Index - Add to Google Calendar - ics Calendar file

DDV - Thursday - 15:00-18:59 PDT

Title: Data Duplication Village - Open for dropoff only
When: Thursday, Aug 5, 15:00 - 18:59 PDT
Where: Data Duplication Village

Description:

Space permitting, last drop off is Saturday at 3:00pm.

Pick your drives full of data anytime 14-24 hours after drop off.

Last chance pickup is Sunday from 10:00 to 11:00.

Yes, 6TB and larger drives are accepted.

Any drives not picked up by Sunday at 11:00am are considered donated to the DDV.

See https://dcddv.org/dc29-schedule for more information.

Return to Index - Add to Google Calendar - ics Calendar file

DDV - Friday - 10:00-16:59 PDT

Title: Data Duplication Village - Open
When: Friday, Aug 6, 10:00 - 16:59 PDT
Where: Data Duplication Village

Description:

Space permitting, last drop off is Saturday at 3:00pm.

Pick your drives full of data anytime 14-24 hours after drop off.

Last chance pickup is Sunday from 10:00 to 11:00.

Yes, 6TB and larger drives are accepted.

Any drives not picked up by Sunday at 11:00am are considered donated to the DDV.

See https://dcddv.org/dc29-schedule for more information.

Return to Index - Add to Google Calendar - ics Calendar file

DDV - Saturday - 10:00-09:59 PDT

Title: Data Duplication Village - Open
When: Saturday, Aug 7, 10:00 - 09:59 PDT
Where: Data Duplication Village

Description:

Space permitting, last drop off is Saturday at 3:00pm.

Pick your drives full of data anytime 14-24 hours after drop off.

Last chance pickup is Sunday from 10:00 to 11:00.

Yes, 6TB and larger drives are accepted.

Any drives not picked up by Sunday at 11:00am are considered donated to the DDV.

See https://dcddv.org/dc29-schedule for more information.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 17:00-18:59 PDT

Title: DC404/DC678/DC770/DC470 (Atlanta Metro) Meetup
When: Saturday, Aug 7, 17:00 - 18:59 PDT
Where: Bally's Skyview 2

Description:

They say Atlanta is the city too busy to hate, but it also has too much traffic for its widespread hacker fam to get together in a single meetup. So instead we're meeting up in the desert during DEF CON! The one time of year when intown, northern burbs, south siders, and anyone else connected to DC404's 20+ year legacy can catch up and share stories. We typically meet up for an hour or two then will go get dinner afterwards before evening events.

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 11:00-11:59 PDT

Title: Decoding NOAA Weather Sat Signals
When: Saturday, Aug 7, 11:00 - 11:59 PDT
Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:

- You’ll need a laptop with internet connection for this workshop

My goal for this workshop is to introduce receiving and decoding NOAA weather satellite signals. I’ll demonstrate this first with a commercially available radio, and then I’ll demonstrate how to listen to to NOAA satellites for free using publicly accessible and internet connected radios scattered across the globe.

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:00-15:59 PDT

Title: Deep Space Networking

When: Friday, Aug 6, 10:00 - 15:59 PDT

Where: Aerospace Village (Virtual Workshop)

Description:

Deep space communications utilize TCP/IP protocols with some added assistance from a TCP Convergence Layer and the Bundle Protocol. In this workshop, participants will contrast data transmission on the Earth terrestrial Internet to the Deep Space Network and then delve into the latest version of the Bundle protocol and the TCP Convergence Layer. We will examine key fields in the headers, locate the first packet of a bundle and the first and second legs of the relay process, as reassembled by Wireshark. Participants will learn to build a custom Wireshark profile to quickly identify key fields of the Bundle Protocol, including fields that define priority, destination type, endpoint IDs, and reporting of bundle delivery.

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 10:00-15:59 PDT

Title: Deep Space Networking
When: Saturday, Aug 7, 10:00 - 15:59 PDT
Where: Aerospace Village (Virtual Workshop)

Description:

Deep space communications utilize TCP/IP protocols with some added assistance from a TCP Convergence Layer and the Bundle Protocol. In this workshop, participants will contrast data transmission on the Earth terrestrial Internet to the Deep Space Network and then delve into the latest version of the Bundle protocol and the TCP Convergence Layer. We will examine key fields in the headers, locate the first packet of a bundle and the first and second legs of the relay process, as reassembled by Wireshark. Participants will learn to build a custom Wireshark profile to quickly identify key fields of the Bundle Protocol, including fields that define priority, destination type, endpoint IDs, and reporting of bundle delivery.

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-19:59 PDT

Title: DEF CON 29 CTF by OOO
When: Friday, Aug 6, 10:00 - 19:59 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/236417

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 10:00-19:59 PDT

Title: DEF CON 29 CTF by OOO
When: Saturday, Aug 7, 10:00 - 19:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236417

Return to Index - Add to Google Calendar - ics Calendar file

CON - Sunday - 10:00-13:59 PDT

Title: DEF CON 29 CTF by OOO
When: Sunday, Aug 8, 10:00 - 13:59 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/236417

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 06:00-11:59 PDT

Title: DEF CON Bike Ride
When: Friday, Aug 6, 06:00 - 11:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236418

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 16:00-16:59 PDT

Title: DEF CON Closing Ceremonies, Black Badge Ceremonies
When: Sunday, Aug 8, 16:00 - 16:59 PDT
Where: Track 1 Live; DCTV/Twitch #1 Live

SpeakerBio: Dark Tangent
No BIO available

Description: No Description available

This talk will be given live in Track 1, and will be streamed to DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 09:00-16:59 PDT

Title: DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open
When: Saturday, Aug 7, 09:00 - 16:59 PDT
Where: Paris DEF CON Registration Desk

Description:

You can start the 2-step process. There is no need to rush, if you have purchased on-line your badge is reserved and there is no concern about them running out:

1st you will pass through the vaccination check line, providing whatever original documentation your health care provider or vaccination center gave you. It will be checked against your State issued ID to make sure the names match, the dates are good, and that enough time has passed for you to be fully vaccinated, etc. We will not record your ID or records. If all is good you will get a WRISTBAND you must wear during the con.

2nd Next you head to the badge pickup desks. There you will show your wristband and your in-person badge bar code and get it scanned. If the scan passes you get your Human reg pack.

Where to register / pick up badges: Paris, near the InfoBooth. Please find "REGISTRATION" on the provided DC29 floorplan (available in HackerTracker and online).

Both registration and the vaccine check processing functions are planning to be available from 8am/08:00 to 5pm/17:00. If those times change, this schedule entry will be updated in HackerTracker and info.defcon.org as soon as possible.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 09:00-13:59 PDT

Title: DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open
When: Sunday, Aug 8, 09:00 - 13:59 PDT
Where: Paris DEF CON Registration Desk

Description:

You can start the 2-step process. There is no need to rush, if you have purchased on-line your badge is reserved and there is no concern about them running out:

1st you will pass through the vaccination check line, providing whatever original documentation your health care provider or vaccination center gave you. It will be checked against your State issued ID to make sure the names match, the dates are good, and that enough time has passed for you to be fully vaccinated, etc. We will not record your ID or records. If all is good you will get a WRISTBAND you must wear during the con.

2nd Next you head to the badge pickup desks. There you will show your wristband and your in-person badge bar code and get it scanned. If the scan passes you get your Human reg pack.

Where to register / pick up badges: Paris, near the InfoBooth. Please find "REGISTRATION" on the provided DC29 floorplan (available in HackerTracker and online).

Both registration and the vaccine check processing functions are planning to be available from 8am/08:00 to 5pm/17:00. If those times change, this schedule entry will be updated in HackerTracker and info.defcon.org as soon as possible.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 08:00-16:59 PDT

Title: DEF CON Human Registration (Badge Pickup) and Vaccine Check Processing Open
When: Friday, Aug 6, 08:00 - 16:59 PDT
Where: Paris DEF CON Registration Desk

Description:

You can start the 2-step process. There is no need to rush, if you have purchased on-line your badge is reserved and there is no concern about them running out:

1st you will pass through the vaccination check line, providing whatever original documentation your health care provider or vaccination center gave you. It will be checked against your State issued ID to make sure the names match, the dates are good, and that enough time has passed for you to be fully vaccinated, etc. We will not record your ID or records. If all is good you will get a WRISTBAND you must wear during the con.

2nd Next you head to the badge pickup desks. There you will show your wristband and your in-person badge bar code and get it scanned. If the scan passes you get your Human reg pack.

Where to register / pick up badges: Paris, near the InfoBooth. Please find "REGISTRATION" on the provided DC29 floorplan (available in HackerTracker and online).

Both registration and the vaccine check processing functions are planning to be available from 8am/08:00 to 5pm/17:00. If those times change, this schedule entry will be updated in HackerTracker and info.defcon.org as soon as possible.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Thursday - 07:00-19:59 PDT

Title: DEF CON Human Registration (Badge Pickup) Open
When: Thursday, Aug 5, 07:00 - 19:59 PDT
Where: Paris DEF CON Registration Desk

Description:

Starting Thursday at 07:00 badge pickup will open and you can start the 2-step process. There is no need to rush, if you have purchased on-line your badge is reserved and there is no concern about them running out:

1st you will pass through the vaccination check line, providing whatever original documentation your health care provider or vaccination center gave you. It will be checked against your State issued ID to make sure the names match, the dates are good, and that enough time has passed for you to be fully vaccinated, etc. We will not record your ID or records. If all is good you will get a WRISTBAND you must wear during the con.

2nd Next you head to the badge pickup desks. There you will show your wristband and your in-person badge bar code and get it scanned. If the scan passes you get your Human reg pack.

Where to register / pick up badges: Paris, near the InfoBooth. Please find "REGISTRATION" on the provided DC29 floorplan (available in HackerTracker and online).

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 20:00-21:59 PDT

Title: DEF CON Movie Night - Tron
When: Friday, Aug 6, 20:00 - 21:59 PDT
Where: See Description

Description:
Tron will be shown in Track 2.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 20:00-21:59 PDT

Title: DEF CON Movie Night - Upgrade
When: Saturday, Aug 7, 20:00 - 21:59 PDT
Where: See Description

Description:

Upgrade will be shown in Track 2.

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-11:59 PDT

Title: DEF CON Scavenger Hunt
When: Friday, Aug 6, 10:00 - 11:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236484

Also see #ce-defcon-scavenger-hunt-text

#ce-defcon-scavenger-hunt-text:
https://discord.com/channels/708208267699945503/711049278163779605/872883588461367366

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 13:00-13:45 PDT

Title: Defeating Physical Intrusion Detection Alarm Wires
When: Saturday, Aug 7, 13:00 - 13:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Bill Graydon
Bill Graydon is a principal researcher at GGR Security, where he hacks everything from locks and alarms to critical infrastructure; this has given him some very fine-tuned skills for breaking stuff. He's passionate about advancing the security field through research, teaching numerous courses, giving talks, and running DEF CON's Lock Bypass Village. He's received various degrees in computer engineering, security, and forensics and comes from a broad background of work experience in cyber security, software development, anti-money laundering, and infectious disease detection.

https://www.youtube.com/channel/UCzZK3vjJL9rKNPXNoCPFO5g/videos

Twitter: @access_ctrl
https://github.com/bgraydon

Description:

Alarm systems are ubiquitous - no longer the realm of banks and vaults only, many people now have them in their homes or workplaces. But how do they work? And the logical follow-up question - how can they be hacked?

This talk focuses on the communication lines in physical intrusion detection systems: how they are secured, and what vulnerabilities exist. We'll discuss the logic implemented in the controllers and protections on the communication lines including end of line resistors - and all the ways that this aspect of the system can be exploited.

In particular, we'll release schematics for a tool we've developed that will enable measuring end-of-line resistor systems covertly, determining the necessary re-wiring to defeat the sensors, and deploy it without setting off the alarm.

After the talk, you can head over to the Lock Bypass Village to try these techniques out for yourself!

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=Liz9R_QxSgk

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20E

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 16:00-16:59 PDT

Title: Defending against nation-state (legal) attack: how to build a privacy-protecting service in the era of ubiquitous surveillance

When: Friday, Aug 6, 16:00 - 16:59 PDT

Where: Track 1 Live; DCTV/Twitch #1 Live

SpeakerBio: Bill "Woody" Woodcock

No BIO available

Description: No Description available

This talk will be given live in Track 1, and will be streamed to DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 17:30-18:15 PDT

Title: Defending IoT in the Future of High-Tech Warfare
When: Friday, Aug 6, 17:30 - 18:15 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Harshit Agrawal
Harshit Agrawal is currently working as a Radio Security Researcher. He is enthusiastic about Sigint, Drone Pentesting, and IoT Security. He presented his research at Security conferences like RSAC USA, HITB Cyberweek, HITB Amsterdam, etc. Previously, he was President at CSI Chapter and Vice President for Entrepreneurship cell at MIT, where he also headed the team of security enthusiasts, giving him a good insight into cybersecurity and increased his thirst to explore more in this field.

Description:
The increase of cyberattacks using IoT devices has exposed the vulnerabilities in the infrastructures that make up the IoT and have shown how small devices can affect networks and services functioning. This talk presents a review of the vulnerabilities that bear the IoT and assessing the experiences in implementing RF attacks targeting the Internet of Things and analyses various facets of the IoT centricity of future military operations based on the IoT concept, IoT-led future shaping of the things, challenges, and developmental trajectories of major powers.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 11:30-11:55 PDT

Title: Defending the Unmanned Aerial Vehicle: Advancements in UAV Intrusion Detection
When: Saturday, Aug 7, 11:30 - 11:55 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Jason Whelan
Jason (OSCP, OSCE, CCNP) holds a Bachelor of IT and is currently working towards a MSc in Computer Science from Ontario Tech University. He has presented at international conferences on UAV security, and has experience in both practical security research and penetration testing of operational UAS.

Description:

Many attacks against the UAV are becoming commonplace as they are simple to conduct with inexpensive hardware, such as spoofing and jamming. Unfortunately, many of the vulnerabilities UAVs suffer from are based on security flaws in the underlying technologies, including GPS and ADS-B. An intrusion detection system (IDS) for UAVs can increase security rapidly without the need to re-engineer underlying technologies. UAVs are cyber-physical systems which introduce a number of challenges for IDS development as they utilize a wide variety of sensors, communication protocols, platforms, and control configurations. Commercial off-the-shelf IDS solutions can be strategically implemented within the Unmanned aerial system (UAS) to detect threats to the underlying traditional IT infrastructure, however, the UAV itself requires specialized detection techniques. This talk discusses advancements in UAV intrusion detection, including proposed solutions in academics, pitfalls of these solutions, and how a practical technique using machine learning can be used to detect attacks across UAV platforms. A fully developed IDS is presented which makes use of flight logs and an onboard agent for autonomous detection and mitigation. The topics covered come from lessons learned in UAS penetration testing, live experiments, and academic research in the UAV security space.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=XEN9LTOUFFQ

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 17:00-16:59 PDT

Title: DeFi Must Change or Hacks Will Accelerate
When: Thursday, Aug 5, 17:00 - 16:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Kadan Stadelmann , CTO Komodo Platform
Kadan Stadelmann is a blockchain developer, operations security expert and Komodo Platform’s chief technology officer. His experience ranges from working in operations security in the government sector and launching technology startups to application development and cryptography. Kadan started his journey into blockchain technology in 2011 and joined the Komodo team in 2016.

Kadan has published numerous articles on Forbes, Cointelegraph, NASDAQ and Yahoo Finance.

https://cointelegraph.com/authors/kadan-stadelmann
https://www.forbes.com/sites/justinoconnell/2020/02/10/in-the-future-you-can-create-your-own-stablecoin-with-just-a-few-clicks-c
https://www.nasdaq.com/articles/can-we-build-a-post-feudal-web-3-2020-03-12
https://www.nasdaq.com/articles/heres-why-blockchain-hasnt-taken-over-the-world-yet-2019-05-09
https://finance.yahoo.com/finance/news/decentralized-exchange-launches-dogecoin-swaps-132541367.html

Description:

Decentralized Finance (DeFi) is here to stay, with over $118 Billion in total locked value highlighting evidence of faith in these new financial tools. This investment will continue increasing, but appears that with each new record in total value locked, there is another network attack being reported with astronomical losses.

Crypto crime cost companies and investors more than $10.5 Billion in 2020. In February 2021 alone, $200 Million was stolen in DeFi within just a 5 day period.

It is clear that there are far too many loopholes and hacks in current blockchain security protocols. From rug pulls to phishing scams, the security and technology is not as mature as the numbers make it out to be in this space. But there are critical practices both developers and users can implement to close this gap.

Return to Index - Add to Google Calendar - ics Calendar file

Title: Depthcharge
When: Saturday, Aug 7, 10:00 - 11:50 PDT
Where: Palace 3+4+5

SpeakerBio: Jon Szymaniak
Jon Szymaniak is Principle Security Consultant in NCC Group’s Hardware & Embedded Systems Services team and a former embedded systems engineer. His areas of interest include U-Boot, Linux, Yocto, and firmware reverse engineering. Through both his day job and hobby hacking adventures, he’s enjoyed exploring and exploiting boot ROMs, automotive ECUs, Android-based platforms, and a myriad of Internet-connected things that shouldn't be.

Description:
Depthcharge: A Framework for U-Boot Hacking

Short Abstract:
In modern embedded systems that implement a “secure boot” flow, the boot loader plays a critical role in establishing the integrity and authenticity of software and data required to boot an operating system. Given the role and vantage point of boot loaders, they are a particularly interesting target for hardware hackers seeking to root a device and instrument it for further vulnerability hunting and reverse engineering. Although the vast majority of devices leveraging the ubiquitous and open source U-Boot boot loader leave it unprotected and trivially exploited, more product vendors are finally implementing secure boot and (attempting to) lock down their U-Boot builds. These less common specimen offer exciting opportunities to pursue creative bypasses and explore underappreciated U-Boot functionality.

The Depthcharge framework was developed to help hardware hackers methodically (ab)use some of that underappreciated U-Boot functionality in novel ways to circumvent boot-time protections, as well as expedite the identification and exploitation of “the usual suspects” within exposed U-Boot device consoles. The project includes a Python 3 library for interfacing with devices, reading and writing memory via available primitives, deploying executable payloads, and analyzing various data structures. A collection of scripts built atop of library make this functionality readily available via the command line, and “Depthcharge Companion” firmware allows the tooling to extend its vantage point by presenting itself as a peripheral device connected to the target. This Demo Lab will introduce the basics of Depthcharge and explore how attendees can leverage and expand upon it when seeking to circumvent boot-time protections or just to further explore a system from within the U-Boot environment. For those wishing to protect their (employer’s) products from fellow DEF CON attendees, we’ll also cover the configuration checker functionality that can be used to avoid common U-Boot pitfalls.

Developer Bio:
Jon Szymaniak is Principle Security Consultant in NCC Group’s Hardware & Embedded Systems Services team and a former embedded systems engineer. His areas of interest include U-Boot, Linux, Yocto, and firmware reverse engineering. Through both his day job and hobby hacking adventures, he’s enjoyed exploring and exploiting boot ROMs, automotive ECUs, Android-based platforms, and a myriad of Internet-connected things that shouldn't be.

URLs
GitHub: https://github.com/nccgroup/depthcharge Documentation: https://depthcharge.readthedocs.io

Blog Posts and Prior Presentations:
Blog: https://research.nccgroup.com/2020/07/22/depthcharge/ Hardwear.io Webinar: https://www.youtube.com/watch?v=fTKMi3Is5x8 Blog: https://research.nccgroup.com/2020/1...hcharge-v0-2-0 OSFC Presentation: https://vimeo.com/488134063 Detailed Explanation:
Additional detail can be found here in the project documentation: https://depthcharge.readthedocs.io/e...is-depthcharge

The Depthcharge project aims to allow hackers, security practitioners, and engineering teams a way to “work smarter” when attempting to root a device or evaluate its security posture. This not only includes gaining control of a target’s U-Boot execution, but also leveraging the bootloader as a vantage point to further explore the target system.

The Python 3 Depthcharge API can be leveraged to enumerate functionality exposed by a U-Boot console and identify memory read/write primitives. Memory access abstractions built atop of these primitives seek to make dumping device firmware quicker and more robust, and custom payload deployment easier. With its colorized serial monitor, Depthcharge provides a more pleasant environment for hacking around and scripting while within a device's U-Boot console. The "Companion" firmware extends Depthcharge reach into a target platform, allowing it to act as a "malicious" peripheral device (e.g. on an I2C bus). While much of the project focuses on console exposure, it also include some data structure identification (e.g. stored environments) functionality aimed at situations where such functionality is not available. For engineers and those on the "blue team" — build configuration checker functionality can help raise red flags and detect U-Boot pitfalls much earlier in the product development lifecycle.

Target Audience:
Hardware / Embedded Systems - Both "offense" and "defense" within this audience

I believe the Depthcharge Demo Lab can show that there's more interesting hackery to be had within the U-Boot boot loader, and that we can work much smarter when we encounter it. Given that I tend to see discussions of U-Boot limited to unprotected IoT junkware, I've always been bummed that folks don't seem to get to appreciate the joy of circumventing secure boot mechanisms, or otherwise leveraging their U-Boot environment to start exploring a hardware platform and its SoC from a lower level vantage point.

Whether it be folks enjoying the abuse of a CRC32 feature as an arbitrary memory primitive, or just gaining an appreciation for how U-Boot exports functionality for use by "stand alone applications" — I hope to share some new tricks and get people excited about hacking deeper on their devices. Demos will be based upon my earlier work bypassing a (now patched) 2019 Sonos vulnerability, as well as some "previously seen on client work" vulnerabilities modeled on development kits to protect the (not so?) innocent.

Warranty voiding and custom firmware development shall be strongly encouraged.

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 16:45-17:45 PDT

Title: Designing a C2 Framework
When: Friday, Aug 6, 16:45 - 17:45 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Daniel "Rasta" Duggan
Daniel Duggan, aka Rasta Mouse, is the Director of Zero-Point Security and creator of the Red Team Ops training course. Daniel has authored and contributed to multiple open source projects including TikiTorch, SharpC2, Covenant and SharpSploit.
Twitter: @_RastaMouse

Description:
Over recent years, there has been a huge boom in open-source C2 frameworks hitting the information security space. So much so they made a website and a logo - that's how you know things are serious! Such a trend naturally drives more people towards taking on the gauntlet but all too often it becomes an insurmountable challenge and another dashed dream of the aspiring red teamer, or veteran alike. Believe me when I say - I've been there. I've felt the pain, the frustration, the imposter syndrome. Heck, I still do. However, I've (mostly) come out the other side with some hard learned lessons. Those lessons are the subject of this talk. The goal is not to write or provide code. We shall discuss how to approach initial design ideas; decide what is important and what is not; anticipate and deal with potential problem areas; consider different use cases and perspectives; and more.

If you are interested in building your own C2 framework, contributing to existing frameworks, or even software development in general, there's something in this talk for you.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Sunday - 10:30-10:59 PDT

Title: Detecting Attackers Using Your Own Sensors with State Estimation
When: Sunday, Aug 8, 10:30 - 10:59 PDT
Where: ICS Village (Virtual)

SpeakerBio: Stefan Stephenson-Moe , Coalfire
I have eight years infosec experience working in critical infrastructure, three years working in the power industry, four years working in the finance sector. My experience is mostly on the operations and implementation side, designing, implementing and operating Security Operations Centers. I have an education in Mechanical Engineering and am a mostly self-taught infosec professional. I currently work as a network and application penetration tester in the government sector.

Description:
As OT technologies like PLCs and RTU become smarter and more capable of running standard operating systems, the concern of malware infecting OT technologies has become more of a realistic threat. In cases like Stuxnet where the attacker wishes to cause damage to a system while keeping the user unaware it must do so by modifying sensor data that would alert the user to a change in the system. State estimation is a technique used in the Power Industry to detect when sensors are providing garbage data. In this talk I plan to explain how state estimation works and how it can be applied as a technique for detecting an attacker attempting to manipulate sensor data for nefarious purposes.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 10:15-10:59 PDT

Title: Detection Challenges in Cloud Connected Credential Abuse Attacks
When: Friday, Aug 6, 10:15 - 10:59 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Rod Soto
Over 15 years of experience in information technology and security. He has spoken at ISSA, ISC2, OWASP, DEFCON, RSA Conference,Hackmiami, DerbyCon, Splunk .CONF, Black Hat,BSides, Underground Economy and also been featured in Rolling Stone Magazine, Pentest Magazine, Univision, BBC, Forbes, VICE, Fox News and CNN. Co-founder of Hackmiami, Pacific Hackers Meetups and Conferences. Co-founder of Pacific Hackers Association.

Description:

With the widespread adoption of cloud technologies, many companies are now managing environments where the line between the perimeter and the internet is blurred. This presentation outlines the challenges defenders face in the light of the implementation of new technologies that enable users to operate seamlessly between the cloud and the perimeter. A "converged" perimeter brings new attacks such as Golden SAML, Pass The SAML, Oauth Token Hijacking which are some of the manifestations of current and future challenges in these types of environments. Presenters will propose a new approach based on current attack research and new defense posture, with specific detections developed to address these new threats.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 15:00-15:25 PDT

Title: Developing Aerospace Security Training 3D Models
When: Friday, Aug 6, 15:00 - 15:25 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Kevin Hood
Kevin Hood is a Software Security Engineering Intern at Collins Aerospace, Project Manager for the Aviation ISAC Cyber Competition, and student at Embry-Riddle Aeronautical university. Kevin has focused his career in aerospace cybersecurity and develops events to bring more people into the industry.

Description:

The challenge for students interested in aerospace cybersecurity is how to jump-start their learning and prepare themselves for this career path. Developing models and simulated aerospace infrastructure can enhance critical skills needed in aerospace cybersecurity. From a student's perspective, learn how to get started in aerospace cybersecurity and the future developments of a hackable, large-scale model airport at the Aerospace Village.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=WXuT-e-Zs80

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 16:00-16:45 PDT

Title: DevSecOps: Merging Security and Software Engineering
When: Saturday, Aug 7, 16:00 - 16:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Magno Logan DELETE ME
No BIO available

Description:
Lately, we’ve been hearing a lot about Dev Ops and DevSecOps, and why they’re so important. While integrating these are considered very good practices, organizations may be unintentionally unaware of how to maximize DevOps to ensure security and compliance are being met without delays. This could be because many researchers and authors believe DevOps already includes security at its core, since software security and quality are closely related. However, in today’s cloud environment, one cannot assume that DevOps can do it all. That’s where a strong DevSecOps strategy and mindset comes into play.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Sunday - 11:00-11:59 PDT

Title: DEX trading without leaking your identity: RAILGUN
When: Sunday, Aug 8, 11:00 - 11:59 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Railgun Team
No BIO available

Description:
Railgun is a tool that offers additional privacy on Ethereum.

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 16:00-16:59 PDT

Title: DFDs Ain't That Bad
When: Friday, Aug 6, 16:00 - 16:59 PDT
Where: AppSec Village (Virtual)
Speakers: Izar Tarandach,Matthew Coles

SpeakerBio: Izar Tarandach
No BIO available

SpeakerBio: Matthew Coles
No BIO available

Description:
Threat Modeling is, at its root, a combination of two separate disciplines: system modeling and threat elicitation (and then a bit of risk management, but that’s another talk). In the last few years the industry has focused mostly on the second part, threat elicitation, and rare was the analysis of the successes and failures of system modeling. Co-authors and members of the Threat Modeling Manifesto Group, Matt & Izar offer a view from the threat modeling pit of why sometimes developers won’t model for threats, what can be done differently, and a view of their pytm tool as a collaborative (remote) system modeler tool with a threat elicitation cherry on top.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 12:00-12:59 PDT

Title: DHS REBOOTING CRITICAL INFRASTRUCTURE PROTECTION Panel with DEF CON Policy Panel
When: Friday, Aug 6, 12:00 - 12:59 PDT
Where: Track 1 Live; DCTV/Twitch #1 Live
Speakers: Lily Newman,Alexander Klimburg,Faye Francy,Eric Goldstein,Amelie Koran,Danny McPherson

SpeakerBio: Lily Newman , WIRED magazine
No BIO available

SpeakerBio: Alexander Klimburg , Director, Global Commission on the Stability of Cyberspace
No BIO available

SpeakerBio: Faye Francy , Executive Director, Automotive Information Sharing and Analysis Center
No BIO available

SpeakerBio: Eric Goldstein , Executive Assistant Director, DHS CISA
No BIO available

SpeakerBio: Amelie Koran , Senior Technology Advocate, Splunk
No BIO available

SpeakerBio: Danny McPherson , Executive Vice President & Chief Security Officer, Verisign
No BIO available

Description:

In 1998 the US government issued the first major policy document on Critical Infrastructure Protection (CIP). Since then, CIP has become one of the most fundamental tasks for governments everywhere, and has given birth to a plethora of institutions and processes seeking to manage what is called a "Public Private Partnership" between government, industry, and civil society. But despite all the efforts put into information exchanges, incident management, but also supply chain protection and even national industrial policies, cyber-attacks have not decreased, both in the United States and elsewhere. What else needs to be done? What lessons learned are there from international experiences? And how can the community help best?

This talk will be given live in Track 1, and will be streamed to DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

Title: Digital Forensics and Incident Response Against the Dark Arts: The Battle of Malicious Email and Downloaders
When: Saturday, Aug 7, 10:00 - 13:59 PDT
Where: Workshops - Las Vegas 5+6 (Onsite Only)
Speakers: Michael Register,Michael Solomon

SpeakerBio: Michael Register
Michael Register (S3curityN3rd) has 5 years of combined experience across IT, Networking, and Cybersecurity. He currently holds multiple certifications, including the GCIH. S3curityN3rd spent the last 3 years working in Incident Response before a recent transition into a Threat Hunting role. His areas of focus have been on forensics, malware analysis, and scripting.

SpeakerBio: Michael Solomon
Michael Solomon (mR_F0r3n51c5) is currently a Threat Hunter for a large managed security service provider. He has ten years of experience conducting Cyber Operations, Digital Forensics & Incident Response (DFIR), and Threat Hunting. He is very passionate about helping grow and inspire cybersecurity analysts for a better tomorrow.

Description:

Ever wondered what it is like being a cybersecurity or incident response analyst? Here is your chance to experience an exciting 4-hour class taught by mR_F0r3n51c5 and S3curityN3rd. Phishing and malicious spam attacks continue to pose a significant risk in today’s cyber threat landscape. Using forensic and malware analysis fundamentals, this class will teach students how to analyze malicious downloaders, phishing emails, and malicious spam.

Upon successful class completion, students will be able to:

Build analysis skills that leverage complex scenarios and improve comprehension. Demonstrate an understanding of forensic fundamentals used to analyze an email. Use open-source information to collect and analyze threat actor data; identify indicators of compromise, and demonstrate how to pivot on that information. Demonstrate how to analyze a malicious downloader; to include but not limited to debugging and deobfuscation. Participate in a hand to keyboard combat capstone. Students will be given a malicious file sample and demonstrate how to analyze it.

Registration Link:
https://www.eventbrite.com/e/digital-forensics-and-ir-against-the-dark-arts-las-vegas-5-6-tickets-162218185961

Prerequisites
None

Materials needed:
Students will be required to download two virtual machines (OVA files). Students will be given a URL for download access. In regards to the downloaded virtual machines, these should be imported into your virtual machine software and ready before the start of class. If any additional technical support is needed, the instructors will make themselves available online.

Students must have a laptop that meets the following requirements:

- A 64 bit CPU running at 2GHz or more. The students will be running two virtual machines on their host laptop.
- Have the ability to update BIOS settings. Specifically, enable virtualization technology such as "Intel-VT."
- The student must be able to access their system's BIOS if it is password protected. This is in case of changes being necessary.
- 8 GB (Gigabytes) of RAM or higher
- At least one open and working USB Type-A port
- 50 Gigabytes of free hard drive space, allowing you the ability to host the VMs we distribute
- Students must have Local Administrator Access on their system.
- Wireless 802.11 Capability

- A host operating system that is running Windows 10, Linux, or macOS 10.4 or later.
- Virtualization software is required. The supplied VMs have been built for out of the box comparability with VMWare Workstation or Player. Students may use other software if they choose, but they may have to troubleshoot unpredictable issues.

At a minimum, the following VM features will be needed:

- NATted networking from VM to Internet
- Copy Paste of text and files between the Host machine and VM

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Friday - 14:00-14:30 PDT

Title: Discord Practice Net
When: Friday, Aug 6, 14:00 - 14:30 PDT
Where: Ham Radio Village (Virtual Talks)

Description:

In this "demo", we'll be hosting a practice "net" (ham-speak for on-air meeting) on the #hrv-get-on-the-air-voice channel in the village. All persons, even non-hams, are invited to join us in this practice so you can become familiar with expected etiquette.

All Ham Radio Village talks will be streamed to Twitch, with discussion in Discord.

For more information, see https://hamvillage.org/dc29.html

Twitch: https://www.twitch.tv/hamradiovillage

#hrv-presentation-text: https://discord.com/channels/708208267699945503/736674835413073991

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 17:00-18:59 PDT

Title: Do No harm; Health Panel : Live version - A DEF CON Policy Panel
When: Friday, Aug 6, 17:00 - 18:59 PDT
Where: Track 1 Live; DCTV/Twitch #1 Live

SpeakerBio:DEF CON Policy Panel
No BIO available

Description:

--

This talk has been released to the DEF CON Media server.

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20C

This talk will be given live in Track 1, and will be streamed to DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Friday - 12:30-12:59 PDT

Title: Do We Really Want to Live in the Cyberpunk World?
When: Friday, Aug 6, 12:30 - 12:59 PDT
Where: ICS Village (Virtual)

SpeakerBio: Mert Can Kilic , Barikat Cyber Security
MsC. Comp. Engineer, Tinker, Maker, Love Legos

Description:
What are the possible future threats when it comes to cyber physical systems? Human augmentations, insulin pumps, and brain computer interfaces are inevitable, but how will their security and possible incidents affect our world?

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 12:00-12:20 PDT

Title: Do you like to read? I know how to take over your Kindle with an e-book
When: Friday, Aug 6, 12:00 - 12:20 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Slava Makkaveev
Slava Makkaveev is a Security Researcher at Check Point Software Technologies Ltd. Holds a PhD in Computer Science. Slava has found himself in the security field more than ten years ago and since that gained vast experience in reverse engineering and vulnerability research. Recently Slava has taken a particularly strong interest in mobile platforms and firmware security.

Description:

Since 2007, Amazon has sold tens of millions of Kindles, which is impressive. But this also means that tens of millions of people can be hacked through a software bug in those same Kindles. Their devices can be turned into bots, their private local networks can be compromised, and perhaps even information in their billing accounts can be stolen.

The easiest way to remotely reach a user's Kindle is through an e-book. A malicious book can be published and made available for free access in any virtual library, including the Kindle Store, or sent directly to the end-user device via Amazon services. While you might not be happy with the writing in a particular book, nobody expects to download one that is malicious. No such scenarios have been publicized. Antiviruses do not have signatures for e-books. But... we succeeded in making a malicious book for you. If you open this book on a Kindle device, it causes a hidden piece of code to be executed with root rights. From this moment on, you lost your e-reader, account and more.

Want to know the details?

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=1jM_r-pe8Ss

Media
(Main Talk)
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%2

(Demo)
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20S

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Friday - 16:30-17:30 PDT

Title: Do You Really Own Your NFTs?
When: Friday, Aug 6, 16:30 - 17:30 PDT
Where: Blockchain Village / Paris Vendome B
Speakers: Francesco Piccoli,Steven Yang

SpeakerBio: Francesco Piccoli
No BIO available

SpeakerBio: Steven Yang , ANCHAIN
No BIO available

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 17:00-17:59 PDT

Title: Don't Dare to Exploit - An Attack Surface Tour of SharePoint Server
When: Saturday, Aug 7, 17:00 - 17:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Steven Seeley,Yuhao Weng,Zhiniang Peng

SpeakerBio: Steven Seeley
Steven Seeley (@mr_me) is a member of the 360 Vulcan team and enjoys finding and exploiting bugs. Currently his focus is on web and cloud tech and has over 10 years experiance in offensive security. Steven won the Pwn2Own Miami competition with his team mate Chris Anastasio in early 2020 and has taught several classes in web security including his own, Full Stack Web Attack.
Twitter: @steventseeley

SpeakerBio: Yuhao Weng
Yuhao Weng(@cjm00nw) is an security researcher of Sangfor and a ctf player of Kap0k. He has been studying the web for three years and found a lot bugs in Sharepoint, Exchange and so on. Now he is focused on .NET security.
Twitter: @cjm00nw

SpeakerBio: Zhiniang Peng
Dr. Zhiniang Peng (@edwardzpeng) is the Principal Security Researcher at Sangfor. His current research areas include applied cryptography, software security and threat hunting. He has more than 10 years of experience in both offensive and defensive security and published much research in both academia and industry.
Twitter: @edwardzpeng

Description:
Due current global issues of 2020, organizations have been forced to make changes in how their business model operates and as such, have opened the doors to remote working. Microsoft SharePoint is one of the most popular and trusted Content Management System's (CMS) deployed today. The product is used to share and manage content, internal knowledge with embeded applications to empower teamwork and seamlessly collaborate across an organization for a truly remote experience.

After the efforts of countless talented engineers in Microsoft, SharePoint has been deployed in the Microsoft cloud as part of their office 365 offering. This presentation will analyze the security architecture of SharePoint server and how it differs from other popular CMS products. From an offensive point of view, we will also reveal several attack surfaces and mitigations implemented and how those mitigations can be bypassed. Finally we will disclose several high impact vulnerabilities detailing the discovery and exploitation.

REFERENCES

1. http://russiansecurity.expert/2016/04/20/mysql-connect-file-read/ 2. https://docs.microsoft.com/en-us/dotnet/api/system.web.ui.control 3. https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms524602(v=vs.90) 4. https://www.youtube.com/watch?v=Xfbu-pQ1tIc 5. https://www.blackhat.com/us-20/briefings/schedule/#room-for-escape-scribbling-outside-the-lines-of-template-security-20
6. https://www.spguides.com/sharepoint-csom-tutorial/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=mVXrl4W1jOU

Media:

https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20Y

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 14:00-14:25 PDT

Title: Don’t fear the BUS, it won’t run you over.

When: Friday, Aug 6, 14:00 - 14:25 PDT

Where: Aerospace Village (Virtual Talk)

SpeakerBio: Nicholas Childs

Nicholas Childs Is a USAF aircraft maintainer with experience with mechanical, electronic, hydraulic, and avionics systems with both military and civilian aerospace platforms. He has worked on C-5, C-17, KC-135, B-1, 737, 747, and L10-11 platforms. With a focus on security he scrutinizes them.

Description:

This talk is a basic introduction to aircraft avionics comm/nav bus systems and the expansion of the network to more vulnerable areas than have seen before. It is more of a primer and 101 for stepping into a the larger world of aerospace networks.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=eiO7F5isPE8

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Friday - 15:00-15:30 PDT

Title: Doors, Cameras, and Mantraps OH MY!
When: Friday, Aug 6, 15:00 - 15:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio: Dylan The Magician
No BIO available

Description:

Lockpicking, door bypassing, and physical security are among the more eye catching components of an on premises risk assessment. It always draws the most questions and gets the most staff popping over to see what's going on. I suppose it's because the physical space is personal, it isn't digital and hence it draws more focus. I do on premises risk assessment and I want to tell you a bit about how the process goes with my company and share my personal philosophies on how I do my engagements. What I hope to gain is a stronger focus on Physical Security, or PhysSec, in the Cybersecurity domain.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 12:00-12:45 PDT

Title: DoS: Denial of Shopping – Analyzing and Exploiting (Physical) Shopping Cart Immobilization Systems
When: Sunday, Aug 8, 12:00 - 12:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Joseph Gabay
Joseph is a robotics engineer in Boston, Massachusetts where he works on a variety of projects ranging from electromechanical designs to embedded systems.

His passion lies in further understanding the way the world works and uncovering the small secrets that we encounter in our day to day lives. This project started as an idle curiosity and grew into an opportunity to further explore the complex and deep world of RF communications and embedded systems.

Joseph is an avid part of the local maker community, with extensive experience in 3D printing, rapid-fabricobbling, and breaking stuff for fun and profit. Outside of his day job, he enjoys woodworking and metalworking and is constantly collecting new hobbies and interests.

Description:

Many supermarkets and shopping centers have implemented devices that “lock” their shopping carts if they’re taken outside of an approved boundary (e.g, a parking lot). This talk examines some of the technology that’s used to do this, as well as ways to capture and spoof the control signals to defeat these devices.

We will go over the anatomy of remotely lockable shopping cart wheels, their basic theory, and get into how they’re controlled. We’ll deconstruct some samples of the lock and unlock signals captured using a homemade antenna and a HackRF, and briefly discuss methods of rebroadcasting them – as well as the challenges inherent to this process.

DISCLAIMER
This talk is the result of a personal project.

Any views, opinions, or research presented in this talk are personal and belong solely to the presenter. They do not represent or reflect those of any person, institution, or organization that the presenter may or may not be associated with in a professional or personal capacity unless explicitly stated otherwise.

REFERENCES

- The ARRL handbook for radio communications, 2007. Newington, CT: American Radio Relay League, 2006. Print.
- https://www.tmplab.org/2008/06/18/consumer-b-gone/
- http://www.woodmann.com/fravia/nola_wheel.htm -The wonderful people over at /r/rfelectronics -FCC.gov

--

This talk has been released to the DEF CON Media server.

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20J

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 15:00-15:50 PDT

Title: Drone Security Research Series – Ep6 Hacking with drones
When: Saturday, Aug 7, 15:00 - 15:50 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Matt Gaffney
Following his career in the British Army, Matt has been working with clients in various industries. However, his best years were spent working in aviation, specifically systems found in the Aircraft Information Systems Domain. More recently he has turned his attention to security in UAS.

Description:

In this series we have uncovered weaknesses in the MAVLink protocol, now we attempt to overcome physical security controls by getting within range of WiFi networks with a drone. In this episode we use a drone to get close to our target by taking the tools airborne and flying over our target. Let's rewrite the physical security model!

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=M0BDHT43Ucc

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 20:00-21:59 PDT

Title: Drunk Hacker History

When: Saturday, Aug 7, 20:00 - 21:59 PDT

Where: See Description

Description:

This event will be held in Track 1 / Bally's Platinum Ballroom. This event was rescheduled from 22:00 to 20:00.

Twitter: https://twitter.com/drunkhackerhist?lang=en

Return to Index - Add to Google Calendar - ics Calendar file

Title: eBPF, I thought we were friends!

When: Friday, Aug 6, 13:00 - 13:59 PDT

Where: DCTV/Twitch #3 Pre-Recorded

Speakers: Guillaume Fournier,Sylvain Afchain,Sylvain Baubeau

SpeakerBio: Guillaume Fournier

Guillaume Fournier is a Security Engineer at Datadog where he focuses on developing a new generation of runtime security tools powered by eBPF. In his free time, he likes to build defensive and offensive security tools such as a chrome-like sandbox for VLC on Linux, or various projects to automate drones and wireless keyboards hacking.
Twitter: @gui774ume

SpeakerBio: Sylvain Afchain

Sylvain Afchain is a staff software engineer at Datadog. He's been working on linux for more than 15 years. He mostly worked on distributed systems, cloud infrastructure and SDN solutions. In his spare time, he enjoys cycling, playing tennis and badminton.

SpeakerBio: Sylvain Baubeau

Sylvain Baubeau is a staff software engineer, mostly working on Linux, cloud and infrastructure technologies. In his spare time, he likes to play drums, reverse engineer old games and build arcades.

Description:

Since its first appearance in Kernel 3.18, eBPF (Extended Berkley Packet Filter) has progressively become a key technology for observability in the Linux kernel. Initially dedicated to network monitoring, eBPF can now be used to monitor and trace any kind of kernel space activity.

Over the past few years, many vendors have started using eBPF to speed up their services or introduce innovative features. Cilium, Calico, Cloudflare, Netflix and Facebook are leading the charge, showing off new complex networking use cases on a monthly basis. On the security side of things, Google recently contributed the Kernel Runtime Security Instrumentation which opens the door to writing Linux Security Modules with eBPF.

In other words, eBPF is the new kid in town and a growing number of companies are running services with eBPF access in production. This leads us to a simple question: how bad can things get if one of those services were to be compromised ? This talk will cover how we leveraged eBPF to implement a full blown rootkit with all the features you would expect: various obfuscation techniques, command and control with remote and persistent access, data theft and exfiltration techniques, Runtime Application Self-Protection evasion techniques, and finally two original container breakout techniques.

Simply put, our goal is to demonstrate that rogue kernel modules might have finally found a worthy opponent. We will also detail how to detect such attacks and protect your infrastructure from them, while safely enjoying the exciting capabilities that eBPF has to offer.

REFERENCES

Bibliography and documentation links cited in the submission:

1. Russian GRU 85th GTsSS deploys previously undisclosed drovorub malware, NSA / FBI, August 2020 https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_
2. Kprobe-based Event Tracing, https://www.kernel.org/doc/html/latest/trace/kprobetrace.html
3. Linux Kernel tracepoints, https://www.kernel.org/doc/html/latest/trace/tracepoints.html
4. “bpf_probe_write_user” bpf helper, https://elixir.bootlin.com/linux/v5.11.11/source/include/uapi/linux/bpf.h#L1472
5. Uprobe-based Event Tracing, https://www.kernel.org/doc/html/latest/trace/uprobetracer.html
6. Cilium’s XDP documentation, https://docs.cilium.io/en/latest/bpf/#xdp

Previous eBPF related talks & projects that helped us build the rootkit:

7. Evil eBPF In-Depth: Practical Abuses of an In-Kernel Bytecode Runtime, Jeff Dileo, DEF CON 27, https://www.defcon.org/html/defcon-27/dc-27-speakers.html#Dileo 8. Process level network security monitoring and enforcement with eBPF, Guillaume Fournier, https://www.sstic.org/2020/presentation/process_level_network_security_monitoring_and_enforcement_with_ebpf/

9. Runtime Security with eBPF, Sylvain Afchain, Sylvain Baubeau, Guillaume Fournier, https://www.sstic.org/2021/presentation/runtime_security_with_ebpf/ 10. Monitoring and protecting SSH sessions with eBPF, Guillaume Fournier, https://www.sstic.org/2021/presentation/monitoring_and_protecting_ssh_sessions_with_ebpf/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=5zixNDolLrg

Media: https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20C

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 17:00-19:59 PDT

Title: EFF Tech Trivia
When: Friday, Aug 6, 17:00 - 19:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236425

This event will be streamed to Twitch with chat in Discord.

Twitch: https://www.twitch.tv/efflive

#ce-eff-tech-trivia-text: https://discord.com/channels/708208267699945503/711644552573747350/

Return to Index - Add to Google Calendar - ics Calendar file

Title: Empire
When: Friday, Aug 6, 14:00 - 15:50 PDT
Where: Palace 3+4+5
Speakers: Anthony "Cx01N" Rose,Vincent "Vinnybod" Rose

SpeakerBio: Anthony "Cx01N" Rose , Lead Security Researcher
Anthony "Cx01N" Rose, CISSP, is the Lead Security Researcher at BC Security, where he specializes in adversary tactic emulation planning, Red and Blue Team operations, and embedded systems security. He has presented at numerous security conferences, including Black Hat, DEF CON, and RSA conferences. Cx01N is the author of various offensive security tools, including Empire and Starkiller, which he actively develops and maintains. He is recognized for his work, revealing wide-spread vulnerabilities in Bluetooth devices and is the co-author of a cybersecurity blog at https://www.bc-security.org/blog/.

SpeakerBio: Vincent "Vinnybod" Rose , Lead Tool Developer
Vincent "Vinnybod" Rose is the Lead Tool Developer for Empire and Starkiller. He is a software engineer with expertise in cloud service and has over a decade of software development and networking experience. Recently, his focus has been on building ad-serving technologies, web and ad-tracking applications. Vinnybod has presented at Black Hat has taught courses at DEF CON on Red Teaming and Offensive PowerShell. He currently maintains a cybersecurity blog focused on offensive security at https://www.bc-security.org/blog/.

Description:
Tool or Project Name: Empire

Short Abstract (What is your tool, what does it do?): Empire is a Command and Control (C2) framework powered by Python 3 that supports Windows, Linux, and macOS exploitation. It leverages many widely used offensive security tools through PowerShell, Python 3, and C# agents. At the same time, it offers cryptologically-secure communications and flexible modular architecture that links Advanced Persistent Threats (APTs) Tactics, Techniques, and Procedures (TTPs) through the MITRE ATT&CK database.

Empire has evolved significantly since its introduction in 2015 and has become one of the most widely used open-source C2 platforms. Through this time, Empire has advanced from a single user experience to allowing multiple user operations through an API with Empire acting as a teamserver. Currently, 2 different applications are available to connect to the Empire teamserver: Empire Command Line Interface (CLI) and Starkiller.

The Empire CLI is built from the ground up as a replacement to the embedded legacy CLI and gives users a familiar feel of the legacy CLI, but is portable and connects through the Empire API. While Starkiller is a cross-platform UI available in Linux, Windows, and macOS powered by ElectronJS.

The framework's flexibility to easily incorporate new modules allows for a single solution for red team operations with the aim for Empire to provide an easy-to-use platform for emulating APTs. Customization is essential to any successful red team operation, which has driven the expansion of user plugins. These plugins allow any custom program to run side-by-side with the Empire teamserver. In addition, the commonality between other C2 platforms allows profiles and modules to be easily dropped in without the need for additional development. These features allow both red and blue teams to easily emulate and defend against the APT attack vectors.

Short Developer Bio:
Vincent "Vinnybod" Rose is the Lead Tool Developer for Empire and Starkiller. He is a software engineer with expertise in cloud service and has over a decade of software development and networking experience. Recently, his focus has been on building ad-serving technologies, web and ad-tracking applications. Vinnybod has presented at Black Hat has taught courses at DEF CON on Red Teaming and Offensive PowerShell. He currently maintains a cybersecurity blog focused on offensive security at https://www.bc-security.org/blog/.

Anthony "Cx01N" Rose, CISSP, is the Lead Security Researcher at BC Security, where he specializes in adversary tactic emulation planning, Red and Blue Team operations, and embedded systems security. He has presented at numerous security conferences, including Black Hat, DEF CON, and RSA conferences. Cx01N is the author of various offensive security tools, including Empire and Starkiller, which he actively develops and maintains. He is recognized for his work, revealing wide-spread vulnerabilities in Bluetooth devices and is the co-author of a cybersecurity blog at https://www.bc-security.org/blog/.

URL to any additional information:
Blogs about new Empire and Starkiller features: https://www.bc-security.org/post/emp...tarkiller-1-6/ https://www.bc-security.org/post/return-of-the-cli/ https://www.bc-security.org/post/emp...e-c2-profiles/ https://www.bc-security.org/post/an-...to-starkiller/ Video walk through of new features: https://www.youtube.com/watch?v=v4nzXCHGzUA https://www.youtube.com/watch?v=CzZmzBIVJHA Detailed Explanation of Tool:
Empire has been a well-established versatile Command and Control (C2) framework for many years. Our work has allowed better adoption by red teams and shifts the focus of the platform to threat emulation. Threat emulation has been enhanced by leveraging a MITRE ATT&CK framework-based database. Every module is tagged with the MITRE ATT&CK techniques that most closely relate to the objectives of that tool and allows operators to search through the database to find and use tools that meet their specific threat emulation plan. This is combined with the new Empire server/client architecture, which has 2 different applications to connect through Starkiller and Empire Command Line Interface (CLI), allowing for multi-user distributed operations. Starkiller is a cross-platform UI available in Linux, Windows, and macOS for interacting with the Empire post-exploitation framework. This application allows red teams to share any instance of Empire and support remote, multi-operator engagements for instant collaboration and efficient event tracking. Each user is tracked in a database, which can be queried to evaluate team progression and generate post-engagement reports. Within a few minutes, a red-teamer can set up a listener (call back server) on Empire, get a target (agent) calling back to that server, and send payloads to it. Not only that, but multiple users can be working with those same agents, 3rd party modules, and listeners. There is no need to duplicate effort in establishing independent red team infrastructures when a common interface can now be used with the enhanced Empire API. When viewing an agent in the interface, we can get live updates of tasks queued to it, which users set that task, and the results.

The Empire CLI is built from the ground up as a replacement to the embedded legacy CLI that was packaged with Empire. This adaption allows users to continue to run an interface that gives the look and feel of the legacy CLI, but is portable and connects through the Empire API. While building this, we looked for areas to improve and constructed it using Python Prompt Toolkit, which gives users a streamlined look with drop-down menus, interactive shell, and multiple user support. While many of these new improvements are still in their early stages, we believe that the new construct for Empire will drive a significant change in how teams use the tool in the future.

Supporting Files, Code, etc:
https://github.com/BC-SECURITY/Empire
https://github.com/BC-SECURITY/Empire-Cli https://github.com/BC-SECURITY/Starkiller

Target Audience:
Offense

These updates bring Empire into parity with some of the top paid Offense tool kits allowing students to gain exposure to how advanced TTPs and teaming workflows are utilized in offensive engagements.

We picked up the project back in August 2019. We actually were teaching a workshop using Empire and were contacted by Kali if we would be interested in publishing our Python 3 copy around November that year. They were wanting to drop Python 2 support but didn’t want to lose older tools. And we have been pushing updates ever since.

What we have done so far?
We designed an API that supports multiple users at once and collaboration within the c2. Added over 30 new tools within the framework, including socks proxy, Rubeus, and seatbelt. Added a graphical user interface, Starkiller. Threat emulation is a big thing that we are pushing for, so we went through at tagged every tool with a MITRE ATT&CK technique which links back to the source material and descriptions of the attack. We also added a cross-compatibility ability that uses Cobalt Strikes

malleable C2 profiles to create malleable listeners in Empire.

Where are we going?
Empire 4.0, which is our current version in development. This is nearly a complete rewrite of the project and almost a new C2. The project now uses a server/client architecture that aligns itself with modern C2s, such as Cobalt Strike, PoshC2, and Silent Trinity.

We added C **implants with on-the-fly compilation using Roslyn Compiler. This ability is something that everyone has been asking about for a while since most advanced frameworks support some flavor of C** implants. We wanted to implement this in a way that allows us to have cross-compatibility with Covenant’s tools but still maintain Empire’s agent capabilities and formatting. What we ended up with is the capability to run C **implants that can compile their modules and use all the PowerShell tools as well. Another advantage of this is that PowerShell agents can compile c** tools on the fly as well.

Visually, we completely redid the CLI to be streamlined and includes new features like dropdown menus, server chatrooms, and suggested values.

We redesigned the plugin functionality within Empire and significantly expanded its capabilities. Plugins are a lesser-known ability which allows user to specially craft tools that can enhance the framework's capabilities. This is similar to how cobalt strike uses aggressor scripts to expand its capabilities.

Return to Index - Add to Google Calendar - ics Calendar file

APV - Sunday - 10:00-10:45 PDT

Title: Encryption for Developers
When: Sunday, Aug 8, 10:00 - 10:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: James McKee (punkcoder)
No BIO available

Description:
Encryption has become a major part of the implementation of many products, but how many of us really understand what is going on behind the scenes. During your implementation, do you really know what an initialization vector does? What is the difference between AES-CBC and AES-CFB, and when should you use one over the other? How do you store the decryption key to prevent the same code leaking both the data and the key?

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

RFV - Thursday - 12:00-11:59 PDT

Title: ESP8266, do you know what's inside your IoT?

When: Thursday, Aug 5, 12:00 - 11:59 PDT

Where: Radio Frequency Village (Virtual)

SpeakerBio: JoshInGeneral

Joshua Schroeder would describe himself as a security researcher that enjoys learning and advocating for people to get involved in RF and Cyber Security. His professional work includes working as a Unix Administrator, Incident Responder and Red Teamer.

As a long time Wireless CTF competitor, he led the Team JackTenna to a win in 2017. Attempting to share his knowledge with others, he previously spoke at the Defcon Wireless Village (Now RF Village) on 802.11 and 802.15 technologies (WiFi and Bluetooth) and later wrote and published the book ""Meeting People via Wifi and Bluetooth"". Prior speaking engagements also include ShmooCon, SkyDogCon, and Carolina Con.

In his free time he enjoys spending time with his wife and their dog, remodeling their house and tinkering with smart home technologies.

Description:

In this presentation we will look through together the inner workings of the ESP8266 chip. A common technology that is at the heart many IoT devices. I will demonstrate where I found this in a IoT switch and how you can identify and find them as well. Lastly I will show how the ESP8266 chip can be purchased for under $20 and deployed with a small as a decoy AP to capture credentials. Similar to what our team built and during the Wireless CTF in 2019.

This talk has been released to YouTube.

YouTube: https://www.youtube.com/watch?v=DIh-y5n_lDg

Radio Frequency Village will not be streaming any talks, but they will be making talks available on their YouTube channel.

YouTube: https://youtube.com/c/RFHackersSanctuary

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Saturday - 12:00-12:59 PDT

Title: Ethereum Hacks & How to Stop Them
When: Saturday, Aug 7, 12:00 - 12:59 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Michael Lewellen , Project Manager - Security Services, OpenZeppelin
Michael works as the Technical Project Manager for the Security Research team managing audit projects. Michael has 9 years of experience as a software consultant and architect working on blockchain technologies. Outside of OpenZeppelin, Michael educates on blockchain technology as a lecturer at UT Dallas and a public policy advisor as part of the Texas Blockchain Council.

Description:
Learn about some of the recent smart contract security incidents and how to stop them using OpenZeppelin security tools like Defender.

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 15:45-16:15 PDT

Title: Ethics at the Edge: IoT as the Embodiment of AI for Rampant Intelligence Actuation
When: Saturday, Aug 7, 15:45 - 16:15 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Ria Cheruvu
Ria Cheruvu is an AI Ethics Lead Architect at the Intel Network and Edge engineering group working on developing trustworthy AI products. She is 17 years old, and graduated with her bachelor's degree in computer science at Harvard University at 11 and her master's degree in data science from her alma mater at 16. Her pathfinding domains include solutions for security and privacy for machine learning, fairness, explainable and responsible AI systems, uncertain AI, reinforcement learning, and computational models of intelligence. She enjoys composing piano music, ocean-gazing with her family, and contributing to open-source communities in her free time.

Description:

In the eyes of a smart device and their human controllers, the world is an immense source of data and power. The expanding Internet of Things ecosystem only adds fuel to this, empowering real-time automatic sensing + actuation posing regulatory dilemmas, easily exploitable definitions of trusted entities (e.g., see the 2021 Verkada hack), and measurements of security, robustness, and ethics that change apropos data in the blink of an eye.

Governance and policing of Internet of Things devices is growing to cover the upcoming trail of destruction by flailing technical solutions, but some intriguing key unanswered questions are starting to reveal themselves.

In this talk, we'll dive into what the sociotechnical problem of ethics means at the edge in the context of machine learning/artificial intelligence and address these questions:

1. Individual vectors of ethics ("Sustainability is an ethical principle?" "Edge devices have their own definition of fairness and bias different from human concepts?")
2. Evolving principles and governance for IoT devices, and the importance of accountable anonymity
3. Definitions of trusted entities ("When are users a threat?" "Should humans be out of the loop?"), and how key ethical principles, such as privacy and transparency, can be a double-edged sword in the context of IoT security.
4. Incorporating morality into machines is now a reality ("How do we define a calculus and value alignment for IoT ethics?") - what are key unconventional ethical concerns for human-centered design?

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Evading Detection a Beginner's Guide to Obfuscation
When: Saturday, Aug 7, 15:00 - 18:59 PDT
Where: Workshops - Las Vegas 3+4 (Onsite Only)
Speakers: Anthony "Cx01N" Rose,Jake "Hubbl3" Krasnov,Vincent "Vinnybod" Rose

SpeakerBio: Anthony "Cx01N" Rose , Lead Security Researcher
Anthony "Cx01N" Rose, CISSP, is the Lead Security Researcher at BC Security, where he specializes in adversary tactic emulation planning, Red and Blue Team operations, and embedded systems security. He has presented at numerous security conferences, including Black Hat, DEF CON, and RSA conferences. Cx01N is the author of various offensive security tools, including Empire and Starkiller, which he actively develops and maintains. He is recognized for his work, revealing wide-spread vulnerabilities in Bluetooth devices and is the co-author of a cybersecurity blog at https://www.bc-security.org/blog/.

SpeakerBio: Jake "Hubbl3" Krasnov , Red Team Operations Lead
Jake "Hubbl3" Krasnov is the Red Team Operations Lead at BC Security. He has spent the first half of his career as an Astronautical Engineer overseeing rocket modifications for the Air Force. He then moved into offensive security, running operational cyber testing for fighter aircraft and operating on a red team. Hubbl3 has presented at DEF CON, where he taught courses on offensive PowerShell and has been recognized by Microsoft for his discovery of a vulnerability in AMSI. Jake has authored numerous tools, including Invoke-PrintDemon and Invoke-ZeroLogon, and is the co-author of a cybersecurity blog at https://www.bc-security.org/blog/.

SpeakerBio: Vincent "Vinnybod" Rose , Lead Tool Developer
Vincent "Vinnybod" Rose is the Lead Tool Developer for Empire and Starkiller. He is a software engineer with expertise in cloud service and has over a decade of software development and networking experience. Recently, his focus has been on building ad-serving technologies, web and ad-tracking applications. Vinnybod has presented at Black Hat has taught courses at DEF CON on Red Teaming and Offensive PowerShell. He currently maintains a cybersecurity blog focused on offensive security at https://www.bc-security.org/blog/.

Description:

Defenders are constantly adapting their security to counter new threats. Our mission is to identify how they plan on securing their systems and avoid being identified as a threat. This is a hands-on class to learn the methodology behind malware delivery and avoiding detection. This workshop explores the inner workings of Microsoft's Antimalware Scan Interface (AMSI), Windows Defender, and Event Tracing for Windows (ETW). We will learn how to employ obfuscated malware using Visual Basic (VB), PowerShell, and C# to avoid Microsoft's defenses. Students will learn to build AMSI bypass techniques, obfuscate payloads from dynamic and static signature detection methods, and learn about alternative network evasion methods.

In this workshop, we will:

i. Understand the use and employment of obfuscation in red teaming. ii. Demonstrate the concept of least obfuscation. iii. Introduce Microsoft's Antimalware Scan Interface (AMSI) and explain its importance. iv. Demonstrate obfuscation methodology for .NET payloads.

Registration Link:
https://www.eventbrite.com/e/evading-detection-a-beginners-guide-to-obfuscation-las-vegas-3-4-tickets-162219734593

Prerequisites
Basic level of PowerShell or C# experience.

Materials needed:

- Laptop
- VMWare or Virtual Box
- Windows Dev machine or other Windows VM - Kali Linux VM

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 12:30-12:55 PDT

Title: Evaluating Wireless Attacks on Real-World Avionics Hardware
When: Friday, Aug 6, 12:30 - 12:55 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Leeloo Granger
Leeloo is a Swiss-French undergraduate student in Communication Systems at EPFL, currently in exchange at ETH Zürich. She is currently learning to become a private pilot and has an interest in avionics security avionics. Besides her studies, she is an athlete in archery currently training for the 2024 Olympics.

Description:

In a nutshell, in this project we prove the critical vulnerabilities of GPS and ADS-B technologies which only had been theoretically discussed in the literature. To do so, we investigated the feasibility and accessibility of GPS and Mode S spoofing on an avionics lab – the Garmin's Navigator GTN750 – and using two types of transmitters: the USRP B210 and Raceologic's LabSat Wideband 3. We successfully spoofed the GPS position of the GTN750, as well as intruders on the Traffic detection system. Unfortunately, we were not able to attack the TCAS II. Our work shows the vulnerabilities of communication technologies that have a major role in the safety of an aircraft, hence attacks are a severe threat and all the more so if they are conducted using as few resources as we did.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=QtM47OmprfQ

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 15:45-16:45 PDT

Title: Everything is a C2 if you're brave enough
When: Friday, Aug 6, 15:45 - 16:45 PDT
Where: Adversary Village (Virtual)
Speakers: Luis Ángel Ramírez Mendoza,Mauro Cáseres Rozanowski

SpeakerBio: Luis Ángel Ramírez Mendoza
No BIO available

SpeakerBio: Mauro Cáseres Rozanowski
Mauro Eldritch is an Argentine Hacker & Speaker, Founder of BCA and DC5411. He was a Speaker at DEF CON (six times!), ROADSEC (LATAM's biggest security conference), DEVFEST Siberia, DragonJAR Colombia (biggest spanish-speaking conference in LATAM), P0SCON Iran, Texas Cyber Summit and EC-Council Hacker Halted among other conferences (25+).

In the past, he worked for many government organisms such as Ministry of Security, Federal Revenue Administration, Ministry of Health, Ministry of Economy, Ministry of Production and both SecBSD & FreeBSD Projects.

Twitter: @mauroeldritch

Description:

It is truly amazing how many and diverse methods an attacker has to "call home", exfiltrate information, or coordinate the next steps in his chain of attack. In this talk we will demonstrate (and automate) the most wacky, unexpected, and interesting methods for setting up a C2 server: Messaging apps? social media profiles? video games or gaming platforms? Yes, and there's more. The more sacred and innocent an app appears to be, the higher the score for us when weaponizing it. We will explain from scratch the function, the construction and even the automation with Ruby and Python of C2 servers based on a wide range of applications of common and daily use. For this we will use a fake toy ransomware, which will try to call home, exfiltrate information and coordinate an attack in the most crazy,bizarre and above all ... unexpected ways. Lots of short demos make this talk suitable to both newcomers and experienced people.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Saturday - 15:00-15:59 PDT

Title: Evils in the DeFi world
When: Saturday, Aug 7, 15:00 - 15:59 PDT
Where: Blockchain Village / Paris Vendome B
Speakers: Minzhi He,Peiyu Wang

SpeakerBio: Minzhi He
No BIO available

SpeakerBio: Peiyu Wang , Sr. Security Engineer CertIK
Peiyu Wang is a Senior Security Engineer at CertiK with years of professional experience in security assessments and blockchain technology, specializing in application penetration testing and smart contract audit. Prior to joining the CertiK, Peiyu was a security consultant at Harbor Labs and NCC group, where he focused on medical device security, software development and security assessments. Peiyu holds a Master's degree in information security from Johns Hopkins University, as well as professional industry certifications, which include Offensive Security Certified Professional(OSCP) and Offensive Security Web Expert (OSWE)

Description:

The growth of DeFi for the past year is astonishing, the TVL, users count and different types of projects prove the concept of DeFi can work. The space has good DeFi projects that bring users and investors. It also has projects that are complete scams; they come up with different ways to scam people and run away with user's money. Scammers have stolen millions of dollars worth of tokens from users for the past years.

How can regular users identify bad projects? What can a security company do to help DeFi users and investors? We can't stop scammers from deploying contracts on the blockchain and setting up fake websites, but we can warn users to stay away from them. CertiK set up a submission form on our website for community members to report risky projects, and we will investigate them. If we find the project is risky, we will publish an alert on our website and Twitter account.

We reviewed more than 50 submissions from community members and identified around 15 risky projects in the past. At the Defcon blockchain village, we want to share our work for the past couple of months. In this talk, we will do a case study to demonstrate different types of scams; we will also talk about how scammers earn trust from users and how we investigate user submitted projects.

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 14:45-15:45 PDT

Title: Exploiting Blue Team OPSEC failures with RedELK
When: Friday, Aug 6, 14:45 - 15:45 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Marc Smeets , Red Teamer, Outflank
Marc is from Infosec class 1999 (hobby) and 2006 (professionally). With a strong background in system and network engineering, he switched to pentesting in 2006. In 2016 he co-founded Outflank, a boutique red teaming and adversary simulation company in Amsterdam. He helps international customers on a daily base. Besides working for his clients, Marc spends his time making tools to optimise the red teamer's workflow, a.o. RedELK. Besides infosec, Marc is a great fan of fast cars and champagne.

Description:

Blue teams and CERTs are increasingly better equipped and better trained. At the same time offensive infrastructures are increasingly diverse in components and growing in size. This makes it a lot harder for red teams to keep oversight but also a lot easier for blue teams to react on the traces that red teams leave behind. However, do blue teams really know what traces they leave behind when doing their investigation and analyses? RedELK was created and open sourced to help red teams with these two goals: 1) make it easy to have operational oversight, 2) abuse blue team OPSEC failures. Come to this talk to learn about blue team detection and how RedELK can help you.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 11:45-12:05 PDT

Title: Exploiting the O365 Duo 2FA Misconfiguration (Lightning Talk)
When: Friday, Aug 6, 11:45 - 12:05 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Cassandra Young
Cassandra is a Senior Scientist at Security Risk Advisors, focusing on Cloud Security architecture and engineering. She is concurrently pursuing a Masters degree in Computer Science, with notable work including academic research on serverless/microservices security, cloud-based app development, and privacy & anonymity technologies. She is also one of the directors of Blue Team Village, a not-for-profit organization bringing free Blue Team talks, workshops and more to the broader InfoSec community.
Twitter: @muteki_rtw

Description:

A common methodology used by companies to implement Duo 2-factor authentication for O365 can, if not configured properly, result in a loophole that allows mobile clients to authenticate without being prompted. This short talk will provide background on the authentication types involved, show the incomplete configuration, and demonstrate how to exploit using mobile devices.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

Title: Extension-Land: exploits and rootkits in your browser extensions
When: Sunday, Aug 8, 13:00 - 13:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Barak Sternberg
Barak Sternberg is an Experienced Security Researcher who specializes in Offensive Security. Founder of "WildPointer", and previously an author at SentinelLabs ("Hacking smart devices for fun and profit", Defcon 2020 IoT Village) and leading innovative cybersecurity research.

Barak spent more than six-years at Unit 8200, IDF, as a team leader of 5-10 security researchers. He is highly skilled in offensive cyber-security, from vulnerabilities research in various areas: Linux, IoT, embedded and web-apps to analyzing malware in the wild. Barak is also a CTF's addict, posting write-ups and technical vulnerabilty analysis in its blog (livingbeef.blogspot.com). Barak also acquires BSc, MSC (in CS) focused on algorithms from Tel-Aviv University and a DJ certificate from BPM college.

https://livingbeef.blogspot.com/
https://www.linkedin.com/in/barakolo/
https://www.barakolo.me

Twitter: @livingbeef

Description:

Browser extensions are installed anywhere, they serve as an integral part of our day-to-day web routine, from AdBlockers to Auto-Translators. But - do we know what is running inside of them? Do we know what goes deep-down inside their communication routines? How do they use their internal API’s? And how do their different JS execution contexts work?

In this session, I will explore these unique internal extension API’s, hidden attack-surfaces and show how these concepts can be broken & exploited using new ways! I start showing how an attacker can "jump" from one low-permissions chrome-app/extension to another, hence elevating its permissions. Then, I will show how to gain full "browser-persistency" inside extensions' background-scripts context.

Chaining it all together, I show how attacker, starting from low permissions chrome-app, gains a fully-armed "extension-rootkit", a persistent JS-malware running inside of a “good” extension, along with C&C features, JS injection techniques to any tab/origin, obfuscation-techniques and more. Eventually, I will present a generic technique, targeting all chrome-users, for taking over any previously installed chrome extension and implant an "extension-rootkit" in it.

REFERENCES

[1] Chrome Developers: Chrome extensions API Reference, https://developer.chrome.com/docs/extensions/reference/
[2] Chrome Developers: Chrome extensions Manfiest v2/v3 Security References, https://developer.chrome.com/docs/extensions/mv2/getstarted/ & https://developer.chrome.com/docs/extensions/mv3/security/ [3] "Websites Can Exploit Browser Extensions to Steal User Data", 2019 - https://www.securityweek.com/websites-can-exploit-browser-extensions-steal-user-data / https://www-sop.inria.fr/members/Doliere.Some/papers/empoweb.pdf [4] "Web Browser Extension User-Script XSS Vulnerabilities", 2020 - https://ieeexplore.ieee.org/document/9251185 [5] "Detecting DOM-Sourced Cross-Site Scripting in Browser Extensions", 2017 - https://ieeexplore.ieee.org/document/8094406 [6] "Attacking browser extensions", Nicolas Golubovic, 2016 - https://golubovic.net/thesis/master.pdf [7] "A Combined Static and Dynamic Analysis Approach to Detect Malicious Browser Extensions", 2018 - https://www.hindawi.com/journals/scn/2018/7087239/ [8] "Chrome Extensions: Threat Analysis and Countermeasures", 2012 - https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.374.8978&rep=rep1&type=pdf
[9] "Extension Breakdown: Security Analysis of Browsers Extension Resources Control Policies", Usenix Security 2017 - https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-sanchez-rola.pdf [10] "Protecting

Browsers from Extension Vulnerabilities", 2010 - https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/38394.pdf

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=PpSftQuCEDw

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20E

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Saturday - 10:00-10:45 PDT

Title: Extracting all the Azure Passwords
When: Saturday, Aug 7, 10:00 - 10:45 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Karl Fosaaen
As a Practice Director at NetSPI, Karl leads the Cloud Penetration Testing service line and oversees NetSPI's Portland, OR office. Karl holds a BS in Computer Science from the University of Minnesota and has over a decade of consulting experience in the computer security industry. Karl spends most of his research time focusing on Azure security and contributing to the NetSPI blog. As part of this research, Karl created the MicroBurst toolkit (https://github.com/Netspi/Microburst) to house many of the PowerShell tools that he uses for testing Azure. Over the last year, Karl has co-authored the book "Penetration Testing Azure for Ethical Hackers" with David Okeyode. Over the years, Karl has held the Security+, CISSP, and GXPN certifications.
Twitter: @kfosaaen

Description:
Whether it's the migration of legacy systems or creation of brand-new applications, many organizations are turning to Microsoft's Azure cloud as their platform of choice. This brings new challenges for penetration testers who are less familiar with the platform, and now have more attack surfaces to exploit. In an attempt to automate some of the common Azure escalation tasks, the MicroBurst toolkit was created to contain tools for attacking different layers of an Azure tenant. In this talk, we will be focusing on the password extraction functionality included in MicroBurst. We will review many of the places that passwords can hide in Azure, and the ways to manually extract them. For convenience, we will also show how the Get-AzPasswords function can be used to automate the extraction of credentials from an Azure tenant. Finally, we will review a case study on how this tool was recently used to find a critical issue in the Azure permissions model that resulted in a fix from Microsoft.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

CAHV - Friday - 12:00-12:59 PDT

Title: F**k You, Pay Me - Knowing your worth and getting paid
When: Friday, Aug 6, 12:00 - 12:59 PDT
Where: Career Hacking Village (Talk)
Speakers: Alyssa Miller,Liana McCrea

SpeakerBio: Alyssa Miller
No BIO available

SpeakerBio: Liana McCrea
No BIO available

Description:

In any job search, you’ll no doubt be asked some variation of the inevitable question, “What are your salary expectations?” For many this question induces anxiety. What should I get paid? What’s a fair salary? It can be a hard question of how to maximize earnings without pricing ourselves out of a potential role. Then the offer comes and it’s less than you asked for. Can you negotiate, should you negotiate, how should you negotiate for better compensation? What other things like bonuses, time off, benefits, etc. are on the table? Let’s talk about real-world strategies for knowing your worth in each job you apply for, how to position yourself for getting the pay you deserve, and considerations to account for in the negotiation process. You’ll hear about lessons learned that every job seeker should be aware of before submitting that first application or sending in a resume. The discussion will even cover how to know when what your prospective employer is saying is a legitimate constraint versus posturing for negotiating purposes. Ultimately, you’ll walk away ready to go into your next job search with the same bravado as Paulie from Goodfellas and be ready to tell them “F**k you, pay me”.

This talk will be available on YouTube: https://www.youtube.com/watch?v=F6I6O-3LCUc

Career Hacking Village content will be available on YouTube.

YouTube: https://youtube.com/careerhackingvillage

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 12:00-12:25 PDT

Title: Federal Perspective on Aerospace Cybersecurity
When: Saturday, Aug 7, 12:00 - 12:25 PDT
Where: Aerospace Village (Virtual Talk)
Speakers: Larry Grossman,Steve Luczynski

SpeakerBio: Larry Grossman
Larry Grossman is the Federal Aviation Administration's Director of the Office of Information Security and Privacy and Chief Information Security Officer. In this role, he provides strategic leadership of FAA's information security and privacy programs. He chairs FAA's Executive Cybersecurity Steering Committee which provides oversight to cybersecurity activities across the FAA enterprise. Larry leads the FAA's security operations, compliance, governance, and risk management functions. Looking externally, he oversees the FAA's Aviation Ecosystem and Stakeholder Engagement Office whose role is to promote awareness and improve cyber resiliency across the aviation ecosystem. He also leads the evolution of FAA's cybersecurity strategy, Security Operations Center modernization, new program deployments, and cyber incident response activities. Additionally, he represents FAA's cybersecurity and programs at the Department of Transportation and other agencies; he participates in government-wide and international cybersecurity initiatives and exercises; and regularly briefs Congress on FAA and aviation cybersecurity. Larry has been with the FAA for over 25 years and prior to his current role, led the deployment of Air Traffic Control and Aviation Safety systems, as well as data modernization and external data distribution efforts.

An avid aviation enthusiast, Larry holds commercial pilot and flight instructor certificates in both land and sea, and travels in his own aircraft whenever possible.

SpeakerBio: Steve Luczynski
No BIO available

Description:
As the Federal Aviation Administration's Chief Information Security Officer, Larry Grossman has a unique perspective on the challenges associated with building and sustaining adequate security for IT systems within a government agency and across the aerospace sector. Join us to learn more about his experiences and gain insight into the FAA's current efforts to sustain the public's trust in safe air travel.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=jcyL0zPNEuA

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Friday - 14:00-14:30 PDT

Title: Finding Hidden Gems via URL Shortener Services
When: Friday, Aug 6, 14:00 - 14:30 PDT
Where: Recon Village (Virtual)

SpeakerBio: Utku Sen
No BIO available
Twitter: @utkusen

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Saturday - 12:00-12:59 PDT

Title: Fireside Chat - August Cole
When: Saturday, Aug 7, 12:00 - 12:59 PDT
Where: ICS Village (Virtual)

SpeakerBio: August Cole
No BIO available

Description: No Description available

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Sunday - 11:00-11:59 PDT

Title: Fishing or Hunting
When: Sunday, Aug 8, 11:00 - 11:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Ohad Zaidenberg , Founder and Executive at CTI League
No BIO available

Description:
Create a safer cyber space for the medical sector and the life-saving organizations.

The CTI League aspires to protect the medical sector and the life-saving organizations (MS-LSO) worldwide from cyber-attacks, supplying reliable information, reducing the level of threat, supporting security departments, and neutralizing cyber threats.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 21:00-20:59 PDT

Title: Flash Loans Demystified
When: Thursday, Aug 5, 21:00 - 20:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Anto Joseph , Blockchain Security Engineer Coinbase
Anto Joseph works as a Blockchain Security Engineer @Coinbase. He enjoys researching distributed systems,DeFi protocols,Android and ML systems.He is involved in developing and advocating security in blockchains & DeFi. Previously, he has worked at Tinder, Intel, Citrix and E&Y in multiple information security roles.He has been a presenter and trainer at various security conferences including BH USA, Defcon, BruCon, HackInParis, HITB Amsterdam, HackLu, Hacktivity, PHdays, X33fCon, NullCon, c0c0n and more. He is an active contributor to many open-source projects and some of his work is available at https://github.com/antojoseph

Description:
Flash Loans are the first unsecured loan option in DeFi! They have been used for arbitrage, flash liquidation, collateral swaps and infamously Flash loan attacks. We explore the concepts behind flash loans, how they are used today and root cause of these attacks with plenty of demos throughout the talk. We also discuss strategies to protect against pump and arbitrage and oracle manipulation attacks.

This talk is now available on YouTube: https://www.youtube.com/watch?v=qSoKGINt7vw

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Friday - 13:30-13:59 PDT

Title: Forensicating Endpoint Artifacts in the World of Cloud Storage Services
When: Friday, Aug 6, 13:30 - 13:59 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Renzon Cruz
Renzon Cruz, a Filipino security professional living in Dubai who works as Digital Forensics & Incident Response in a company based in UK. He previously worked as Sr. Security Consultant as part of a National Cyber Security Agency in Qatar. He was also accepted to various international conferences as a speaker such as BSides Vancouver (2019), BSides London (2019), BSides Doha (2020), and ROOTCON Hacking Conference (2020). He is also co-founder and instructor of GuideM, a real-world cybersecurity training center based in the Philippines. He's mainly interested in defensive strategy, threat hunting, DFIR, malware analysis, & adversary simulation.
Twitter: @r3nzsec

Description:

In this presentation, I will discuss the key forensic artifacts that can be used whenever DFIR professionals encounter cloud storage services into the host such as OneDrive, GoogleDrive, Box and Dropbox. These are all essentials especially when the attacker or insider threat leverage these services to exfiltrate data. I will also show how to perform data acquisition to get these artifacts in forensically sound manner.

Today we are embracing the benefits and advantages of having cloud storage in most environments especially now when everyone is working work from home and data transmits from one place to another by the use of cloud storage services such as one drive, box, dropbox & google drive. There are a couple of artifacts on the endpoint side that gives us the ability to see the bigger picture when these cloud services are being used to perform data exfiltration and any malicious actions. In short, cloud storage data can be more accessible on the local device and can contain files and metadata distinctly different than the current cloud repository. I'm going to show how to perform data acquisition on these cloud storage applications installed in endpoint and what are those metadata and evidence that we can extract from the forensics standpoint.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Saturday - 13:30-13:59 PDT

Title: Fortifying ICS - Hardening and Testing
When: Saturday, Aug 7, 13:30 - 13:59 PDT
Where: ICS Village (Virtual)

SpeakerBio: Dieter Sarrazyn , Secudea
Dieter is a freelance SCADA/ICS/OT security consultant who’s working extensively on industrial control system security since 2008. He performs different kinds of security assessments within industrial environments including intrusion testing, physical penetration testing, technical system assessments, risk assessments and provides assistance in securing these environments. He also helps customers to manage security of solutions deployed by their industrial suppliers and integrators through doing security requirements management and security FAT and SAT tests. Next to assessing environments, he is also providing training and awareness sessions on scada/ics/ot security and coaches young graduates within this field.
Twitter: @dietersar

Description:

Every ICS environment will sooner or later have to deal with updates, upgrades or additions to the control system environment. Nowadays it is important to include cybersecurity within such projects, although that is still sometimes forgotten (sad but true). One of the ways to include security is to set security requirements but also perform hardening and cybersecurity testing within FAT and SAT cycles.

This talk will explain important elements of hardening as well as things to keep in mind when performing cybersecurity testing during FAT/SAT phases after performing said hardening.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

Title: Frack
When: Sunday, Aug 8, 10:00 - 11:50 PDT
Where: DemoLab Video Channel 2

SpeakerBio: William Vermaak
William is a Security Analyst at Orange Cyberdefense's SensePost team, specialising in penetration testing. He has been an ethical hacker since 2012 working on many different types of projects for many major banks and insurance houses in South Africa and abroad. Mobile platforms are his focus as he thoroughly enjoys breaking mobile applications and figuring out how they work. He has done several radio interviews (https://iono.fm/e/892386 and https://iono.fm/e/893010) and has also presented several training courses such as the SensePost SecDevOps training. William is currently focussing on designing a Mobile Hacking course.

Description:

Tool or Project Name: Frack

Short Abstract:
Frack is a tool created to be an end-to-end solution to store, manage and query collected breach data. The tool has a basic workflow making it easy to use. Using a very minimal cloud footprint, Frack makes it possible to store vast amounts of data in the cloud while retaining an extremely fast query speed. Query results end up in a neat Excel sheet where all of the breaches the domain was found in, including user passwords or hashes (depending on what was leaked in the breach). The Excel sheet also gives information regarding the breach it was found in and the date the breach first appeared. Having this data at your fingertips makes it easy to show a client their exposure and to use the data as a starting point when doing external or infrastructure assessments. The tool also includes the ability to use custom parse plugins which will parse raw dumps into usable data and convert it so you can use it directly in the database.

Short Developer Bio:
William is a Security Analyst at Orange Cyberdefense's SensePost team, specialising in penetration testing. He has been an ethical hacker since 2012 working on many different types of projects for many major banks and insurance houses in South Africa and abroad. Mobile platforms are his focus as he thoroughly enjoys breaking mobile applications and figuring out how they work. He has done several radio interviews (https://iono.fm/e/892386 and https://iono.fm/e/893010) and has also presented several training courses such as the SensePost SecDevOps training. William is currently focussing on designing a Mobile Hacking course.

URL to any additional information:
The tool leverages Apache ORC as a destination file format for parsed breaches. These are uploaded to Google's Big Query for processing. See: https://orc.apache.org/
https://github.com/noirello/pyorc
Detailed Explanation of Tool:
The tool was written in Python and will be distributed under the GNU General Public v3 License. The tool consists of three modulesmain features; generic parsing, plugin-based parsing and database maintenance.

The parse module is used to parse a semi clean .CSV file consisting of any of the following formats: <email>,<password>
<email>,<hash>
<email>,<hash>,<salt>
For known data breaches, a plugin system lets you consume raw data dumps without any need for modification.The parser will then convert the data to the .ORC file format (https://orc.apache.org/) resulting in small uploads to the cloud and very fast query times. These .ORC files are then ingested into a Google BigQuery table. The query module can then be used to query the data that you have uploaded into the BigQuery table.

The tool also includes a DB module where you can perform basic DB maintenance, start ingestion jobs, and see stats of the database.

Supporting Files, Code, etc:
If needed, an invitation to look at the source code beforehand can be arranged. It currently lives in a private GitHub repository.

Target Audience:
Offense, Defense, OSINT

Nothing can stop the data flow! Every day we are bombarded with news reports of another data breach that has been published on the internet. Frack provides an easy way to manage this data on Google cloud infrastructure.

This content will be presented on a Discord video channel.

#dl-video2-voice: https://discord.com/channels/708208267699945503/734027778646867988

Return to Index - Add to Google Calendar - ics Calendar file

RFV - Thursday - 12:00-11:59 PDT

Title: Frag, You’re it - Hacking Laser Tag
When: Thursday, Aug 5, 12:00 - 11:59 PDT
Where: Radio Frequency Village (Virtual)

SpeakerBio: Eric Escobar , Principal Security Consultant
Eric is a seasoned pentester and a Principal Security Consultant at Secureworks. On a daily basis he attempts to compromise large enterprise networks to test their physical, human, network and wireless security. His team consecutively won first place at DEF CON 23, 24, and 25's Wireless CTF, snagging a black badge along the way. Forcibly retired from competing in the Wireless CTF, he’s now a member of the DEF CON Wireless Village team. Before entering the cyber security arena, Eric attained both a BS and MS in Civil Engineering along with his Professional Engineering license.

Description:

What do inexpensive hardware purchased from Amazon and a little git magic have in common? They are the ingredients to become a laser tag juggernaut armed with unlimited respawns and Contraesqe widespread rapid-fire. Hacking doesn't always have to be so serious; relegated to newsworthy 0days, Nation State actors, and vulnerable supply chains. Sometimes hacks are just to wreck your friends. This talk will dive into how laser tag actually uses focused beams of infrared light (similar to your TV remote) to ""tag"" your opponent. We'll look under the hood to see what qualifies as ""lasers"", and how they are interpreted by the game server. I'll discuss how these infrared signals can be replayed stealthily. Then we'll get to the carnage of warehouse Halo godmode.

This talk has been released to YouTube.

YouTube: https://www.youtube.com/watch?v=tNLddWViPl0

Radio Frequency Village will not be streaming any talks, but they will be making talks available on their YouTube channel.

YouTube: https://youtube.com/c/RFHackersSanctuary

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Thursday - 12:00-12:59 PDT

Title: Friends of Bill W.
When: Thursday, Aug 5, 12:00 - 12:59 PDT
Where: Bally's Pool Cabana

Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun. The location is in a Bally's poolside cabana, look for the sign.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 12:00-12:59 PDT

Title: Friends of Bill W.

When: Friday, Aug 6, 12:00 - 12:59 PDT

Where: Bally's Pool Cabana

Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun. The location is in a Bally's poolside cabana, look for the sign.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 12:00-12:59 PDT

Title: Friends of Bill W.

When: Saturday, Aug 7, 12:00 - 12:59 PDT

Where: Bally's Pool Cabana

Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun. The location is in a Bally's poolside cabana, look for the sign.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Sunday - 12:00-12:59 PDT

Title: Friends of Bill W.

When: Sunday, Aug 8, 12:00 - 12:59 PDT

Where: Bally's Pool Cabana

Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun. The location is in a Bally's poolside cabana, look for the sign.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Thursday - 17:00-17:59 PDT

Title: Friends of Bill W.
When: Thursday, Aug 5, 17:00 - 17:59 PDT
Where: Bally's Pool Cabana

Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun. The location is in a Bally's poolside cabana, look for the sign.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 17:00-17:59 PDT

Title: Friends of Bill W.
When: Friday, Aug 6, 17:00 - 17:59 PDT
Where: Bally's Pool Cabana

Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun. The location is in a Bally's poolside cabana, look for the sign.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 17:00-17:59 PDT

Title: Friends of Bill W.

When: Saturday, Aug 7, 17:00 - 17:59 PDT

Where: Bally's Pool Cabana

Description:

For all those Friends of Bill W. looking for a meeting or just a quiet moment to regroup, we have you covered with meetings throughout #DEFCON - Noon & 5pm Thurs-Sat, Noon Sun. The location is in a Bally's poolside cabana, look for the sign.

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Friday - 13:00-13:59 PDT

Title: From CTF to CVE

When: Friday, Aug 6, 13:00 - 13:59 PDT

Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Bill Hatzer
No BIO available

Description:
A brief overview of my approach to hacking things and how preparing for a CTF discovered my first CVE on Hyundai Bluelink. I was practicing some burpsuite stuff and decided to tap and trap my Phone... and caught something strange.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=8LI19B5lmk8

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 13:45-14:45 PDT

Title: From On-Prem to the Cloud - Hybrid AD attack path
When: Friday, Aug 6, 13:45 - 14:45 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Sergey Chubarov
Sergey Chubarov is a Security and Cloud Expert, Instructor with 15+ years experience on Microsoft technologies. His day-to-day job is to help companies securely embrace cloud technologies. He has certifications and recognitions such as Microsoft MVP: Microsoft Azure, Offensive Security Certified Professional (OSCP), Offensive Security Experienced Penetration Tester (OSEP), Microsoft Certified Trainer, MCT Regional Lead, EC Council CEH, CPENT, CEI, CREST CPSA, CRT and more. Frequent speaker on local and international conferences. Prefers live demos and cyberattacks simulations.
https://ru.linkedin.com/in/schubarov

Description:

Most businesses today use hybrid cloud and many of us will retire before companies fully migrate to the cloud. Cloud identity service Azure AD provides protection from advanced cybersecurity attacks, but what additional challenges appear when integrating with on-prem AD? Let's check that out in advanced scenario-based session, Live demos only.

THE SESSION CONTAINS:

Getting Domain Admin through Azure AD Connect Getting Domain Admin through Azure AD Connect Cloud Sync (new offering) Bypass Azure AD authentication & MFA
Azure reconnaissance with AzureHound

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

Title: From Zero to Hero in Web Security Research
When: Saturday, Aug 7, 10:00 - 13:59 PDT
Where: Workshops - Jubilee 2 (Onsite Only)
Speakers: Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki

SpeakerBio: Dikla Barda
Dikla Barda is a Security Expert at Check Point Software Technologies. Her research has revealed significant flaws in popular services, and major vendors like: Facebook, WhatsApp, Telegram, eBay, AliExpress, LG, DJI, Microsoft, TikTok and more. She has over 15 years of experience in the field of cyber security research. She spoke at various leading conferences worldwide.

SpeakerBio: Oded Vanunu
Oded Vanunu has more than 15 years of InfoSec experience. He is a Security Leader and Offensive Security Expert who leads a security research domain from product design stages until post release. Vanunu leads security ideas into products. His expertise is in building a security research team, vulnerability research, security best practice and security design. He has been issued five patents on cybersecurity defense methods and has published dozens of research papers and product CVEs.

SpeakerBio: Roman Zaikin
Roman Zaikin is a Security Expert at Check Point Software Technologies. His research has revealed significant flaws in popular services, and major vendors (Facebook, WhatsApp, Telegram, eBay, AliExpress, LG, DJI, Microsoft and more). He has over 10 years of experience in the field of cyber security research. He spoke at various leading conferences worldwide and taught more than 1000 students, he is also responsible for the design and the material of various cyber courses worldwide. He holds more than 15 Certifications and extensive experience with system administration, network architecture, software development, penetration testing and reverse engineering. He has outstanding self-taught skills, having the ability to develop and thinking outside the box. Love technology and want to know exactly how things work behind the scenes at lowest level of the bit and the bytes. He has an innate curiosity of how software can be broken down or bypassed so you can do things with it that weren't intended to be done.

SpeakerBio: Yaara Shriki
Yaara Shriki is an experienced security researcher at Check Point. She is an IDF technological unit graduate with experience in penetration testing, vulnerability research and forensics. Outside of work, Yaara volunteers to promote women and girls in tech.

Description:
Web applications play a vital role in every modern organization. If your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions.

In this workshop we will teach you how to find vulnerabilities in web security according to the latest methods and techniques. We will demonstrate every vulnerability by giving an example from vulnerability we have found in major tech companies like: Facebook, WhatsApp, Amazon, AliExpress, Snapchat, LG and more!

Registration Link: https://www.eventbrite.com/e/from-zero-to-hero-in-web-security-research-jubilee-2-tickets-162214757707

Prerequisites

Basic Web Concepts, Basic Web Development Skills, Ability to Understand JavaScript.

Materials needed:
Personal Laptop

Return to Index - Add to Google Calendar - ics Calendar file

Title: From Zero to Hero in Web Security Research
When: Sunday, Aug 8, 10:00 - 13:59 PDT
Where: Workshops - Jubilee 2 (Onsite Only)
Speakers: Dikla Barda,Oded Vanunu,Roman Zaikin,Yaara Shriki

SpeakerBio: Dikla Barda
Dikla Barda is a Security Expert at Check Point Software Technologies. Her research has revealed significant flaws in popular services, and major vendors like: Facebook, WhatsApp, Telegram, eBay, AliExpress, LG, DJI, Microsoft, TikTok and more. She has over 15 years of experience in the field of cyber security research. She spoke at various leading conferences worldwide.

SpeakerBio: Oded Vanunu
Oded Vanunu has more than 15 years of InfoSec experience. He is a Security Leader and Offensive Security Expert who leads a security research domain from product design stages until post release. Vanunu leads security ideas into products. His expertise is in building a security research team, vulnerability research, security best practice and security design. He has been issued five patents on cybersecurity defense methods and has published dozens of research papers and product CVEs.

SpeakerBio: Roman Zaikin
Roman Zaikin is a Security Expert at Check Point Software Technologies. His research has revealed significant flaws in popular services, and major vendors (Facebook, WhatsApp, Telegram, eBay, AliExpress, LG, DJI, Microsoft and more). He has over 10 years of experience in the field of cyber security research. He spoke at various leading conferences worldwide and taught more than 1000 students, he is also responsible for the design and the material of various cyber courses worldwide. He holds more than 15 Certifications and extensive experience with system administration, network architecture, software development, penetration testing and reverse engineering. He has outstanding self-taught skills, having the ability to develop and thinking outside the box. Love technology and want to know exactly how things work behind the scenes at lowest level of the bit and the bytes. He has an innate curiosity of how software can be broken down or bypassed so you can do things with it that weren't intended to be done.

SpeakerBio: Yaara Shriki
Yaara Shriki is an experienced security researcher at Check Point. She is an IDF technological unit graduate with experience in penetration testing, vulnerability research and forensics. Outside of work, Yaara volunteers to promote women and girls in tech.

Description:

Web applications play a vital role in every modern organization. If your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions.

In this workshop we will teach you how to find vulnerabilities in web security according to the latest methods and techniques. We will demonstrate every vulnerability by giving an example from vulnerability we have found in major tech companies like: Facebook, WhatsApp, Amazon, AliExpress, Snapchat, LG and more!

Registration Link: https://www.eventbrite.com/e/from-zero-to-hero-in-web-security-research-jubilee-2-tickets-162219662377

Prerequisites

Basic Web Concepts, Basic Web Development Skills, Ability to Understand JavaScript.

Materials needed:
Personal Laptop

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Saturday - 13:00-13:59 PDT

Title: Fuzzing CAN / CAN FD ECU's and Network
When: Saturday, Aug 7, 13:00 - 13:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Samir Bhagwat
No BIO available

Description:
Get an overview of fuzzing, various techniques used in vulnerability testing, and how to automate your Fuzzing.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=L7RCalagQ&feature=youtu.be

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 11:00-11:59 PDT

Title: Fuzzing Linux with Xen
When: Sunday, Aug 8, 11:00 - 11:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Tamas K Lengyel
Tamas works as Senior Security Researcher at Intel. He received his PhD in Computer Science from the University of Connecticut where he built hypervisor-based malware-analysis and collection tools. In his free time he is maintainer of the Xen Project Hypervisor's VMI subsystem, LibVMI & the DRAKVUF binary analysis project. He currently serves as the Chief Research Officer at The Honeynet Project, a leading international non-profit organization that coordinates the development of open-source tools to fight against malware. Tamas gave prior talks at conferences such as BlackHat, CCC and Hacktivity.
Twitter: @tklengyel

Description:
Last year we've successfully upstreamed a new feature to Xen that allows high-speed fuzzing of virtual machines (VMs) using VM-forking. Recently through collaboration with the Xen community external monitoring of VMs via Intel(r) Processor Trace has also been upstreamed. Combined with the native Virtual Machine Introspection (VMI) capability Xen now provides a unique platform for fuzzing and binary analysis.

To illustrate the power of the platform we'll present the details of a real-world fuzzing operation that targeted Linux kernel-modules from an attack-vector that has previously been hard to reach: memory exposed to devices via Direct Memory Access (DMA) for fast I/O. If the input the kernel reads from DMA-exposed memory is malformed or malicious - what could happen?

So far we discovered: 9 NULL-pointer dereferences; 3 array index out-of-bound accesses; 2 infinite-loops in IRQ context and 2 instances of tricking the kernel into accessing user-memory but thinking it is kernel memory. The bugs have been in Linux for many years and were found in kernel modules used by millions of devices. All bugs are now fixed upstream.

This talk will walk you through how the bugs were found: what process we went through to identify the right code-locations; how we analyzed the kernel source and how we analyzed the runtime of the kernel with Xen to pinpoint the input points that read from DMA. The talk will explain the steps required to attach a debugger through the hypervisor to collect kernel crash logs and how to perform triaging of bugs via VM-fork execution-replay, a novel technique akin to time-travel debugging. Finally, we'll close with the release of a new open-source tool to perform full-VM taint analysis using Xen and Intel(r) Processor Trace.

REFERENCES

https://github.com/intel/kernel-fuzzer-for-xen-project https://www.youtube.com/watch?v=3MYo8ctD_aU

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=_dXC_I2ybr4

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20T

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 16:00-16:25 PDT

Title: Fuzzing NASA Core Flight System Software
When: Saturday, Aug 7, 16:00 - 16:25 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Ronald Broberg
No BIO available

Description:
NASA Core Flight System (cFS) provides an open source software framework used in multiple NASA missions including the Lunar Reconnaissance Orbiter, the Parker Solar Probe, and the protoype Mighty Eagle robotic lunar lander. The cFS suite includes Command Ingest (CI_Lab) and Telemetry Output (TO_Lab) applications which are only representative of similar applications in actual mission software. Fuzzing techniques applied to cFS reveal issues in the Command Ingest application (CI_Lab).

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=D5yiIlMy2Lg

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 18:45-19:45 PDT

Title: Game Theory: Understanding and Strategy and Deception
When: Saturday, Aug 7, 18:45 - 19:45 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Juneau Jones
Raised in the woods of Alaska, Juneau attributes her love of hacking to a childhood spentbuilding and breaking things outside. After studying computer science and economics, she moved to Dallas, Texas, where she found a home in the local hacker community. Juneau began research on applying behavioral economics to adversarial tactics. After her successful first talk at Dallas Hacker's Association on the prisoner’s dilemma, she began presenting her research at cons across the country. Currently, she works as an adversarial analyst doing consultant red teaming. She is also continuing her research and education as a cybersecurity fellow at NYU. When she is not hacking or asking strangers to act out the prisoner's dilemma, Juneau breathes fire, plays the bass, and runs DC214; Dallas's DefCon group.

Description:
Game Theory is the study of choices and strategies made by rational actors, called "players," in competitive situations, and it offers us a way to study and map human conflict. Statisticians use game theory to model war, biology, and even football. We will model the choices and behavior demonstrated by real-world adversarial conflict. Usingthese models, we will discuss how players form strategies and how other actors can influence those strategies. The talk will begin with an overview of game-theoretic modeling and its application to adversary behavior. Using the Prisoner's Dilemma as an example, we will look at how to model and analyze a single game. We can then model repeated interactions and demonstrate how "players" can influence each other's choices. These models will lay the foundations we need to look at more realistic adversary conflict. Next, we are going to look at how players can exploit information asymmetry. Emerging techniques such as dynamic honeynets and virtual attack surfaces both investigate attackers while manipulating their beliefs. We will build a Signaling Game model to show how defenders can credibly deceive adversaries. Using this model, we will look at a scenario where a defender observes multiple attacker movements within a network. While sustained engagement can help the defender learn more about the attacker and provide them false information, it comes at the risk of added exposure. In this scenario, there is a trade-off between information gained and short-term security. This talk will not look at network topology or protocols but will instead look at information exchange and strategy. We will then apply the same models to an adversarial perspective. Sustained engagement with a defender can provide an attacker with information and the opportunity to deceive defenders. However, that comes with a risk. How does an attacker's strategy change when a defender can eject them from the network at any time? By analyzing conflict where strategy and choices determine the outcome, we learn more about how to understand others' tactics and influence them with our own decisions.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Friday - 11:00-11:30 PDT

Title: Getting Started with Decentralized Object Storage
When: Friday, Aug 6, 11:00 - 11:30 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Storj Team
No BIO available

Description:
Join Storj for this brief demo. The team will be available most other times in the village to answer questions.

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Saturday - 16:00-16:30 PDT

Title: Getting started with low power & long distance communications - QRP
When: Saturday, Aug 7, 16:00 - 16:30 PDT
Where: Ham Radio Village (Virtual Talks)

SpeakerBio: Eric Escobar , Principal Security Consultant
Eric is a seasoned pentester and a Principal Security Consultant at Secureworks. On a daily basis he attempts to compromise large enterprise networks to test their physical, human, network and wireless security. His team consecutively won first place at DEF CON 23, 24, and 25's Wireless CTF, snagging a black badge along the way. Forcibly retired from competing in the Wireless CTF, he’s now a member of the DEF CON Wireless Village team. Before entering the cyber security arena, Eric attained both a BS and MS in Civil Engineering along with his Professional Engineering license.

Description:
Solar minimums have you down? Anxious to get out of the shack? This talk is for the ham who wants to take their gear on the go and still have reliable and long distance communications. Be prepared to be amazed at just how far 5 watts will truly go. I'll be covering the hardware, software, and configuration for the shack that will fit in a backpack.

All Ham Radio Village talks will be streamed to Twitch, with discussion in Discord.

For more information, see https://hamvillage.org/dc29.html

Twitch: https://www.twitch.tv/hamradiovillage

#hrv-presentation-text: https://discord.com/channels/708208267699945503/736674835413073991

Return to Index - Add to Google Calendar - ics Calendar file

Title: Git Wild Hunt
When: Saturday, Aug 7, 12:00 - 13:50 PDT
Where: Palace 3+4+5
Speakers: Rod Soto,José Hernandez

SpeakerBio: Rod Soto
Over 15 years of experience in information technology and security. He has spoken at ISSA, ISC2, OWASP, DEFCON, RSA Conference,Hackmiami, DerbyCon, Splunk .CONF, Black Hat,BSides, Underground Economy and also been featured in Rolling Stone Magazine, Pentest Magazine, Univision, BBC, Forbes, VICE, Fox News and CNN. Co-founder of Hackmiami, Pacific Hackers Meetups and Conferences. Co-founder of Pacific Hackers Association.

SpeakerBio: José Hernandez
Principal Security Researcher at Splunk. He started his professional career at Prolexic Technologies (now Akamai), fighting DDOS attacks against Fortune 100 companies perpetrated by "anonymous" and "lulzsec." As an engineering co-founder of Zenedge Inc. (acquired by Oracle Inc.), José helped build technologies to fight bots and web-application attacks. He has also built security operation centers and run a public threat-intelligence service.
Twitter: @d1vious

Description:
Tool or Project Name: Git Wild Hunt A tool for hunting leaked credentials

Short Abstract:
Git Wild Hunt is a tool designed to search and identify leaked credentials at public repositories such as Github. Git Wild Hunt searches for footprints and patterns of over 30 of the most used secrets/credentials on the internet, especially those used in Devops and IT Operations. This tool helps developers and security operation departments discover leaked credentials in public repositories. This tool is also a recon tool for red teamers and pentesters, as it also provides metadata from leaks such as usernames, company names, secret types and dates.

License: Apache-2.0 License

Short Developer Bio:
José Hernandez @d1vious
Principal Security Researcher at Splunk. He started his professional career at Prolexic Technologies (now Akamai), fighting DDOS attacks against Fortune 100 companies perpetrated by "anonymous" and "lulzsec." As an engineering co-founder of Zenedge Inc. (acquired by Oracle Inc.), José helped build technologies to fight bots and web-application attacks. He has also built security operation centers and run a public threat-intelligence service.

Rod Soto @rodsoto
Principal Security Research Engineer at Splunk. Worked at Prolexic Technologies (now Akamai), and Caspida. Cofounder of Hackmiami and Pacific Hackers meetups and conferences. Creator of Kommand && KonTroll / NoQrtr-CTF.

URL to any additional information: https://github.com/d1vious/git-wild-hunt

Detailed Explanation of Tool:
This tool is very effective in finding leaked credentials here is a list of the credentials that are detected: AWS API Key
Amazon AWS Access Key ID
Amazon MWS Auth Token
Facebook Access Token
Facebook OAuth
Generic API Key
Generic Secret

GitHub
Google (GCP) Service-account
Google API Key
Google Cloud Platform API Key
Google Cloud Platform OAuth
Google Drive API Key
Google Drive OAuth
Google Gmail API Key
Google Gmail OAuth
Google OAuth Access Token
Google YouTube API Key
Google YouTube OAuth
Heroku API Key
MailChimp API Key
Mailgun API Key
PGP private key block
Password in URL
PayPal Braintree Access Token
Picatic API Key
RSA private key
SSH (DSA) private key
SSH (EC) private key
Slack Token
Slack Webhook
Square Access Token
Square OAuth Secret
Stripe API Key
Stripe Restricted API Key
Twilio API Key
Twitter Access Token
Twitter OAuth
Target Audience:
Offense, Vulnerability Assessment

This tool is very effective in bringing awareness of the danger of leaked credentials in public repositories.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 11:00-11:45 PDT

Title: Glitching RISC-V chips: MTVEC corruption for hardening ISA
When: Sunday, Aug 8, 11:00 - 11:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded
Speakers: Adam 'pi3' Zabrocki,Alex Matrosov

SpeakerBio: Adam 'pi3' Zabrocki
Adam 'pi3' Zabrocki is a computer security researcher, pentester and bughunter, currently working as a Principal Offensive Security Researcher at NVIDIA. He is a creator and a developer of Linux Kernel Runtime Guard (LKRG) - his moonlight project defended by Openwall. Among others, he used to work in Microsoft, European Organization for Nuclear Research (CERN), HISPASEC Sistemas (known from the virustotal.com project), Wroclaw Center for Networking and Supercomputing, Cigital. The main area of his research interest is a low-level security (CPU architecture, uCode, FW, hypervisor, kernel, OS).

As a hobby, he was a developer in The ERESI Reverse Engineering Software Interface project, a bughunter (discovered vulnerabilities in Hyper-V hypervisor, Intel/NVIDIA vGPU, Linux kernel, OpenSSH, gcc SSP/ProPolice, Apache, Adobe Acrobat Reader, Xpdf, Torque GRID server, FreeBSD, and more) and studied exploitation and mitigation techniques, publishing results of his research in Phrack Magazine.

Twitter: @Adam_pi3
http://pi3.com.pl

SpeakerBio: Alex Matrosov
Alex Matrosov is a well-recognized offensive security researcher. He has more than two decades of experience with reverse engineering, advanced malware analysis, firmware security, and exploitation techniques. Alex served as Chief Offensive Security Researcher at Nvidia, Intel Security Center of Excellence (SeCoE), spent more than six years in the Intel Advanced Threat Research team, and was Senior Security Researcher at ESET. Alex has authored and co-authored numerous research papers, and is a frequent speaker at security conferences, including REcon, Zeronigths, Black Hat, DEF CON, and others. Additionally, he is awarded by Hex-Rays for open-source plugin efiXplorer and HexRaysCodeXplorer which has been developed and supported since 2013 by REhint's team.
Twitter: @matrosov
https://medium.com/firmware-threat-hunting

Description:
RISC-V is an open standard instruction set architecture (ISA) provided under open-source licenses that do not require fees to use. ISA is based on established reduced instruction set computer (RISC) principles. RISC-V has features to increase computer speed, while reducing cost and power use.

Many industry players like Google, IBM, NVIDIA, Qualcomm, and Samsung are members of the RISC-V Foundation and have long supported RISC-V development. In 2016, NVIDIA unveiled plans to replace the internal microcontrollers of their graphic cards with next-gen RISC-V-based controllers built for upcoming NVIDIA GPUs.

NVIDIA's Product Security undertook a detailed architectural analysis and research of the RISC-V IP, discovering a potential risk with the ambiguous specification of the Machine Trap Base Address (MTVEC) register. This ambiguity leads to potential fault injection vulnerabilities under physical attack models.

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=iz_Y1lOtX08

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20A

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Saturday - 15:30-16:30 PDT

Title: Gold Bug Q&A
When: Saturday, Aug 7, 15:30 - 16:30 PDT
Where: Crypto & Privacy Village (Virtual)

Description:

Join puzzlemasters Kevin & Maya to discuss this year's puzzle!

goldbug.cryptovillage.org

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 10:00-10:45 PDT

Title: Gone Apple Pickin': Red Teaming macOS Environments in 2021
When: Friday, Aug 6, 10:00 - 10:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Cedric Owens
Cedric is currently an offensive security engineer who came from a blue team background. His passion revolves around red teams and blue teams working closely together to improve each other's tradecraft. Cedric enjoys researching techniques and writing tools related to macOS post exploitation and infrastructure automation.

His blogs can be found here: https://medium.com/@cedowens His tools can be found here: https://github.com/cedowens

Twitter: @cedowens

Description:

Though the vast majority of US companies are enterprise Windows shops, there is a growing percentage of companies that are shifting away from this model. Most of these types of companies tend to be based in the SF Bay Area and are often tech companies. This talk will provide a glimpse into what common attack paths in these environments look like in the absence of typical enterprise Active Directory implementations. Examples include techniques for targeting macOS endpoints, cloud and IdaaS, CI/CD pipeline, and other fun approaches. I will begin by discussing common tech stacks and macOS deployments and then move into macOS initial access (including the Gatekeeper bypass I found) and post exploitation options in these modern tech environments as well as detection opportunities.

--

This talk has been released to the DEF CON Media server.

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20C

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 21:00-01:59 PDT

Title: Gothcon 2021 (Virtual)
When: Friday, Aug 6, 21:00 - 01:59 PDT
Where: See Description

Description:

Join us, hybrid style, as we continue yet another year of #DCGOTHCON. Digital hangs will be found at https://www.twitch.tv/dcgothcon. Watch our twitter @dcgothcon for updates about some renegade IRL meet-ups. We will be streaming our fav goth DJ's Friday evening, 10p-2a Pacific. DM on twitter to join our discord.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 20:00-01:59 PDT

Title: Gothcon 2021

When: Saturday, Aug 7, 20:00 - 01:59 PDT

Where: Bally's Skyview 4

Description:

Join us, hybrid style, as we continue yet another year of #DCGOTHCON. Digital hangs will be found at https://www.twitch.tv/dcgothcon. Watch our twitter @dcgothcon for updates about some renegade IRL meet-ups. We will be streaming our fav goth DJ's Friday evening, 10p-2a Pacific. DM on twitter to join our discord.

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Friday - 13:00-13:30 PDT

Title: Hack the Conspiracies
When: Friday, Aug 6, 13:00 - 13:30 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Barb Byrum

Barb Byrum is currently in her third term as Ingham County Clerk, serving as the county's chief elections official. As Clerk of one of the most populous counties in the State of Michigan, Byrum has successfully conducted 27 elections, 4 union elections, and the 2016 Presidential Recount. Since 2016, Byrum has been credentialed as a Certified Elections/Registration Administrator by Election Center, the only national program of continuing professional education that specializes in elections administration and voter registration. In 2017, she served on Election Center's Security Task Force.

Byrum has previously served on Michigan's Election Security Commission, the Secretary of State's team of advisors tasked with strengthening and better securing elections in the state. Byrum has been a consistent advocate for the voting rights of qualified registered voters, with a focus on voting rights of military and overseas voters. Byrum serves on the Overseas Voting Initiative, which is a joint effort by the Federal Voting Assistance Program and Council of State Governments. As a member of the Initiative, Byrum met with military service members in San Diego, California in March 2019, Puerto Rico in December of 2019 and continues to have military and overseas voters' interests in mind, when advocating for increased access to the ballot.

Byrum graduated from Michigan State University with a Bachelor of Science degree in agribusiness management. She also holds a law degree from the MSU College of Law.

Byrum previously served three terms as a Michigan State Representative. During her time in the Legislature, Byrum served as the ranking Democrat on the House Committee on Redistricting and Elections.

Description:

The conspiracy theories surrounding the November 2020 General Election have had a profound and significant impact on the American people but the devastating damage done to the integrity of our elections will take years to repair. This has resulted in death threats, attacks, and shows of force against our election workers, armed protests that turned violent and legislation that would take states backward to a time when America more blatantly disenfranchised certain groups and demographics of voters. The result is that many qualified election administrators are leaving the profession for positions where their lives are not in danger.

We must fight back against disinformation and the misinformation relating to our elections and those that would seek to speak fear and lies. We must pledge to push back on those lies and that disinformation in the media and online at every opportunity. We must work together on our elections to make sure that they are safe and secure as they can possibly be. Together, we can hack the conspiracies and take back our democracy.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

---

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 12:30-12:50 PDT

Title: Hack the hackers: Leaking data over SSL/TLS
When: Saturday, Aug 7, 12:30 - 12:50 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Ionut Cernica
Ionut Cernica started his security career with the bug bounty program from Facebook. His passion for security led him to get involved in dozens of such programs and he found problems in very large companies such as Google, Microsoft, Yahoo, AT&T, eBay, VMware. He has also been testing web application security for 9 years and has had a large number of projects on the penetration testing side.

Another stage of his career was to get involved in security contests and participated in more than 100 such contests. He also reached important finals such as Codegate, Trend Micro and Defcon with the PwnThyBytes team. He also won several individual competitions, including the mini CTF from the first edition of Appsec village - Defcon village.

Now he is doing research in the field of web application security, being also a PhD student at University Polytechnic of Bucharest. Through his research he wants to innovate in the field and to bring a new layer of security to web applications. He has also been working as a Security Researcher @Future Networks 5G Lab for a few months now and hopes to make an important contribution to the 5G security area through research.

Twitter: @CernicaIonut

Description:

Have you considered that in certain situations the way hackers exploit vulnerabilities over the network can be predictable? Anyone with access to encrypted traffic can reverse the logic behind the exploit and thus obtain the same data as the exploit.

Various automated tools have been analyzed and it has been found that these tools operate in an unsafe way. Various exploit databases were analyzed and we learned that some of these are written in an insecure (predictable) way.

This presentation will showcase the results of the research, including examples of exploits that once executed can be harmful. The data we obtain after exploitation can be accessible to other entities without the need of decrypting the traffic. The SSL/TLS specs will not change. There is a clear reason for that and in this presentation I will argue this, but what will change for sure is the way hackers will write some of the exploits.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=WNXEuFaRUkU

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20I

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

HTSV - Saturday - 12:00-14:59 PDT

Title: Hack the Sea Cabana Party

When: Saturday, Aug 7, 12:00 - 14:59 PDT

Where: Hack the Sea (Virtual)

Description:

For more information see https://hackthesea.org/cabana-party/

Come visit our Cabana Saturday from 12:00-3:00pm PST pool-side at Bally’s!

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Sunday - 11:00-11:55 PDT

Title: Hack the Wind
When: Sunday, Aug 8, 11:00 - 11:55 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: Mary Ann Hoppa
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:30-11:20 PDT

Title: Hack-A-Sat 2: The Good, The Bad and the Cyber-Secure
When: Friday, Aug 6, 10:30 - 11:20 PDT
Where: Aerospace Village (Virtual Talk)
Speakers: Bryce Kerley,Capt Aaron Bolen,Frank Pound,Steve Wood

SpeakerBio: Bryce Kerley
No BIO available

SpeakerBio: Capt Aaron Bolen
No BIO available

SpeakerBio: Frank Pound
No BIO available

SpeakerBio: Steve Wood
No BIO available

Description:

Take a deep dive into the last frontier of cybersecurity: Space. We take an inside look at the Hack-A-Sat prize competition, a joint effort of the Air Force and Space Force, in collaboration with the Aerospace Village, aimed at educating and inspiring a new generation of hackers to tackle this ever-important domain. In this talk, we will discuss: Satellite hacking 101, recap HAS1 insights, provide HAS2 Quals challenge explainers, and preview the HAS2 Finals…and beyond

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=G3YA5Sa5Wbs

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:00-15:59 PDT

Title: Hack-A-Sat2 Satellite Platform
When: Friday, Aug 6, 10:00 - 15:59 PDT
Where: Aerospace Village (Workshop - Virtual + Paris Rivoli B)

Description:

Come and gets hands on with Hack-a-Sat 2 hardware and learn about the unique problems presented by cybersecurity in the space realm. The Air Force and Space Force will be presenting the HAS2 flatsat – the primary platform hosting the hacking challenges for HAS2, comprised of a variety of software and processor architectures commonly used in space vehicles. Visitors can command various settings changes in the flatsat and see the resulting changes in the telemetry from the device as well as visual attitude changes in the NASA 42 simulation. Visitors will also be introduced to the HAS2 Digital Twin, an emulated version of all the flight software running on the flatsat, and will have a chance to capture and analyze an exploit being thrown against the flight software. Lastly, the Aerospace Corporation will demonstrate cyber defense onboard a satellite by using machine learning and signatures to detect anomalous command sequences and onboard cyber events.

For virtual attendees, the Digital twin demonstration will also be accessible via VNC to an instance running inside Docker containers in Amazon AWS (remote viewers will need to have a VNC client on their own computer).

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 10:00-15:59 PDT

Title: Hack-A-Sat2 Satellite Platform
When: Saturday, Aug 7, 10:00 - 15:59 PDT
Where: Aerospace Village (Workshop - Virtual + Paris Rivoli B)

Description:

Come and gets hands on with Hack-a-Sat 2 hardware and learn about the unique problems presented by cybersecurity in the space realm. The Air Force and Space Force will be presenting the HAS2 flatsat – the primary platform hosting the hacking challenges for HAS2, comprised of a variety of software and processor architectures commonly used in space vehicles. Visitors can command various settings changes in the flatsat and see the resulting changes in the telemetry from the device as well as visual attitude changes in the NASA 42 simulation. Visitors will also be introduced to the HAS2 Digital Twin, an emulated version of all the flight software running on the flatsat, and will have a chance to capture and analyze an exploit being thrown against the flight software. Lastly, the Aerospace Corporation will demonstrate cyber defense onboard a satellite by using machine learning and signatures to detect anomalous command sequences and onboard cyber events.

For virtual attendees, the Digital twin demonstration will also be accessible via VNC to an instance running inside Docker containers in Amazon AWS (remote viewers will need to have a VNC client on their own computer).

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-15:59 PDT

Title: Hack3r Runw@y
When: Friday, Aug 6, 10:00 - 15:59 PDT
Where: See Description

Description:

More info: https://forum.defcon.org/node/236429

More info: https://hack3rrunway.github.io/

https://twitter.com/hack3rrunway

Also see #ce-hack3r-runway.

Register here:
https://docs.google.com/forms/d/e/1FAIpQLSdua561gCbWEbGk7_ZuS7cg3w7_IFbtrahibeKsU0iR%20ENiIiw/viewform?usp=sf_

#ce-hack3r-runway: https://discord.com/channels/708208267699945503/711644666239647824

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 10:00-15:59 PDT

Title: Hack3r Runw@y
When: Saturday, Aug 7, 10:00 - 15:59 PDT
Where: See Description

Description:

More info: https://forum.defcon.org/node/236429

More info: https://hack3rrunway.github.io/

https://twitter.com/hack3rrunway

Also see #ce-hack3r-runway.

Register here:
https://docs.google.com/forms/d/e/1FAIpQLSdua561gCbWEbGk7_ZuS7cg3w7_IFbtrahibeKsU0iR%20ENiIiw/viewform?usp=sf_

#ce-hack3r-runway: https://discord.com/channels/708208267699945503/711644666239647824

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 20:00-22:59 PDT

Title: Hacker Flairgrounds
When: Saturday, Aug 7, 20:00 - 22:59 PDT
Where: Paris Chillout 2

Description:

The destination for badge collectors, designers, and hardware hacks to celebrate the flashier side of DEF CON. It is a melding of the 1337 and the un1eet interested in hardware and IoT. We see #badgelife, #badgelove, SAOs and badge hacking as a great potential for securing IoT and keeping the power in the hands of the consumer by spreading knowledge about the craft/trade. Those involved should be celebrated for sharing their knowledge. Many of them do not like the limelight, so this gives us a chance to personally say thank you.

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 20:00-21:59 PDT

Title: Hacker Jeopardy
When: Saturday, Aug 7, 20:00 - 21:59 PDT
Where: Bally's Gold Ballroom (and Virtual)

Description:

Hacker Jeopardy is being held in Bally's Gold Ballroom at 20:00 Saturday.

For more information, see https://forum.defcon.org/node/236486

Twitch: https://www.twitch.tv/DFIUtv

Twitter: https://twitter.com/HackerJeopardy

#ce-hacker-jeopardy-text: https://discord.com/channels/708208267699945503/732439600391389184/

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 20:00-21:59 PDT

Title: Hacker Jeopardy
When: Friday, Aug 6, 20:00 - 21:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236486

This event will be held VIRTUALLY ONLY, on Twitch. Discussion will be held in #ce-hacker-jeopardy-text.

Twitch: https://www.twitch.tv/DFIUtv

Twitter: https://twitter.com/HackerJeopardy

#ce-hacker-jeopardy-text: https://discord.com/channels/708208267699945503/732439600391389184/

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 18:00-23:59 PDT

Title: Hacker Karaoke (Virtual)
When: Friday, Aug 6, 18:00 - 23:59 PDT
Where: See Description

Description:

Even though we cannot be there in person to run the event, we will be event on the Discord Defcon Channel in the Hacker Karaoke room. We will be running from 6PM pacific to Midnight Pacific on Friday and Saturday night. Additional information on joining the event will be available online. Follow us at @hackerkaraoke for more information.

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 18:00-23:59 PDT

Title: Hacker Karaoke (Virtual)
When: Saturday, Aug 7, 18:00 - 23:59 PDT
Where: See Description

Description:

Even though we cannot be there in person to run the event, we will be event on the Discord Defcon Channel in the Hacker Karaoke room. We will be running from 6PM pacific to Midnight Pacific on Friday and Saturday night. Additional information on joining the event will be available online. Follow us at @hackerkaraoke for more information.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 18:00-18:59 PDT

Title: HACKERS INTO THE UN? Engaging in the cyber discussions on war & peace
When: Saturday, Aug 7, 18:00 - 18:59 PDT
Where: Track 1 Live; DCTV/Twitch #1 Live

SpeakerBio:DEF CON Policy Panel
No BIO available

Description: No Description available

This talk will be given live in Track 1, and will be streamed to DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 15:00-15:45 PDT

Title: Hacking G Suite: The Power of Dark Apps Script Magic
When: Saturday, Aug 7, 15:00 - 15:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Matthew Bryant
mandatory (Mathew Bryant) is a passionate hacker currently leading the red team effort at Snapchat. In his personal time he's published a variety of tools such as XSS Hunter, CursedChrome, and tarnish. His security research has been recognized in publications such as Forbes, The Washington Post, CBS News, Techcrunch, and The Huffington Post. He has previously presented at Blackhat, RSA, Kiwicon, Derbycon, and Grrcon. Previous gigs include Google, Uber, and Bishop Fox.
Twitter: @IAmMandatory
https://thehackerblog.com

Description:

You've seen plenty of talks on exploiting, escalating, and exfiltrating the magical world of Google Cloud (GCP), but what about its buttoned-down sibling? This talk delves into the dark art of utilizing Apps Script to exploit G Suite (AKA Google Workspace).

As a studious sorcerer, you'll discover how to pierce even the most fortified G Suite enterprises. You'll learn to conjure Apps Script payloads to bypass powerful protective enchantments such as U2F, OAuth app allowlisting, and locked-down enterprise Chromebooks.

Our incantations don't stop at the perimeter, we will also discover novel spells to escalate our internal privileges and bring more G Suite accounts under our control. Once we've obtained the access we seek, we'll learn various curses to persist ourselves whilst keeping a low profile so as to not risk an unwelcome exorcism.

You don't need divination to see that this knowledge just might rival alchemy in value.

REFERENCES

No real academic references, this is all original research gleaned from real-world testing and reading documentation.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=6AsVUS79gLw

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20M

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

Title: Hacking Humans with AI as a Service

When: Friday, Aug 6, 14:00 - 14:45 PDT

Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

Speakers: Eugene Lim,Glenice Tan,Tan Kee Hock

SpeakerBio: Eugene Lim

Eugene Lim, also known as spaceraccoon, is a security researcher and white hat hacker. He regularly participates in live-hacking events and was awarded the Most Valuable Hacker title in the h1-213 Live-Hacking Event by Hackerone. Besides white hat hacking, he enjoys building security tools, including a malicious npm package scanner and an open-source intelligence social engineering honeypot that were presented at Black Hat Asia Arsenal 2019 and Black Hat USA Arsenal 2020. His writeups on https://spaceraccoon.dev are regularly cited by other white hat hackers.
Twitter: @spaceraccoonsec
https://www.linkedin.com/in/limzhiweieugene/

SpeakerBio: Glenice Tan

Glenice is a security researcher that enjoys exploring the quirks of different systems, applications, and processes. In the past year, she had the opportunity to conduct social engineering exercises, which includes phishing and vishing. Apart from applications and human hacking, she also experiments on ways to automate or improve red team operations.
https://www.linkedin.com/in/glenicetan/

SpeakerBio: Tan Kee Hock

Tan Kee Hock is a Cybersecurity Specialist who simply likes to 'hack' things. He loves to play CTFs and is always keen to explore more!
https://www.linkedin.com/in/tankeehock/

Description:

As the proliferation of Artificial Intelligence as a Service (AIaaS) products such as OpenAI's GPT-3 API places advanced synthetic media generation capabilities in the hands of a global audience at a fraction of the cost, what does the future hold for AI-assisted social engineering attacks? In our talk, we will present the nuts and bolts of an AIaaS phishing pipeline that was successfully deployed in multiple authorized phishing campaigns. Using both paid and free services, we emulated the techniques that even low-skilled, limited resource actors could adopt to execute effective AI-assisted phishing campaigns at scale. By repurposing easily-accessible personality analysis AIaaS products, we generated persuasive phishing emails that were automatically personalized based on a target's public social media information and created by state-of-the-art natural language generators. We will also discuss how an AI-assisted phishing workflow would impact traditional social engineering teams and operations. Finally, we look at how AIaaS suppliers can mitigate the misuse of their products.

REFERENCES

1. T. Karras, S. Laine, and T. Aila, “A Style-Based Generator Architecture for Generative Adversarial Networks,” arXiv:1812.04948 [cs.NE], 2019.
2. S. Gehrmann, H. Strobelt, and A. M. Rush, “GLTR: Statistical Detection and Visualization of Generated Text,” arXiv:1906.04043 [cs.CL], 2019.
3. G. Jawahar, M. Abdul-Mageed, and L. V. S. Lakshmanan, “Automatic Detection of Machine Generated Text: A Critical Survey,” arXiv:2011.01314 [cs.CL], 2020.
4. J. Seymour and P. Tully, “Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter,” 2016.
5. P. Tully and F. Lee, “Repurposing Neural Networks to Generate Synthetic Media for Information Operations,” 2020.
6. OpenAI, “OpenAI Charter,” OpenAI, 09-Apr-2018. [Online]. Available: https://openai.com/charter/.
7. G. Brockman, M. Murati, and P. Welinder, “OpenAI API,” OpenAI, 11-Jun-2020. [Online]. Available: https://openai.com/blog/openai-api/.

8. A. Pilipiszyn, “GPT-3 Powers the Next Generation of Apps,” OpenAI, 25-Mar-2021. [Online]. Available: https://openai.com/blog/gpt-3-apps/.

Would like to thank contributing author Timothy Lee Timothy is a security researcher who likes to break things and tries to understand how the system works during the process. In the past year, he is researching with iOS security and is starting his journey on iOS vulnerability research. Additionally, he has contributed to red team social engineering operations and security tooling, with practical experience in vishing and in-person social engineering. https://www.linkedin.com/in/timothylee0/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=tWWhRbzhkrg

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20E

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

Title: Hacking the Apple AirTags
When: Saturday, Aug 7, 17:00 - 17:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Thomas Roth
Thomas Roth, also known as stacksmashing, is a security researcher from Germany with a focus on embedded devices: From hacking payment terminals, crypto wallets, secure processor, the Nintendo Game & Watch, up to Apple's AirTag he loves to explore embedded & IoT security. On how YouTube channel "stacksmashing" he attempts to make reverse-engineering & hardware hacking more accessible.
Twitter: @ghidraninja
https://youtube.com/stacksmashing

Description:

Apple's AirTags enable tracking of personal belongings. They are the most recent and cheapest device interacting with the Apple ecosystem. In contrast to other tracking devices, they feature Ultrawide-band precise positioning and leverage almost every other Apple device within the Find My localization network.

Less than 10 days after the AirTag release, we bypassed firmware protections by glitching the nRF52 microcontroller. This opens the AirTags for firmware analysis and modification. In this talk, we will explain the initial nRF52 bypass as well as various hacks built on top of this. In particular, AirTags can now act as phishing device by providing malicious links via the NFC interface, be cloned and appear at a completely different location, used without privacy protections that should alert users as tracking protection, act as low-quality microphone by reutilizing the accelerometer, and send arbitrary data via the Find My network. Besides these malicious use cases, AirTags are now a research platform that even allows access to the new Ultrawide-band chip U1.

REFERENCES

> LimitedResults nRF52 APPROTECT Bypass:
> https://limitedresults.com/2020/06/nrf52-debug-resurrection-approtect-bypass/

Positive Security's Send My Research for sending arbitrary data via the find my network:
https://positive.security/blog/send-my

Colin O'Flynn's notes on the AirTag Hardware: https://github.com/colinoflynn/airtag-re

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=paxErRRsrTU

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20T

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

WS - Saturday - 10:00-13:59 PDT

Title: Hacking the Metal: An Introduction to Assembly Language Programming
When: Saturday, Aug 7, 10:00 - 13:59 PDT
Where: Workshops - Las Vegas 3+4 (Onsite Only)

SpeakerBio:eigentourist , Programmer
Eigentourist is a programmer who learned the craft in the early 1980s. He began formal education in computer science when the height of software engineering discipline meant avoiding the use of GOTO statements. Over the course of his career, he has created code of beautiful simplicity and elegance, and of horrific complexity and unpredictability. Sometimes it's hard to tell which was which. Today, he works on systems integration and engineering in the healthcare industry.

Description:

Deep below the surface of the web, the visible desktop, and your favorite mobile apps, lies a labyrinth where the rules of most programming languages cease to exist. This is the world of the reverse engineer, the malware analyst, and the veteran systems programmer. Here, we write code in assembly language, the lowest level at which a computing machine can be programmed. This workshop will introduce you to the world of assembly language programming, give you the opportunity to write some real-world code, and finally, to play the role of reverse engineer and try your hand at some guided malware analysis.

Registration Link:
https://www.eventbrite.com/e/hacking-the-metal-an-introduction-to-assembly-language-programming-lv-34-tickets-162218563089

Prerequisites
Some previous programming experience is helpful but not vital.

Materials needed:
Laptop

Return to Index - Add to Google Calendar - ics Calendar file

WS - Sunday - 10:00-13:59 PDT

Title: Hacking the Metal: An Introduction to Assembly Language Programming
When: Sunday, Aug 8, 10:00 - 13:59 PDT
Where: Workshops - Las Vegas 3+4 (Onsite Only)

SpeakerBio:eigentourist , Programmer
Eigentourist is a programmer who learned the craft in the early 1980s. He began formal education in computer science when the height of software engineering discipline meant avoiding the use of GOTO statements. Over the course of his career, he has created code of beautiful simplicity and elegance, and of horrific complexity and unpredictability. Sometimes it's hard to tell which was which. Today, he works on systems integration and engineering in the healthcare industry.

Description:

Deep below the surface of the web, the visible desktop, and your favorite mobile apps, lies a labyrinth where the rules of most programming languages cease to exist. This is the world of the reverse engineer, the malware analyst, and the veteran systems programmer. Here, we write code in assembly language, the lowest level at which a computing machine can be programmed. This workshop will introduce you to the world of assembly language programming, give you the opportunity to write some real-world code, and finally, to play the role of reverse engineer and try your hand at some guided malware analysis.

Registration Link:
https://www.eventbrite.com/e/hacking-the-metal-an-introduction-to-assembly-language-programming-lv-34-tickets-162218597191

Prerequisites

Some previous programming experience is helpful but not vital.

Materials needed:
Laptop

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Friday - 10:30-10:59 PDT

Title: Hacking to Save Democracy: What Technologists Need to Know About Election Administration
When: Friday, Aug 6, 10:30 - 10:59 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Eddie Perez
Eddie Perez is the Global Director of Technology Development & Open Standards for the Open Source Election Technology Institute. He is a principal liaison to the TrustTheVote Project's election officials' stakeholder community.

Eddie has a wealth of expertise in election systems design, implementation, security, usability, and standards. A veteran of the commercial election technology industry, he formerly served as director of product management for one of the three major voting systems vendors in the U.S. Now, Eddie utilizes his skills to drive open source voting technology design, as well as federal and state certification for open source technologies, and voter education initiatives.

Eddie is a regular contributor to media outlets from MSNBC news to Fox News, including The Washington Post, Associated Press, and POLITICO, to name a few. He is also an NBC News contributing elections analyst on topics of technology, practices, security, and public policy.

Eddie speaks to policy leaders on election technology and administration, and has given testimony to several agencies and government bodies including the U.S. Election Assistance Commission and The National Conference of State Legislatures.

Eddie is co-inventor of two U.S. patents in voting technology.

Edward is on Twitter at @eddieperezTX with contributions via @OSET and @TrustTheVote

Twitter: @eddieperezTX

Description:
No technology is more consequential to democracy than election technology. When it's done well, election technology undergirds democracy and ensures that even the losers of elections respect the result. When it's done poorly, trust in democracy erodes and even the most powerful countries are shaken to their cores.

Time to panic? No, it’s time to roll up our sleeves!

Where others might despair, we see a golden opportunity! At no other time in our history have so many Americans of all political stripes been so focused on election integrity. We want security-minded, tech-savvy people of all genders, races, creeds, and political stripes to step up. And if we’re going to lower the temperature and bolster public confidence in election integrity, it’s critical to understand how elections are actually run, and how election technology is used. Election administration is a complex profession limited by law, policy, and specific practices.

Whether you’re new to election security, or an experienced practitioner, this presentation is a snapshot of the operating environment for election technology. Our goal is to help you learn what to anticipate, and how best to apply your technology skills in defense of democracy. Together, we can enhance election integrity and help to ensure that accurate information gets widely shared, and misinformation does not.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

---

CAHV - Friday - 13:00-13:59 PDT

Title: Hacking Your Career: The Options
When: Friday, Aug 6, 13:00 - 13:59 PDT
Where: Career Hacking Village (Talk)
Speakers: Chris Sperry,Deb Herrity,Jennifer Haverman

SpeakerBio: Chris Sperry
No BIO available

SpeakerBio: Deb Herrity
No BIO available

SpeakerBio: Jennifer Haverman
No BIO available

Description:

One common theme in the community: a lack of understanding over what jobs exist in the career field that encompasses Infosec, Information Assurance, Cyber Security, and related fields; and what it’s like to work and live in them. What’s right for you; what career path you create: there is no “right” answer or limits: knowing the options and leveraging your “why” will help guide your way. This presentation abstract proposes a small panel of sages, diverse on purpose, with those that have a combination of career experience in government, military, industry sharing their career path experiences; their “whys” of where they worked and why they are where they are now; but with the focus on giving attendees ideas and options they might not have considered before.

This talk will be available on YouTube: https://www.youtube.com/watch?v=T4r2ZpEUjJs

Career Hacking Village content will be available on YouTube.

YouTube: https://youtube.com/careerhackingvillage

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:00-15:59 PDT

Title: HACMS Live Demo

When: Friday, Aug 6, 10:00 - 15:59 PDT

Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:

As part of DARPA-s High-Assurance Cyber Military Systems program, Collins Aerospace led a team of researchers using formal methods tools to construct aircraft software that was provably secure against many classes of cyber attack. We will have an operational (but non-flying) version of our secure quadcopter present whose mission and telemetry software runs on the formally verified seL4 kernel. We will provide wifi access to an isolated virtual machine running on its mission computer. DEF CON participants will be challenged to break out of the VM environment to read or write the encryption keys used for vehicle telemetry.

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 10:00-15:59 PDT

Title: HACMS Live Demo
When: Saturday, Aug 7, 10:00 - 15:59 PDT
Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:
As part of DARPA-s High-Assurance Cyber Military Systems program, Collins Aerospace led a team of researchers using formal methods tools to construct aircraft software that was provably secure against many classes of cyber attack. We will have an operational (but non-flying) version of our secure quadcopter present whose mission and telemetry software runs on the formally verified seL4 kernel. We will provide wifi access to an isolated virtual machine running on its mission computer. DEF CON participants will be challenged to break out of the VM environment to read or write the encryption keys used for vehicle telemetry.

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Sunday - 11:00-13:59 PDT

Title: Ham Radio Exams
When: Sunday, Aug 8, 11:00 - 13:59 PDT
Where: Ham Radio Village (Onsite - Bally's Bronze 1-2)

Description:

Come stop by the Ham Radio Village to get your amateur radio license during our free license exams! More info on the DEF CON fourms

Register here: https://ham.study/sessions/610f2beb8f563a4f685389bf/1

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Friday - 09:00-15:59 PDT

Title: Ham Radio Exams

When: Friday, Aug 6, 09:00 - 15:59 PDT

Where: Ham Radio Village (Onsite - Bally's Bronze 1-2)

Description:

Come stop by the Ham Radio Village to get your amateur radio license during our free license exams! More info on the DEF CON fourms

Register here: https://ham.study/sessions/60fa3250a6684b06a0c6f327/1

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Saturday - 12:00-17:59 PDT

Title: Ham Radio Exams

When: Saturday, Aug 7, 12:00 - 17:59 PDT

Where: Ham Radio Village (Onsite - Bally's Bronze 1-2)

Description:

Come stop by the Ham Radio Village to get your amateur radio license during our free license exams! More info on the DEF CON fourms

Register here: https://ham.study/sessions/60fa327596cc8a184ebc8f89/1

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Sunday - 14:00-14:15 PDT

Title: Ham Radio Village Closing Commentary
When: Sunday, Aug 8, 14:00 - 14:15 PDT
Where: Ham Radio Village (Onsite - Bally's Bronze 1-2)

Description:
As our village wraps up for this year, a huge thank you to everyone for participating!

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Sunday - 12:00-13:59 PDT

Title: Hands-On TCP Deep Dive with Wireshark
When: Sunday, Aug 8, 12:00 - 13:59 PDT
Where: Packet Hacking Village - Workshops (Virtual)

SpeakerBio: Chris Greer , NETWORK ANALYST AND WIRESHARK INSTRUCTOR AT PACKET PIONEER
Chris Greer is a network analyst and Wireshark instructor for Packet Pioneer, a Wireshark University partner. He has focused much of his career at the transport layer, specifically TCP, specializing in how this core protocol works to deliver applications, services, and attacks between systems. Chris is a regular speaker at Sharkfest - the Wireshark Developer and User Conference, as well as an author for Pluralsight.

Description:
A solid understanding of how TCP works is critical for anyone interested in cybersecurity. Almost all enumeration, incident response, and traffic forensics require the analyst to dig into and interpret TCP flows. In this video we will take a look at how TCP is used to investigate and establish connections, how data is transmitted and acknowledged, how connections are torn down, and what problem indicators should catch our eye in Wireshark. This video welcomes all cybersecurity and Wireshark experience levels.

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 10:00-10:30 PDT

Title: Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables
When: Friday, Aug 6, 10:00 - 10:30 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Federico Lucifredi
Federico Lucifredi is the Product Management Director for Ceph Storage at Red Hat and a co-author of O'Reilly's ““Peccary Book”” on AWS System Administration. Previously, he was the Ubuntu Server product manager at Canonical, where he oversaw a broad portfolio and the rise of Ubuntu Server to the rank of most popular OS on Amazon AWS. A software engineer-turned-manager at the Novell corporation, he was part of the SUSE Linux team, overseeing the update lifecycle and delivery stack of a $150 million maintenance business. A CIO and a network software architect at advanced technology and embedded Linux startups, Federico was also a lecturer for over 200 students in Boston University's graduate and undergraduate programs, and simultaneously a consultant for MIT implementing fluid-dynamics simulations in Java.
Twitter: @0xF2
f2.svbtle.com

Description:
This is a live tutorial of hacking with keystroke injection attacks. We take advantage of the inherent trust that computers place on what is believed to be a regular keyboard to unleash pre-programmed keystroke payloads at well over 1000 words a minute. We access the host system and bypass traditional security countermeasures for payloads that can include reverse shells, binary injection, brute force password attacks, and just about any attack that can be fully automated.

We misuse the trust the operating system places on USB human-interaction devices to demonstrate once again the old adage that if you can physically access a computing device, there is no real security to be had. I will review hardware, its capabilities, how to breach OS security, and how attackers can enable it to perform a variety of tasks with its own tools. I will then show how to build and install additional software and customize the device with binary or scripted payloads.

We take the discussion to the next level by removing the need for a device and exploring attacks that can be delivered directly by a plain USB cable. We dissect easily-sourced, low-cost hardware implants embedded in standard, innocent-looking USB cables providing an attacker with further capabilities, including among them the ability to track its own geolocation.

#hhv-talk-qa-hw-hacking-101-text https://discord.com/channels/708208267699945503/709255105479704636

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 08:30-08:59 PDT

Title: Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables
When: Saturday, Aug 7, 08:30 - 08:59 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Federico Lucifredi
Federico Lucifredi is the Product Management Director for Ceph Storage at Red Hat and a co-author of O'Reilly's ""Peccary Book"" on AWS System Administration. Previously, he was the Ubuntu Server product manager at Canonical, where he oversaw a broad portfolio and the rise of Ubuntu Server to the rank of most popular OS on Amazon AWS. A software engineer-turned-manager at the Novell corporation, he was part of the SUSE Linux team, overseeing the update lifecycle and delivery stack of a $150 million maintenance business. A CIO and a network software architect at advanced technology and embedded Linux startups, Federico was also a lecturer for over 200 students in Boston University's graduate and undergraduate programs, and simultaneously a consultant for MIT implementing fluid-dynamics simulations in Java.
Twitter: @0xF2
f2.svbtle.com

Description:
This is a live tutorial of hacking with keystroke injection attacks. We take advantage of the inherent trust that computers place on what is believed to be a regular keyboard to unleash pre-programmed keystroke payloads at well over 1000 words a minute. We access the host system and bypass traditional security countermeasures for payloads that can include reverse shells, binary injection, brute force password attacks, and just about any attack that can be fully automated.

We misuse the trust the operating system places on USB human-interaction devices to demonstrate once again the old adage that if you can physically access a computing device, there is no real security to be had. I will review hardware, its capabilities, how to breach OS security, and how attackers can enable it to perform a variety of tasks with its own tools. I will then show how to build and install additional software and customize the device with binary or scripted payloads.

We take the discussion to the next level by removing the need for a device and exploring attacks that can be delivered directly by a plain USB cable. We dissect easily-sourced, low-cost hardware implants embedded in standard, innocent-looking USB cables providing an attacker with further capabilities, including among them the ability to track its own geolocation.

#hhv-talk-qa-hw-hacking-101-text https://discord.com/channels/708208267699945503/709255105479704636

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Sunday - 14:00-14:30 PDT

Title: Hardware Hacking 101: Rogue Keyboards and Eavesdropping Cables
When: Sunday, Aug 8, 14:00 - 14:30 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Federico Lucifredi
Federico Lucifredi is the Product Management Director for Ceph Storage at Red Hat and a co-author of O'Reilly's ““Peccary Book”” on AWS System Administration. Previously, he was the Ubuntu Server product manager at Canonical, where he oversaw a broad portfolio and the rise of Ubuntu Server to the rank of most popular OS on Amazon AWS. A software engineer-turned-manager at the Novell corporation, he was part of the SUSE Linux team, overseeing the update lifecycle and delivery stack of a $150 million maintenance business. A CIO and a network software architect at advanced technology and embedded Linux startups, Federico was also a lecturer for over 200 students in Boston University's graduate and undergraduate programs, and simultaneously a consultant for MIT implementing fluid-dynamics simulations in Java.
Twitter: @0xF2
f2.svbtle.com

Description:
This is a live tutorial of hacking with keystroke injection attacks. We take advantage of the inherent trust that computers place on what is believed to be a regular keyboard to unleash pre-programmed keystroke payloads at well over 1000 words a minute. We access the host system and bypass traditional security countermeasures for payloads that can include reverse shells, binary injection, brute force password attacks, and just about any attack that can be fully automated.

We misuse the trust the operating system places on USB human-interaction devices to demonstrate once again the old adage that if you can physically access a computing device, there is no real security to be had. I will review hardware, its capabilities, how to breach OS security, and how attackers can enable it to perform a variety of tasks with its own tools. I will then show how to build and install additional software and customize the device with binary or scripted payloads.

We take the discussion to the next level by removing the need for a device and exploring attacks that can be delivered directly by a plain USB cable. We dissect easily-sourced, low-cost hardware implants embedded in standard, innocent-looking USB cables providing an attacker with further capabilities, including among them the ability to track its own geolocation.

#hhv-talk-qa-hw-hacking-101-text https://discord.com/channels/708208267699945503/709255105479704636

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Friday - 14:00-14:59 PDT

Title: Hardware Wallet Show and Tell
When: Friday, Aug 6, 14:00 - 14:59 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Michael Schloh von Bennewitz
No BIO available

Description:

Michael will show off a variety of village badges and hardware. Michael will also be available at other times in the village for various other hardware activities.

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Friday - 15:30-15:59 PDT

Title: Healthcare Innovation With People of All Abilities
When: Friday, Aug 6, 15:30 - 15:59 PDT
Where: Biohacking Village (Talk - Virtual)
Speakers: Joel Isaac,Pia Zaragoza

SpeakerBio: Joel Isaac
No BIO available

SpeakerBio: Pia Zaragoza , Presidential Innovation Fellow, #uxdesign, #civictech, #uxresearch, #accessibility
No BIO available

Description:
The World Bank reported in their 2020 Disability Inclusion report that there are one billion people or 15% of the world's population that experience some form of disability. During this presentation, Joel Isaac and Pia Zaragoza will go over key concepts around disability inclusion, universal design and accessibility to spark ideas around healthcare innovation amongst the disability, medical manufacturers, regulators, cyber research, citizen science, and biohacker communities.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 10:00-10:59 PDT

Title: Hi! I'm DOMAIN\Steve, please let me access VLAN2
When: Sunday, Aug 8, 10:00 - 10:59 PDT
Where: Track 2 CLOSED; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Justin Perdok
Justin is a Security Specialist at Orange Cyberdefense. Prior to working in 'The Cybers' he has worked at multiple MSPs as a jack of all trades with a focus on security and automation. Stuck in his old ways he's always trying to learn new things; Followed up by him spending 6 hours automating the 'new thing' instead of relying on 5 minutes of manual labor.
Twitter: @justinperdok

Description:

By responding to probing requests made by Palo Alto and SonicWALL firewalls, it's possible to apply security policies to arbitrary IPs on the network, allowing access to segmented resources.

Segmentation using firewalls is a critical security component for an organization. To scale, many firewall vendors have features that make rule implementation simpler, such as basing effective access on a user identity or workstation posture. Security products that probe client computers often have their credentials abused by either cracking a password hash, or by relaying an authentication attempt elsewhere. Prior work by Esteban Rodriguez and by Xavier Mertens cover this. In this talk I will show a new practical attack on identity-based firewalls to coerce them into applying chosen security policies to arbitrary IPs on a network by spoofing logged in users instead of cracking passwords.

Logged on user information is often gathered using the WKST (Workstation Service Remote Protocol) named pipe. By extending Impacket with the ability to respond to these requests, logged on users on a device can be spoofed, and arbitrary firewall rules applied.

We will dive into the details of how client probing has historically been a feature that should be avoided while introducing a new practical attack to emphasize that fact.

REFERENCES
https://www.coalfire.com/the-coalfire-blog/august-2018/the-dangers-client-probing-on-palo-alto-firewalls
https://isc.sans.edu/forums/diary/The+Risk+of+Authenticated+Vulnerability+Scans/24942/
https://github.com/SecureAuthCorp/impacket
https://www.rapid7.com/blog/post/2014/10/14/palo-alto-networks-userid-credential-exposure/
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXHCA0

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=lDCoyxIhTN8

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20J

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will only be broadcast to DCTV2, in local hotels and on Twitch. This talk is not being presented in Track 2.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Saturday - 11:30-11:59 PDT

Title: High Turnout, Wide Margins
When: Saturday, Aug 7, 11:30 - 11:59 PDT
Where: Voting Village (Talks - Virtual)
Speakers: Brianna Lennon,Eric Fey

SpeakerBio: Brianna Lennon
Brianna Lennon is the County Clerk and local election official for Boone County, Missouri. She holds a Master's in Public Policy and a law degree, both from the University of Missouri. Prior to her election as Boone County Clerk, Brianna served as an Assistant Attorney General in the Consumer Protection Division of the Missouri Attorney General's Office before joining the Missouri Secretary of State's Office under former Secretary Jason Kander. As the Deputy Director of Elections and first coordinator of the Election Integrity Unit in the Secretary of State's Office, she worked closely with local election authorities across the state to ensure that elections were simple, secure, and accessible for voters.

SpeakerBio: Eric Fey
Eric Fey is the Director of the St. Louis County Board of Elections in St. Louis, Missouri. Along with a bachelor's degree from Webster University in political science, Fey holds a Master’s in public administration from the University of Missouri-St. Louis with a specialty in election management and has served as a foreign election observer in a range of countries, from the now Russian-occupied territory in Ukraine to Belarus to Kazakhstan to Macedonia.

Description:
Local election officials faced unprecedented challenges while administering elections in 2020, from widespread disinformation to COVID-19 safety precautions. Unlike in previous election cycles, though, the global pandemic prevented officials from connecting in person to commiserate, share best practices, and support each other.

In December of 2020, the High Turnout Wide Margins podcast launched to fill the void and give administrators an outlet for discussing the nuts and bolts of elections. Co-hosts Brianna Lennon, an elected county clerk in Boone County, Missouri and Eric Fey, an appointed director of elections in St. Louis County, Missouri, talk to subject-matter experts on topics like cybersecurity, disinformation, and elections integrity. In this presentation, Lennon and Fey share key takeaways from these discussions.

High Turnout Wide Margins is not a commercial podcast.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

---

Return to Index - Add to Google Calendar - ics Calendar file

Title: High-Stakes Updates | BIOS RCE OMG WTF BBQ
When: Saturday, Aug 7, 10:00 - 10:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded
Speakers: Jesse Michael,Mickey Shkatov

SpeakerBio: Jesse Michael
Jesse Michael is an experienced security researcher focused on vulnerability detection and mitigation who has worked at all layers of modern computing environments from exploiting worldwide corporate network infrastructure down to hunting vulnerabilities inside processors at the hardware design level. His primary areas of expertise include reverse engineering embedded firmware and exploit development. He has also presented research at DEF CON, Black Hat, PacSec, Hackito Ergo Sum, Ekoparty, and BSides Portland.
Twitter: @JesseMichael

SpeakerBio: Mickey Shkatov
Mickey has been doing security research for almost a decade, one of specialties is simplifying complex concepts and finding security flaws in unlikely places. He has seen some crazy things and lived to tell about them at security conferences all over the world, his past talks range from web pentesting to black badges and from hacking cars to BIOS firmware.
Twitter: @HackingThings

Description:

With attacks moving below the operating system and computer firmware vulnerability discovery on the rise, the need to keep current platforms updated becomes important and new technology is developed to help defend against such threats. Major computer manufacturers are adding capabilities to make it easier to update BIOS.

Our research has identified multiple vulnerabilities in Dell's BiosConnect feature used for remote update and recovery of the operating system. These vulnerabilities are easy to exploit by an adversary in the right position, and are not prevented by protective technologies such as Secured Core PCs, BitLocker, BootGuard, and BIOS Guard.

Join us and together we will explore the new attack surfaces introduced by these UEFI firmware update mechanisms -- including a full walk-through of multiple vulnerability findings and the methods we used to create fully working exploits that gain remote code execution within the laptop BIOS and their effects on the operating system.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=qxWfkSonK7M

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20M

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

ASV - Friday - 16:00-16:25 PDT

Title: Holistic View of a Flight with Crowd Sourced Data

When: Friday, Aug 6, 16:00 - 16:25 PDT

Where: Aerospace Village (Virtual Talk)

SpeakerBio: Allan Tart

Allan Tart has worked in the field of Air Traffic Management over a decade, where he has had several roles. His latest position in OpenSky Network, has included air-ground VHF communications to his list of interests, which previously mainly concentrated only on surveillance systems.

Description:

During the talk an overview will be given about how one can use crowd sourced data for creating a holistic view of flight. The data used for the purpose will include both ADS-B and VHF voice communications.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=2FTSGCAG3EE

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: House of Heap Exploitation
When: Friday, Aug 6, 10:00 - 13:59 PDT
Where: Workshops - Las Vegas 5+6 (Onsite Only)
Speakers: James Dolan,Maxwell Dulin,Nathan Kirkland,Zachary Minneker

SpeakerBio: James Dolan , Security Engineer
James Dolan works for Security Innovation as a Security Engineer focusing on engagements ranging from IoT hacking to kiosk exploitation. His current research interests include emerging threats against Mobile and IoT devices. He has a degree in Computer and Information Science from University of Oregon. In his free time, James enjoys composing music, playing video games or hiking in the greater Seattle area.

SpeakerBio: Maxwell Dulin , Security Consultant
Maxwell Dulin (Strikeout) is a security consultant at Security Innovation hacking all things under the sun, from robots to web applications. Additionally, he started the Spokane Mayors Cyber Cup and has written pwnables for SSD. Maxwell has published many articles for a plethora of heap exploitation techniques, assorted web application hacking exploits and IoT device vulnerability hunting. He has previously spoken at DEFCON 27 IoT Village. In his free time, he plays with RF toys, hikes to fire lookouts and catches everything at dodgeball.

SpeakerBio: Nathan Kirkland , Security Researcher & Engineer
Raised on a steady diet of video game modding, when Nathan found programming as a teenager, he fit right into it. Legend says he still keeps his coffee (and tear) stained 1980s edition of The C Programming Language by K&R stored in a box somewhere. A few borrowed Kevin Mitnick books later, he had a new interest, and began spending more and more time searching for buffer overflows and SQL injections. Many coffee fueled sleepless nights later, he had earned OSCP, and graduated highschool a few months later. After a few more years of working towards a math degree and trying fervently to teach himself cryptanalysis, he decided to head back to the types of fun hacking problems that were his real first love, and has worked at Security Innovation ever since.

SpeakerBio: Zachary Minneker , Security Researcher & Engineer
Zachary Minneker is a security researcher and security engineer at Security Innovation. His first computer was a PowerPC Macintosh, an ISA which he continues to defend to this day. At Security Innovation, he has performed security assessments on a variety of systems, including robots for kids, audio transcription codecs, and electronic medical systems. He has previous experience administrating electronic medical systems, and deep experience in fuzzing, reverse engineering, and protocol analysis. His research has focused on techniques for in-memory fuzzing, macOS sandbox security, and IPC methods.

Description:
Heap exploitation is an incredibly powerful tool for a hacker. As exploit mitigations have made exploitation more difficult, modern exploit development has moved to the heap. However, heap exploitation is a subject that has evaded many people for years for one reason: they focus on the techniques instead of the allocator. By learning with an allocator first style, the techniques are easily understood and practical to use.

This workshop is for learning heap exploit development in GLibC Malloc. GLibC Malloc is the default allocator on most Linux distros. With this hands-on introduction into GLibC Malloc heap exploitation you will learn how the allocator functions, heap specific vulnerability classes and to pwn with a variety of techniques. Whether you're an avid CTFer or just trying to get into heap exploitation on your pwnables site, this course is good for adding another tool to the tools arsenal. After taking this course you will understand the GLibC Malloc allocator, be able to discover heap specific vulnerability classes and pwn the heap with a variety of techniques, with the capability to easily learn more.

Registration Link: https://www.eventbrite.com/e/house-of-heap-exploitation-las-vegas-5-6-tickets-162214679473

Prerequisites

Basic computer science background (x86_64 assembly, stack, programming skills in C & Python) Basic binary exploitation skills (buffer overflow exploitation, ROP, ASLR, etc.) Familiar with Linux developer tools such as the command line, Python scripting and GDB. Previous usage of pwntools is a plus

Materials needed:
Laptop with enough power for a moderately sized Linux VM Administrative access to the laptop 8GB RAM minimum 50GB harddrive space Virtualbox or another virtualization platform installed

---

Return to Index - Add to Google Calendar - ics Calendar file

BICV - Saturday - 16:30-16:30 PDT

Title: How Bias and Discrimination in Cybersecurity will have us locked up or dead
When: Saturday, Aug 7, 16:30 - 16:30 PDT
Where: Blacks in Cyber

SpeakerBio: Tennisha Martin
Tennisha Martin is the founder and Executive Director of a National Cybersecurity non-profit organization dedicated to providing education and resources to underserved communities and increasing the diversity in cyber. She has worked in a government consulting capacity for over 15 years and in her spare time is a Cyber Instructor, mentor, and red-team leaning ethical hacking advocate for diversity in Cyber and the executive suites.
Twitter: @misstennisha

Description:

This talk focuses on algorithmic analysis and machine learning in the healthcare and criminal justice settings. Algorithms make a lot of important decisions including selecting candidates for a particular residency in medical school, tests that identify skin cancer in patients or determining the sentencing recommendations for people convicted of a crime. The outcome of these decisions includes impacting the number of people (or people of color) in certain specialties, failing to identify skin cancer in people of color and recommending longer sentences for black people and in particular black men. Studies have been shown that bias in algorithms have a wide-ranging impact, especially in the areas of clinical decision support and in criminal justice. Clinical decision support is integrated into electronic health records around the world and are used to establish things like best practices, medication guidelines, and prioritization of patients. The idea behind clinical decision support is that the algorithms are used based on aggregated data to help health care providers provide a standard of care. The reality, however, is that there is a thin line between the algorithms acting as the basis for recommendations and them acting autonomously. The aggregation of data and the formulation of algorithms by a largely homogeneous population results in bias and discrimination against people of color. In criminal justice, the racial impact of predictive policing is that black people serve longer times in jail. In healthcare, the impact of algorithmic bias results in poorer health outcomes, and failure to diagnose and treat patients of color. The result is that bias and discrimination in artificial intelligence will have members of the Black community incarcerated or dead.

Blacks in Cyber talks will be streamed on YouTube.

YouTube: https://www.youtube.com/c/BlacksInCybersecurity

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 12:15-12:45 PDT

Title: How do you ALL THE CLOUDS?
When: Saturday, Aug 7, 12:15 - 12:45 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio:henry
As a security {engineer | data scientist}, Henry operates as an information/data security architect, previously as a security consultant and developer in the industry. In his current role, he interfaces with internal business partners in providing architectural guidance and aligning the business with best practices and building countless tools and automation for the benefit of IT and security personnel alike. He has learned the hard and fun way that learning itself shouldn't be considered a chore or a negative, but an opportunity to be able to be more effective and adaptive with the ever-changing needs of the business.
Twitter: @Bazinga73

Description:

If you think I'm shouting something about security strategy for a multi-cloud environment...it's because I AM. Secure your dangling DNS records. Your object storage is showing. I can see your compute workload from here. Get your security groups straight. Have you seen the laundry list of accounts no one has performed nary an IAM credential analysis? Are your analytic processes hamstrung and kludgey from, you know, being cloudy? Don't know to even assess your options? Let's talk about how to evaluate cloud security tools and the considerations you need to make for your enterprise.

By now, every company should not only be aware of the cloud but actively using it to some degree—whether run by your IT department or, unofficially, by your engineering teams and sales organizations itching to invite a script kiddie to pluck your precious intellectual property—I mean, POC and strut their stuff that they can take their security and IT matters into their own hands.

Either way, you need a strategy or a clue. One is good. Both are better. Tying them together is best.

In this talk, I'll cover a number of random things. The generic reasons why many teams want to use cloud accounts. The common gotchas that may improve or disrupt your obviously super awesome demo for your customer, boss, team. Or just to actually do real work and expand your organization's compute demand en masse.

The focus will be addressing the technical gotchas in managing, monitoring, and assessing the security needs against the "business" needs for your organization: engineering, IT, and compliance. Operationally, you'll hit a breaking point. Too many users, too many accounts, too many workloads hammering your cloud interface. I'll focus primarily on AWS but also generically cover the other major Cloud Service Provider flavors, as, in the end, it's all the same: your org may have gotten wind that there are other cloud accounts and they just wanted to play with ALL OF THEM. How do you corral these little beasts? Tools. Technology. Processes.

I'll focus on open source tools like Prowler and ScoutSuite, touch some for closed source, but you'll still need to understand how to operationally point, aim, and fire to make it scale for you. In my experience, there's a certain level of "je ne sais quoi" element to getting to a comfortable level in overseeing the management of all these cloud accounts. I'll probably spend the balance of the time critiquing each tool in the end and present pros/cons and likely scenarios for you/your team/your org's maturity here to help you to drive your choice. Who knows, maybe I'll talk about my own open-source spin on things!

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Friday - 11:30-12:30 PDT

Title: How expensive is quantum factoring, really?
When: Friday, Aug 6, 11:30 - 12:30 PDT
Where: Crypto & Privacy Village (Virtual)

SpeakerBio: Craig Gidney
Software engineer turned research scientist on Google's quantum team. Cut the cost of quantum factoring by 100x. Unofficial record holder for largest number not-actually-factored on a quantum computer.

Description:

Quantum computers are expected to eventually break RSA and ECC. But how big would the machine have to be, and how long would it need to run? This talk will discuss the hype, the reality, and the difficulties around quantum attacks on public key cryptography.

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 14:00-14:45 PDT

Title: How I broke into Mexico City's justice system application and database

When: Saturday, Aug 7, 14:00 - 14:45 PDT

Where: AppSec Village (Virtual)

SpeakerBio: Alfonso Ruiz Cruz
No BIO available

Description:
Brief talk about how a chain of simple vulnerabilities gained me admin access to the whole database and application of Mexico City's justice system. Leaving exposed every file from criminal, civil and familiar trials since 2008.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Saturday - 13:00-13:59 PDT

Title: How I defeated the Western Electric 30c
When: Saturday, Aug 7, 13:00 - 13:59 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:N thing
No BIO available

Description:
I will take you through my thoughts, motivation and techniques on how I defeated the infamous Western Electric 30c.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Sunday - 15:15-15:59 PDT

Title: How I got COVID in a RedTeam: Social engineering and physical intrusion for realistic attack simulations.
When: Sunday, Aug 8, 15:15 - 15:59 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Daniel Isler , Senior Social Engineer Pentester, Dreamlab Technologies
Senior Social Engineer Pentester, Bachelor in Arts of Representation, Actor and Scenic Communicator. With more than 10 years of experience as an academic in Acting classes in several Universities.

Since 2015 leads Fr1endly RATs, the Social Engineering unit at Dreamlab Technologies Chile. Specializing and developing techniques and methodologies for simulations of Phishing attacks, Vishing, Pretexting, Physical Intrusions and Red Team.

Twitter: @Fr1endlyRATs
https://www.linkedin.com/in/daniel-isler

Description:

Is it correct to define as Red Team a service that only exploits vulnerabilities from a single vector without including elements typical of highly complex attacks such as social engineering and physical intrusion? By leaving out the starting point of actual attacks to create simulations of these, are we really focusing on potential threats or just particular vulnerabilities? Isn't layer eight the first layer we should consider for threats and consequently recognize vulnerabilities? Through four extremely particular and highly probable scenarios. Under a storytelling format we will immerse ourselves in a test narrated in first person, under the context of a Red Team exercise. We will understand the importance of including social engineering and physical intrusion actions for highly complex attack simulations.

Even having the best preparation, state-of-the-art devices and overwhelming information gathering. Reality will always have variants and surprises that attackers know how to take advantage of. Exposure to these variants is critical for simulation practitioners to emulate and recognize potential threats.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

Title: How I use a JSON Deserialization 0day to Steal Your Money On The Blockchain
When: Friday, Aug 6, 18:00 - 18:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Hao Xing,Zekai Wu

SpeakerBio: Hao Xing
Hao Xing is a Security researcher from Tencent Security Xuanwu Lab. He made some presentations at Chaos Communication Congress and BlackHat Asia. His research foucs on Web security, Andoird security and Red Team. He reported lots of vulnerabilities for many internet giants such as Google, Microsoft, Alibaba etc.
Twitter: @RonnyX2017

SpeakerBio: Zekai Wu
No BIO available
Twitter: @hellowuzekai

Description:

Fastjson is a widely used open source JSON parser with 23'100 stars on GitHub. As a basic module of countless java web services, it serves hundreds of millions of users. We managed to find a way to bypass many security checks and mitigations by using the inheritance process of some basic classes, and achieve remote code execution successfully. We will disclose these high-risk and universal gadgets for the first time in this talk.

Now, we can control many important websites and affect millions of users. Let's make things more interesting. We found that this fastjson vulnerability affect a multi-billion-dollar blockchain. We designed multiple complex gadgets based on the features of the blockchain, and exquisitely achieved information leakage and pointer hijacking. Putting all these gadgets together, we achieved remote code execution on the blockchain nodes.

However, generally after remote code execution, we seem to have no better exploit method other than the 51% attack, which will lead to serious accounting confusion. After a detailed analysis of the architecture design of the public blockchain, we found a way from RCE to steal the public blockchain users' assets almost without any notification.

To the best of our knowledge, this is the first published attack case on the realization of covertly stealing user assets after RCE on the public blockchain nodes. We will propose a more covert post penetration exploit method for public blockchain nodes in this talk.

Blockchain is not bulletproof to security vulnerability. We will show you how to use classical web vulnerabilities attack the blockchain and how to steal real money from the decentralized cyber world.

REFERENCES

1. https://github.com/threedr3am/gadgetinspector 2. https://github.com/JackOfMostTrades/gadgetinspector 3. http://i.blackhat.com/us-18/Thu-August-9/us-18-Haken-Automated-Discovery-of-Deserialization-Gadget-Chains.pdf 4. http://i.blackhat.com/eu-19/Thursday/eu-19-Zhang-New-Exploit-Technique-In-Java-Deserialization-Attack.pdf 5. https://asm.ow2.io/asm4-guide.pdf

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=pUexrXOGCkE

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20H

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Saturday - 15:00-15:30 PDT

Title: How to Contact the ISS with a $30 Radio
When: Saturday, Aug 7, 15:00 - 15:30 PDT
Where: Ham Radio Village (Virtual Talks)

SpeakerBio: Gregg Horton
Gregg Horton K6XSS is a security professional by day and by night explores the airwaves with ham radio. He got his general license in January 2021 and is very interested in digital modes like JS8CALL. When not playing with antennas, He enjoys gardening and getting beat at pokemon cards by his 5 year old son.

Description:

This presentation will go over the basics of how to listen to the international space station using a handheld ham radio. We will also cover how to utilize the repeater on the ISS, Capturing SSTV images from the ISS, and what equipment you can use to maximize your contacts.

All Ham Radio Village talks will be streamed to Twitch, with discussion in Discord.

For more information, see https://hamvillage.org/dc29.html

Twitch: https://www.twitch.tv/hamradiovillage

#hrv-presentation-text: https://discord.com/channels/708208267699945503/736674835413073991

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 10:00-10:59 PDT

Title: How to Not Miss The Point: Reflections on Race, Health, and Equity
When: Saturday, Aug 7, 10:00 - 10:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Nia Johnson , Bioethicist, Lawyer, and Harvard Health Policy Ph.D. student
Nia Johnson is a bioethicist, a lawyer, and a Health Policy Ph.D. student at Harvard University, with a concentration in Political Analysis. She is originally from the Washington, D.C. Metropolitan area. Nia received her Bachelor of Arts in International Studies at Oakwood University, her Masters of Bioethics from the University of Pennsylvania, and her law degree from Boston University School of Law. Her research interests are at the intersection of health policy, race, bioethics, and the law. She is a writer for Crash Course's forthcoming African-American History series, has lectured at multiple institutions such as Yale University and the International Bioethics Retreat. She ran and founded The Neighborhood Bioethicist - a bioethics blog geared towards millennials and Black Americans - and served as the Editor-in-Chief of the American Journal of Law and Medicine from 2018-2019. Her work has been featured in Hastings Law Journal, JAMA Health Forum, and the Journal of Urban Health. She loves mentoring young women, bouldering, and entertaining in her spare time. Her favorite quote is from Beyoncé's Diva – "Where's my ladies up in here that like to talk back?"

Description: No Description available

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Saturday - 11:00-11:30 PDT

Title: How to Weaponize RLAs to Discredit an Election
When: Saturday, Aug 7, 11:00 - 11:30 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Carsten Schürmann
Carsten is a professor in computer science at the IT University of Copenhagen and heads the Center for Information Security and Trust. His research focuses on cyber- and information security, with particular emphasis on election security. He consults with EMBs, governmental, and non-governmental organizations on requirements and quality assurance for election technologies. Carsten is an expert in voting machine security and demonstrated at DefCon 2017 vulnerabilities of the WinVote voting machine. He has conducted experiments with risk-limiting audits in Denmark in 2014. Carsten has participated as core team member (IT expert) in the Carter Center Mission to Kenya 2017 and was part of the IFES Cyber Assessment Week in Ukraine 2018.He has also served as New Voting Technology Analyst for the OSCE Limited Election Observation Mission to the United States in 2018 and the Expert Election Mission to Estonia in 2019. Prior to moving to Denmark, Carsten was a member of the computer science faculty at Yale University. He holds a PhD degree from Carnegie-Mellon University.

Description:
Risk-limiting audits (RLAs) are widely considered to be the gold standard of election auditing, and there is an implicit assumption that a successful audit will also create confidence among the voters and hence public trust. If this were true, there would be little reason to fear that RLAs could ever be misused in a disinformation campaign. It turns out, however, that this assumption is not necessarily true: In a recent user study to appear this year's E-Vote-ID, we show that a significant number of survey participants change their opinion whether to trust an election after they learn the size of the sample needed to complete the RLA. In this talk we argue that even a well-intended correctly conducted RLA can be weaponized in a disinformation campaign.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Saturday - 14:00-14:30 PDT

Title: How vigilant researchers can uncover APT attacks for fun and non profit
When: Saturday, Aug 7, 14:00 - 14:30 PDT
Where: Recon Village (Virtual)

SpeakerBio: Ladislav Baco
No BIO available
Twitter: @ladislav_b

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: HTTP/2: The Sequel is Always Worse
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: James Kettle
James Kettle is Director of Research at PortSwigger Web Security, where he cultivates novel web attack techniques. Recent work has focused on HTTP Request Smuggling, and using web cache poisoning to turn caches into exploit delivery systems. Past research includes server-side RCE via Template Injection, client-side RCE via malicious formulas in CSV exports, and abusing the HTTP Host header to poison password reset emails and server-side caches. He is also the author of multiple popular Burp Suite extensions including HTTP Request Smuggler, Param Miner and Turbo Intruder. He has spoken at numerous prestigious venues including DEF CON, both BlackHat USA and EU, and OWASP AppSec USA and EU.
Twitter: @albinowax
https://skeletonscribe.net/

Description:

HTTP/2 is easily mistaken for a transport-layer protocol that can be swapped in with zero security implications for the website behind it. Two years ago, I presented HTTP Desync Attacks and kicked off a wave of request smuggling, but HTTP/2 escaped serious analysis. In this presentation, I'll take you beyond the frontiers of existing HTTP/2 research, to unearth horrifying implementation flaws and subtle RFC oversights.

I'll show you how these flaws enable HTTP/2-exclusive desync attacks, with case studies targeting high-profile websites powered by servers ranging from Amazon's Application Load Balancer to WAFs, CDNs, and bespoke stacks by big tech. I'll demonstrate critical impact by hijacking thick clients, poisoning caches, and stealing plaintext passwords to net multiple max-bounties.

After that, I'll unveil novel techniques and tooling to crack open a widespread but overlooked request smuggling variant affecting both HTTP/1 and HTTP/2 that is typically mistaken for a false positive.

Finally, I'll drop multiple exploit-primitives that resurrect a largely-forgotten class of vulnerability, and use HTTP/2 to expose fresh application-layer attack surface.

I'll leave you with an open-source scanner, a custom, open-source HTTP/2 stack, and free interactive labs so you can hone your new skills on live systems.

REFERENCES

> The HTTP/2 RFC is essential reading: https://tools.ietf.org/html/rfc7540 This research is built on my previous work on this topic: https://portswigger.net/research/http-desync-attacks-request-smuggling-reborn This presentation by defparam has good explanations of response queue poisoning and self-desync attacks: https://www.youtube.com/watch?v=3tpnuzFLU8g I had a partial research collision with Emil Lerner. His work provides an alternative perspective on certain techniques: https://github.com/neex/http2smugl

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=rHxVVeM9R-M

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20J

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Friday - 12:00-13:59 PDT

Title: Hunting Evil with Wireshark
When: Friday, Aug 6, 12:00 - 13:59 PDT
Where: Packet Hacking Village - Workshops (Virtual)

SpeakerBio: Michael Wylie
Michael Wylie, MBA, CISSP is the Sr. Manager of a 24/7/365 global managed threat hunting team. Prior to his current role, he was the Director of Cybersecurity at a top 100 CPA firm where he built out the offensive/defensive security service practice. Michael has developed and taught numerous courses for the U.S. Department of Defense, DEFCON, Colleges, and for clients around the world. Michael is the winner of numerous SANS challenge coin and holds the following credentials: CISSP, CCNA R&S, GPEN, GMON, GCFE, TPN, CEH, CEI, VCP-DCV, CHPA, PenTest+, CNVP, Microsoft Azure, and more.
Twitter: @themikewylie

Description:
This workshop will take attendees' Wireshark skills to the next level with a heavy emphasis on incident response, threat hunting, and identifying anomalous network traffic. This workshop will begin with a brief introduction to Wireshark and other Network Security Monitoring (NSM) tools/concepts. Throughout the workshop, we'll examine what different attacks and malware look like while using Wireshark. Attendees will then have hands-on time in the lab to search for Indicators of Compromise (IOCs) and TTPs utilizing staged packet capture files. Labs start out easy and quickly progress in difficulty. There will be plenty of take-home labs for additional practice.

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 13:20-14:05 PDT

Title: Hunting for AWS Exposed Resources
When: Friday, Aug 6, 13:20 - 14:05 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Felipe Pr0teus Espósito
Felipe Espósito graduated in Information Technology at UNICAMP and has a master's degree in Systems and Computing Engineering by COPPE-UFRJ, both among the top technology universities in Brazil. He has over ten years of experience in information security and IT, with an emphasis on security monitoring, networking, data visualization, and threat hunting. He is a founder of the HackerMakerSpace in Rio de Janeiro and presented at respected conferences such as Hackers 2 Hackers Conference, BHACK, BSides (Las Vegas and São Paulo), FISL, Latinoware, SecTor and SANS SIEM Summit.
Twitter: @pr0teusbr

Description:
Like all major public cloud providers, AWS allows users to expose managed resources like S3 buckets, SQS queues, RDS databases, and others publicly on the Internet. There are legitimate uses for making resources public, such as publishing non-sensitive data. However, we often find that this functionality is mistakenly used, often due to a lack of cloud security expertise, to erroneously expose sensitive data. News of exposed S3 buckets are sadly very frequent in the specialized media. It is important to note, however, that there are many other relevant kinds of AWS resources that can be equally dangerous when publicly exposed but that doesn't get nearly as much scrutiny as S3 buckets. In this talk we are going to describe some of the methods that researchers and attackers use to discover and exploit these publicly exposed resources, and how cloud providers and defenders can have taken action to monitor, prevent and respond to these activities.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Saturday - 11:00-11:30 PDT

Title: Hybrid PhySec tools - best of both worlds or just weird?
When: Saturday, Aug 7, 11:00 - 11:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:d1dymu5
No BIO available

Description:
A few years ago, I invented lock pick collar stays (#GentlemansLockPicks). Since then, I've had some other ideas of practical, small-form factored lockpicking and bypass tools that I can easily carry. I came up with a few ideas. I'll talk about inspiration, designing, manufacturing, and possible collab projects.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 09:00-09:15 PDT

Title: I know who has access to my cloud, do you?
When: Saturday, Aug 7, 09:00 - 09:15 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Igal Flegmann
Igal started his career in Microsoft's Azure Security team creating and managing identity services for Azure's secure production tenants. During his time at Azure Security, Igal had the opportunity to create and manage PKI services, Identity Management products, tools for migrating running services across Azure tenants, and created products for password-less bootstrap to new domains. After a successful career in Azure Security, Igal transferred teams to work in Azure's ASCII (Azure Special Capabilities, Infrastructure, and Innovation) team, where he used his identity and security expertise to design and create security services to protect the critical infrastructure devices of the world.

To follow his passion for identity and security, Igal decided to leave Microsoft and Co-found, Keytos a security company with the mission of eliminating passwords by creating easy to use PKI offerings. Earlier this year they launch their first product "EZSSH" which takes aim at stopping SSH Key theft by making it easy to use short lived SSH Certificates.

Twitter: @igal_fs

Description:

In this talk, we will talk about the importance of monitoring your Azure RBAC and we will introduce SubWatcher our newly released open-source tool that we use internally to compliment Azure security tools and scan our subscriptions to make sure our systems are not being accessed by bad actors. Can't wait to see where the community takes this amazing tool!

When comparing security reviews with red team findings, I always found that security reviews are based on what they think their system looks like and not how it actually is. Is the SSH port really closed? Or did I forget to close it the last time I was debugging something? Wait who added this identity as owner of the resources and when?!

Azure Security Center provides us with some great tools to check some of these errors. For example, from the two examples above it will alert on the SSH port being left open but it would not alert on some new person being added to your production subscription.

The Solution? SubWatcher our internal tool that it was too good to keep in-house and not share it with the world. SubWatches is an open-source tool that monitors your Azure Subscription ACLs and will alert you if they changed based on the baseline you have created.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Sunday - 10:45-11:15 PDT

Title: I know who has access to my cloud, do you?

When: Sunday, Aug 8, 10:45 - 11:15 PDT

Where: Cloud Village (Virtual)

SpeakerBio: Igal Flegmann

Igal started his career in Microsoft's Azure Security team creating and managing identity services for Azure's secure production tenants. During his time at Azure Security, Igal had the opportunity to create and manage PKI services, Identity Management products, tools for migrating running services across Azure tenants, and created products for password-less bootstrap to new domains. After a successful career in Azure Security, Igal transferred teams to work in Azure's ASCII (Azure Special Capabilities, Infrastructure, and Innovation) team, where he used his identity and security expertise to design and create security services to protect the critical infrastructure devices of the world.

To follow his passion for identity and security, Igal decided to leave Microsoft and Co-found, Keytos a security company with the mission of eliminating passwords by creating easy to use PKI offerings. Earlier this year they launch their first product "EZSSH" which takes aim at stopping SSH Key theft by making it easy to use short lived SSH Certificates.

Twitter: @igal_fs

Description:

Working in security over the last few years I have learned that it is nearly impossible to stop a breach from happening. While having great security practices such as: Isolated password-less identities, isolated devices, and condition access; will help you stop 99% of the attacks we need to ask ourselves the following questions: Are we monitoring our infrastructure for changes that might open an attack vector? Are we ready to detect and remediate our next breach before the attacker can do any damage? Azure Security Center provides us with some great tools to check some of these errors. For example, it will alert on the SSH port being left open but it would not alert on a very large IP address range being added to your networking rules. The Solution? CloudWatcher our open-source tool that monitors your Azure Subscription ACLs and will alert you if they changed based on the baseline you have created.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 10:00-10:45 PDT

Title: I used AppSec skills to hack IoT, and so can you
When: Saturday, Aug 7, 10:00 - 10:45 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Alexei Kojenov
Alexei began his career as a software developer. A decade later, he realized that breaking code was way more fun than writing code, and decided to switch direction. He is now a full-time application security professional, with several years of assisting various development teams in delivering secure code, as well as security consulting. Outside of his day job, Alexei enjoys doing security research and learning new hacking techniques.

Description:

We tend to think of AppSec and IoT as two separate infosec disciplines. Sure, the domain knowledge, attack vectors, and threat mitigation are not exactly the same in those two worlds. At the same time, as the hardware continues to evolve, we see more and more tiny general purpose computers around us. Many of these tiny computers nowadays run software that is written in a conventional programming language, listen on network ports, process data inputs, and communicate with the outside world. These devices can be attacked just like any other application running on a desktop, on a server, or in the cloud.

In this talk, I am going to tell you a story about my hacking journey that unexpectedly took me from device configuration settings to software reverse engineering, vulnerability discovery, and six new CVEs. Together, we'll go step by step through reconnaissance, firmware analysis, decompiling, code review, and remote debugging. I'll also share my experience with the responsible disclosure process. I hope this talk inspires you to apply your general hacking skills to new areas such as IoT, even if you've never done that before.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 10:00-10:45 PDT

Title: I used AppSec skills to hack IoT, and so can you
When: Saturday, Aug 7, 10:00 - 10:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Alexei Kojenov
Alexei began his career as a software developer. A decade later, he realized that breaking code was way more fun than writing code, and decided to switch direction. He is now a full-time application security professional, with several years of assisting various development teams in delivering secure code, as well as security consulting. Outside of his day job, Alexei enjoys doing security research and learning new hacking techniques.

Description:
We tend to think of AppSec and IoT as two separate infosec disciplines. Sure, the domain knowledge, attack vectors, and threat mitigation are not exactly the same in those two worlds. At the same time, as the hardware continues to evolve, we see more and more tiny general purpose computers around us. Many of these tiny computers nowadays run software that is written in a conventional programming language, listen on network ports, process data inputs, and communicate with the outside world. These devices can be attacked just like any other application running on a desktop, on a server, or in the cloud.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: ICS Cyber Threat Intelligence (CTI) Information Sharing Between Brazil and the United States
When: Sunday, Aug 8, 12:00 - 12:59 PDT
Where: ICS Village (Virtual)
Speakers: Helio Sant'ana,John Felker,Max Campos,Paul de Souza,Tom VanNorman

SpeakerBio: Helio Sant'ana
Master's student in Cyber Security, Post-Graduate in IT Management, Digital Forensic and graduated in Information Systems. Held many management positions in Information Technology units, working last decades within Private, Civil, and Military Public agencies. Experienced in the development of Public Policies, Data Protection, Information, and Cyber Security, currently holds the position of Director of Information Technology at the Presidency of Brazil.
https://www.linkedin.com/in/hcsantana/

SpeakerBio: John Felker
Building upon a long career in government and the private sector, John Felker works with senior leaders to see and understand the big cybersecurity picture, the risk, and the business impact of cyber threats. He brings wide-ranging leadership, organizational, and business experiences that can help you prepare for the worst, understand, and address the issues, and ultimately, succeed. A sought-after cybersecurity and leadership expert, he is a frequent speaker at national and international cybersecurity conferences.

Felker is the former Assistant Director for Integrated Operations, Cybersecurity, and Infrastructure Security Agency (CISA) where he brought focus to integrated operations across the Agency that extended to Regional CISA elements, intelligence, operational planning, and mission execution with emphasis on risk mitigation and response efforts.

He previously served as the Director of the National Cybersecurity and Communications Integration Center from 2015 to 2019. Prior to joining CISA, Felker worked as Director of Cyber and Intelligence Strategy for HP Enterprise Services and in a 30-year career, served as Deputy Commander, Coast Guard Cyber Command; Commander, Coast Guard Cryptologic Group, as Executive Assistant to the Director of Coast Guard Intelligence and commanded the cutters CAPE UPRIGHT and RED CEDAR.

Felker is President of Morse Alpha Associates, Inc., a cyber leadership consultancy, serves as a member of the Parsons Corporation Senior Advisory Board, a Senior Advisor to the Chertoff Group, as a Senior Advisor to the Maritime Transportation System ISAC, a Senior Advisor to S-RM, an international cyber intelligence, response, and resilience company and a Senior Fellow at the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University. He is a member of the National Technology Security Coalition’s Advisory Council and is currently on the Board of Directors of the Operation Renewed Hope Foundation and the Boards of Advisors for the Military Cyber Professionals Association, and the Cyber Security Forum Initiative.

He is the recipient of the Department of Homeland Security Outstanding Public Service Medal, and his military awards include the Defense Superior Service Medal, the Legion of Merit, and the Meritorious Service Medal.

Felker graduated from Ithaca College with a Bachelor of Science and earned his Master of Arts in Public Administration from the Maxwell School of Citizenship and Public Affairs at Syracuse University and has co-authored several papers on cyber intelligence under the auspices of the Intelligence and National Security Alliance.

https://www.linkedin.com/in/jofelker/

SpeakerBio: Max Campos
Brazilian Army Major Max Campos is Head of the Knowledge Management Section of the Department of Strategic Management of the Cyber Defense Command and serves as Coordinator of the Cyber Guardian Exercise Study Group. He has a master’s degree in Computer Systems from the University of Salvador (Brazil) and has earned his CISSP, GISCP, CISO and Cyber Ops certifications. With over a decade of cyber experience, Major Campos has supported various major international

events such as Rio + 20, Confederations Cup, World Cup, and in many strategic projects of the Brazilian Ministry of Defense. Starting with the first iteration of the Cyber Guardian Exercise in 2018, he has acted as Coordinator of the Study Group and the leading representative of national critical infrastructure for the development of scenarios for sectors of interest in the formulation of themes and matters of interest to the sector.
https://www.linkedin.com/in/maxcampos/

SpeakerBio: Paul de Souza , Founder and President for the Cyber Security Forum Initiative (CSFI)
Mr. Paul de Souza is the Founder of the Cyber Security Forum Initiative (CSFI), a nonprofit organization specializing in cyberspace operations awareness and training. As a former Federal Director of Training and Education for Norman Data Defense Systems, Chief Security Engineer for AT&T, and security engineer for Computer Sciences Corporation (CSC) and US Robotics, Mr. de Souza has over 20 years of cybersecurity experience. He has consulted for several governments, military organizations, and private institutions around the globe. He is a recipient of the Order of Thor Medal.

Mr. de Souza holds various cybersecurity, cyber intelligence, and counter-terrorism Advisory Board positions for organizations such as the Military Cyber Professionals Association (MCPA), the Ben-Gurion University of the Negev in Israel, and IntellCorp in Portugal. Past board positions include the Institute of World Politics (IWP) and Visiting Research Fellow at the National Security Studies (INSS), Tel Aviv, Israel.

Paul serves as a visiting researcher, guest lecturer, ambassador, and faculty member for several higher educational institutions, such as Sheffield Hallam University (UK), Tel Aviv University, the Swedish Defence University (F˜rsvarsh˜gskolanand), American Public University, and George Washington University.

In addition to earning a master’s degree in National Security Studies with a concentration in Terrorism from American Military University, Mr. de Souza has completed the Executive Certificate Program in Counter-Terrorism Studies from the Interdisciplinary Center (IDC) Herzliya in Israel, is an alumnus from the Harvard Kennedy School’s Cybersecurity Executive Education program with a Higher Education Teaching certification from Harvard University, and is currently pursuing his Ph.D. in Critical Infrastructure from Capitol Technology University.

https://www.linkedin.com/in/paulcsfi/

SpeakerBio: Tom VanNorman
Tom co-founded the ICS Village, a non-profit organization focused on Control System security and awareness. He is also retired from the Air National Guard, where he worked in Cyber Warfare Operations. Tom leads the CyPhy Product group at GRIMM, where his primary focus is securing Industrial Control Systems and the networking of such systems. Tom brings an unparalleled level of operational knowledge and experience, as he has been working in the Operational Technology (OT) field for almost three decades. He also has considerable knowledge in constructing Cyber-Physical testing environments for OT systems.
https://www.linkedin.com/in/thomasvannorman/

Description:

The panelists will touch on topics such as the annual critical infrastructure themed exercise Cyber Guardian run by the Brazilian Cyber Command and the opportunities for industrial control systems (ICS) professionals in the US to become more involved. Topics such as national Malware Information Sharing Platform (MISP) implementation in Brazil focusing on information sharing, particularly in the ICS world, will be discussed. The ICS Village and the Cyber Security Forum Initiative will engage in conversation with the Brazilian government during this session.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

ICSV - Sunday - 13:00-13:30 PDT

Title: ICS Intrusion KillChain explained with real simulation
When: Sunday, Aug 8, 13:00 - 13:30 PDT
Where: ICS Village (Virtual)
Speakers: Javier Perez,Juan Escobar

SpeakerBio: Javier Perez , Dreamlab Technologies
Director of R&D at Dreamlab Technologies. Fan of tech and cybersecurity, more than 10 years in the cybersecurity world. ISECOM OSSTMM and MILE2 instructor, trainer for private cybersecurity courses, speaker, researcher, cybersecurity consultant, penetration tester. During recent years, I have specialized in payment systems (EMV, NFC, POS, ATM) and industrial environment (ICS/SCADA).
Twitter: @the_s41nt

SpeakerBio: Juan Escobar
Professional with solid skills and knowledge in pentesting methodologies such as OWASP and OSSTMM, with extensive expertise in projects of Ethical hacking web applications, mobile applications and infrastructure, ATM Pentesting and Code analysis, combined with a good attitude to work. He has extensive experience in the development of exploits for the Metasploit Framework, with excellent command of Python, PHP, Java, C#, C and Ruby programming languages. He developed a translation extension for Mozilla Firefox that currently has more than half a million active users: https://addons.mozilla.org/firefox/addon/to-google-translate/He has participated in international computer security competitions, together with the Latin American team NULL Life, as well as internationally recognized talks and conference.
Twitter: @itsecurityco

Description:

Cyber attacks on Industrial Control Systems (ICS) differ in scope and impact based on a number of factors, including the adversary's intent, sophistication and capabilities, and familiarity with ICS and automated indutrial processes. In order to understand, identify and address the specific points that can prevent or stop an attack, a systematic model known as "Cyber Kill Chain" is detailed, a term that comes from the military environment and registered by the Lockheed Martin company. While most are familiar with terms and theoretical diagrams of how security should be implemented, in this talk we want to present live how an attack chain occurs from scratch to compromise industrial devices, the full kill chain, based in our experiences. The goal is to land these threats into the real world without the need to carry out these attacks with a nation-state budget.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

Title: ICS Jeopardy

When: Sunday, Aug 8, 14:00 - 14:59 PDT

Where: ICS Village (Virtual)

Speakers: Chris Sistrunk,Maggie Morganti,Mary Brooks,Tatyana Bolton

SpeakerBio: Chris Sistrunk , Mandiant

Chris Sistrunk is Technical Manager on the Mandiant ICS/OT Security Consulting team at FireEye focusing on protecting critical infrastructure. Before FireEye, Sistrunk was a Senior Engineer at Entergy where he was a subject matter expert for Transmission & Distribution SCADA systems. Sistrunk was awarded Energy Sector Security Professional of the Year in 2014. He is a Senior Member of the IEEE and is a registered Professional Engineer in Louisiana. He founded BSidesJackson, co-founded the BEER-ISAC, and helped organize the ICS Village at DEFCON 22. He holds BS Electrical Engineering and MS Engineering & Technology Management degrees from Louisiana Tech University.
Twitter: @chrissistrunk

SpeakerBio: Maggie Morganti , Schneider Electric

Maggie Morganti is a Product Security Researcher at Schneider Electric where she works on vulnerability handling, supply chain security, and secure product development for power systems. She also serves as the Director-Elect of the ISA Communications Division (COMDIV). She previously held roles as a Cyber Technical Staff member for Oak Ridge National Laboratory’s Power & Energy Systems team and as a Threat Intelligence Analyst for FireEye Mandiant’s Cyber-Physical team. She holds a M.S. in Intelligence Studies with a focus on cybersecurity from Mercyhurst University.
Twitter: @magg_py

SpeakerBio: Mary Brooks , R Street Institute

Mary Brooks is a senior research associate for Cybersecurity and Emerging Threats at R Street Institute. Before joining R Street, she was lead researcher and associate producer for The Perfect Weapon (2020). Prior to this, she served as the special assistant for the international human rights law firm Perseus Strategies, LLC, based in Washington, D.C. She graduated cum laude from Harvard University with a bachelor’s degree in government and a language certificate in Arabic.
Twitter: @Mary_K_Brooks

SpeakerBio: Tatyana Bolton , R Street Institute

Tatyana Bolton is the Policy Director for R Street’s Cybersecurity & Emerging Threats team. She crafts and oversees the public policy strategy for the department with a focus on secure and competitive markets, data security and data privacy, and diversity in cybersecurity. Most recently, Tatyana worked as the senior policy director for the U.S. Cyberspace Solarium Commission focusing on U.S. government reorganization and resilience portfolios. From 2017-2020, Tatyana also served at the Cybersecurity and Infrastructure Security Agency as the cyber policy lead in the Office of Strategy, Policy and Plans where she developed strategies for strengthening the cybersecurity of our nation’s critical infrastructure.
Twitter: @TechnoTats

Description:

This. Is. Jeopardy. ICS-style. Join our intrepid contestants in a full round of the iconic game show Jeopardy as they test their knowledge of the various categories every good cybersecurity expert should know—including historical ICS incidents, nerdy fiction and random trivia—all the while performing on-the-spot asset identification (aka: figuring out the remote buzzer system because we're still in a pandemic.) Tune in to watch Maggie Morganti of Schneider Electric, Chris Sistrunk of Mandiant, and Tatyana Bolton of the R Street Institute battle it out to win one of three, appropriately mediocre, prizes.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 15:00-15:30 PDT

Title: Identifying Excel 4.0 Macro strains using Anomaly Detection
When: Friday, Aug 6, 15:00 - 15:30 PDT
Where: AI Village (Virtual)
Speakers: Elad Ciuraru,Tal Leibovich

SpeakerBio: Elad Ciuraru
No BIO available

SpeakerBio: Tal Leibovich
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Sunday - 10:00-10:45 PDT

Title: Identifying toxic combinations of permissions in your cloud infrastructure
When: Sunday, Aug 8, 10:00 - 10:45 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Michael Raggo
Michael Raggo has over 20 years of security research experience. His current research focuses on Cloud security. His research has been highlighted on television's CNN Tech, and numerous media publications including TIME, Forbes, Bloomberg, Dark Reading, TechCrunch, TechTarget, The Register, and countless others. Michael is the author of "Mobile Data Loss: Threats & Countermeasures" and "Data Hiding" for Syngress Books, and is a contributing author for "Information Security the Complete Reference 2nd Edition". His Data Hiding book is also included at the NSA's National Cryptologic Museum at Ft. Meade. A former security trainer, Michael has briefed international defense agencies including the FBI and Pentagon; and is a former participating member of the PCI Council. He is also a frequent presenter at security conferences, including Black Hat, DEF CON, RSA, OWASP, HackCon, and SANS. He was also awarded the Pentagon's Certificate of Appreciation.
Twitter: @datahiding

Description:

With more than 24,000 permissions across AWS, Azure, and GCP, how does one determine who gets what permissions? Half of the 10,000 permissions in AWS are admin-like permissions. This is even more complicated when new permissions and services are being added almost daily. Mapping these out and understanding their implications is a difficult task, yet attackers understand them well enough to leverage toxic combinations of these permissions for privilege escalation and exploiting your cloud infrastructure. In this presentation, we'll share our experiences in doing > 150 risk assessments across AWS, Azure, and GCP. We'll review common admin permissions that we commonly find accidentally assigned to developers and users. We'll reveal some extremely powerful permissions that can be mapped to a Cyber Kill Chain specific to cloud infrastructure. This will uncover toxic combinations of permissions that can lead to lateral movement, privilege escalation, exfiltration, and more. We'll provide real world examples of findings from audit logs, activity monitoring, and ML-based anomaly analysis. We'll then outline a strategy to tracking this moving forward actively within your environment and how to mitigate this over-permissioned access to build a permissions management lifecycle.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 12:00-15:59 PDT

Title: In Space, No One Can Hear You Hack
When: Saturday, Aug 7, 12:00 - 15:59 PDT
Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:

In Space, No One Can Hear You Hack: DEF CON participants will learn the basics of space hacking and space vehicle security. This is the perfect point of entry for those interested in space hacking.

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Friday - 14:00-15:50 PDT

Title: In-person broadcast via demolabs
When: Friday, Aug 6, 14:00 - 15:50 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: Constantine Macris
No BIO available

Description:
This is a placeholder event.

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

WS - Friday - 10:00-13:59 PDT

Title: Inspecting Signals from Satellites to Shock Collars
When: Friday, Aug 6, 10:00 - 13:59 PDT
Where: Workshops - Las Vegas 1+2 (Onsite Only)
Speakers: Eric Escobar,Trenton Ivey

SpeakerBio: Eric Escobar , Principal Security Consultant
Eric is a seasoned pentester and a Principal Security Consultant at Secureworks. On a daily basis he attempts to compromise large enterprise networks to test their physical, human, network and wireless security. His team consecutively won first place at DEF CON 23, 24, and 25's Wireless CTF, snagging a black badge along the way. Forcibly retired from competing in the Wireless CTF, he's now a member of the DEF CON Wireless Village team. Before entering the cyber security arena, Eric attained both a BS and MS in Civil Engineering along with his Professional Engineering license.

SpeakerBio: Trenton Ivey , Senior Security Researcher
Trenton is a Senior Security Researcher for Secureworks' Counter Threat Unit and is a Technical Lead for Secureworks Adversary Group. He currently builds tools to assist with offensive testing, and helps defenders find creative ways to respond. Prior to joining Secureworks, Trenton helped build the network penetration team for a Fortune 500 company, performed web-application and device testing for a PA-QSA company, and provided IT support for one of the largest health systems in the US. Trenton received his Bachelors of Science in Biology and Chemistry and now regularly tries to find ways to apply lessons learned from the physical world to the digital one. Trenton has his Expert Class Amateur Radio license and is a lifelong member of AMSAT (Amateur Radio in Space).

Description:

Invisible signals control everything from satellites to shock collars. Wireless security can be intimidating, especially when research requires a low-level understanding of the many ways radio waves can carry data. The concept of using light to send messages is not hard to grasp, but the several abstraction layers between physical radio waves and decoded data packets obscure what is really happening when wireless devices communicate. By examining several topics that are rarely presented together, this workshop provides the introduction to wireless hacking that we both wish we had when starting out. If you want the ability to see and manipulate the unseen, this workshop is for you.

Registration Link: https://www.eventbrite.com/e/inspecting-signals-from-satellites-to-shock-collars-tickets-162215666425

Prerequisites
Students are expected to have basic familiarity with the Linux command line.

Materials needed:
Students will need to bring a wifi-enabled laptop with a modern browser.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 14:00-14:20 PDT

Title: Instrument and Find Out: Writing Parasitic Tracers for High(-Level) Languages
When: Sunday, Aug 8, 14:00 - 14:20 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Jeff Dileo
Jeff Dileo (chaosdata) is a security consultant by day, and sometimes by night. He hacks on embedded systems, mobile apps and devices, web apps, and complicated things that don't have names. He likes candy and arguing about text editors and window managers he doesn't actually use.
Twitter: @chaosdatumz

Description:

Modern programming languages are, more and more, being designed not just around performance, ease-of-use, and (sometimes) security, but also performance monitoring and introspectability. But what about the languages that never adopted such concepts from their peers? Or worse, what about the languages that tacked on half-hearted implementations as an afterthought? The answer is simple, you write your own and instrument them into the language dynamically.

In this talk, we will discuss the process for developing generalized parasitic tracers targeting specific programming languages and runtimes using Ruby as our case study. We will show how feasible it is to write external tracers targeting a language and its runtime, and discuss best practices for supporting different versions over time.

REFERENCES
* https://github.com/ruby/ruby * https://frida.re/docs/javascript-api/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=Iy1BNywebpY

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20J

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Friday - 10:00-10:59 PDT

Title: Internet Protocol (IP)
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: Packet Hacking Village - Talks (Virtual)

SpeakerBio: Roy Feng
Roy Feng (Twitter: @LPF613) is a networking and cybersecurity enthusiast. He has six years of experience working as a network engineer and one year working in threat intelligence. His latest role is at a managed security service provider, where he leads a team of incident responders and threat hunters to help investigate and respond to incidents as well as hunt for threats in customer environments. In his spare time, Roy can be seen building and maintaining his home lab, and learning about and tinkering with the latest and greatest technologies.
Twitter: @LPF613

Description:
The Internet Protocol is one of the foundational protocols of the Internet, and is what keeps devices connected. This video talks about the fundamentals of the Internet Protocol.

All Packet Hacking Village talks will stream on YouTube, Twitch, Facebook, and Periscope.

YouTube: https://youtube.com/wallofsheep

Twitch: https://twitch.tv/wallofsheep

Facebook: https://www.facebook.com/wallofsheep/

Periscope: https://www.periscope.tv/wallofsheep

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Sunday - 10:30-10:59 PDT

Title: Internet-of-Ingestible-Things Security by Design
When: Sunday, Aug 8, 10:30 - 10:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Mariam Elgabry , Co-founder & Director of Enteromics
Co-founder and Director of Enteromics, a MedTech startup that builds smart pills for smart health. She has led award winning projects at AstraZeneca and Microsoft and her bio-crime research has been recognised by the UK Parliament Joint Committee on National Security.
Twitter: @MariamElgabry11

Description:

In this talk I will share the outcomes of the very first Internet-of-Ingestible-Things workshop that brings cybersecurity experts and medical device regulatory bodies together to think about cyber-biosecurity at design stage of medical devices and to inform policy by delivering a set of principles for Security by Design.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Sunday - 15:00-15:59 PDT

Title: Intro to high security locks and lockpicking
When: Sunday, Aug 8, 15:00 - 15:59 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:N thing
No BIO available

Description:
This is a quick introduction to high security locks, what they are, what they look like and how to get started defeating them.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Friday - 10:00-10:30 PDT

Title: Intro To Lockpicking
When: Friday, Aug 6, 10:00 - 10:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:

New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Friday - 12:00-12:30 PDT

Title: Intro To Lockpicking
When: Friday, Aug 6, 12:00 - 12:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Friday - 14:15-14:45 PDT

Title: Intro To Lockpicking
When: Friday, Aug 6, 14:15 - 14:45 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Friday - 16:15-16:45 PDT

Title: Intro To Lockpicking
When: Friday, Aug 6, 16:15 - 16:45 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Saturday - 10:00-10:30 PDT

Title: Intro To Lockpicking
When: Saturday, Aug 7, 10:00 - 10:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Saturday - 12:00-12:30 PDT

Title: Intro To Lockpicking
When: Saturday, Aug 7, 12:00 - 12:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Saturday - 14:15-14:45 PDT

Title: Intro To Lockpicking
When: Saturday, Aug 7, 14:15 - 14:45 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Saturday - 16:15-16:45 PDT

Title: Intro To Lockpicking
When: Saturday, Aug 7, 16:15 - 16:45 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Sunday - 10:00-10:30 PDT

Title: Intro To Lockpicking
When: Sunday, Aug 8, 10:00 - 10:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Sunday - 12:00-12:30 PDT

Title: Intro To Lockpicking
When: Sunday, Aug 8, 12:00 - 12:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Sunday - 14:15-14:45 PDT

Title: Intro To Lockpicking
When: Sunday, Aug 8, 14:15 - 14:45 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio:TOOOL
No BIO available

Description:
New to lock picking? Haven't picked in a year and need a refresher? Don't know a half-diamond from a turner? This talk is for you! Join one of our knowledgable village volunteers as we walk you through the very basics of lock picking, from how to hold your tools to the theory behind the technique that makes lock picking possible.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 09:30-10:59 PDT

Title: Intro to ML Workshop
When: Friday, Aug 6, 09:30 - 10:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Gavin Klondike
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 09:30-10:59 PDT

Title: Intro to ML Workshop
When: Saturday, Aug 7, 09:30 - 10:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Gavin Klondike
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Sunday - 09:30-10:59 PDT

Title: Intro to ML Workshop
When: Sunday, Aug 8, 09:30 - 10:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Gavin Klondike
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Sunday - 09:00-10:59 PDT

Title: Intrusion Analysis and Threat Hunting with Suricata
When: Sunday, Aug 8, 09:00 - 10:59 PDT
Where: Packet Hacking Village - Workshops (Virtual)
Speakers: Peter Manev,Josh Stroschein

SpeakerBio: Peter Manev , CSO OF STAMUS NETWORKS
Peter Manev (Twitter: @pevma) is a co-founder of Stamus Networks, where he acts as CSO. He has been an active OISF member for a decade and has a 15 year-long record of activity in the field of IT security. An adamant admirer and explorer of innovative open-source security software, Peter is also the lead developer of SELKS.
Twitter: @pevma

SpeakerBio: Josh Stroschein , DIRECTOR OF IT TRAINING AT OPEN INFORMATION SECURITY FOUNDATION (OISF)
Josh Stroschein (Twitter: @jstrosch) is an experienced malware analyst and reverse engineer and has a passion for sharing his knowledge with others. He is the Director of Training for OISF, where he leads all training activity for the foundation and is also responsible for academic outreach and developing research initiatives. Josh is also an Associate Professor of Cyber Security at Dakota State University where he teaches malware analysis and reverse engineering, an author on Pluralsight, and a threat researcher for Bromium.
Twitter: @jstrosch

Description:
In today’s threat landscape, sophisticated adversaries have routinely demonstrated the ability to compromise enterprise networks and remain hidden for extended periods of time. In Intrusion Analysis and Threat Hunting with open-source Tools, you will learn how to dig deep into network traffic to identify key evidence that a compromise has occurred, learn how to deal with new forms of attack, and develop the skills necessary to proactively search for evidence of new breaches. We will explore key phases of adversary tactics and techniques - from delivery mechanisms to post-infection traffic to get hands-on analysis experience. Open-source tools such as Suricata and Moloch will be utilized to generate data, perform exhaustive traffic analysis, and develop comprehensive threat hunting strategies. By the end of this workshop, you will have the knowledge and skills necessary to discover new threats in your network.

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 16:30-16:59 PDT

Title: IoT devices as government witnesses: Can IoT devices ever be secure if law enforcement has unlimited access to their data?

When: Saturday, Aug 7, 16:30 - 16:59 PDT

Where: IoT Village (Talk - Virtual)

Speakers: Anthony Hendricks,Jordan Sessler

SpeakerBio: Anthony Hendricks

Anthony Hendricks is an attorney who advises clients as the chair of Crowe & Dunlevy's Cybersecurity & Data Privacy Practice Group. In that role, he frequently analyzes and litigates legal issues related to IoT devices. Prior to beginning his practice, he studied as Howard University's first Marshall Scholar and later graduated from Harvard Law School. He now teaches cybersecurity law as an adjunct professor at Oklahoma City University School of Law.

SpeakerBio: Jordan Sessler

Jordan Sessler is an attorney who advises clients on data security as a member of Crowe & Dunlevy's Cybersecurity & Data Privacy Practice Group. In that role, he regularly engages with legal issues related to IoT devices and has represented companies in disputes with law enforcement regarding the discoverability of user- and device-generated data. Prior to beginning his practice, he graduated from Harvard Law School and clerked for U.S. District Court Judge D.P. Marshall Jr.

Description:

A man in Connecticut was arrested after his wife's Fitbit implicated him in her murder. Prosecutors in Arkansas sought to use data from an Amazon Echo as evidence against a murder suspect. Local police sought access to car, TV, and even refrigerator data to monitor Black Lives Matter protestors—and the FBI did the same thing to help track down suspects in the aftermath of the January 6th, 2021 riot at the U.S. Capitol.

These examples are hardly isolated instances—there are thousands of other cases just like them. And they all speak to an important truth: IoT devices are increasingly being used by law enforcement for investigational purposes and, in some cases, even being made into star witnesses at trial. But law enforcement's use of IoT devices raises two important questions. First, does allowing the government to use IoT data violate consumer expectations of privacy, particularly at a time when IoT products are being made and marketed with an eye toward information security? Second, are criminal suspects being provided with the same near-limitless access to IoT data for purposes of mounting their legal defense?

The answers to both of these questions are troubling, in large part because the law is inherently back-ward looking and is thus not equipped to grapple with the raw amount of information is now generated. Just as many consumers did not realize several years that their watch or car audio system would be used by law enforcement to track their location 24/7, so lawmakers and judges did not either. For example, the Federal Privacy Act of 1974 never contemplated that, rather than maintaining records, the government would simply buy access to private records—as ICE recently did by purchasing access to CLEAR—or create its own iOS app to ensnare criminals, as the FBI recently did. Likewise, although the Supreme Court noted the private nature of cell phone location data in Carpenter v. United States, this was a 5-4 decision (while RBG was still on the bench) that only applied the Fourth Amendment to historical cell phone GPS data, effectively leaving the law unsettled on many other types of IoT data. This has led courts, including a New York federal court in a case involving Apple, to express concerns that, even where warrants are involved, allowing the government to force companies to produce IoT device data could "result in a virtually limitless expansion of the government's legal authority to surreptitiously intrude on personal privacy."

These concerns are heightened by the fact that, although the Federal Rules of Criminal Procedure are supposed provide defendants with equal discovery rights, the Stored Communications Act often prevents defendants from accessing the IoT data of others, such as witnesses, accusers, or potential other defendants. In practice, this means that IoT data can effectively be used against criminal suspects but is not available for them to use in arguing their legal defense. This results in an incredible inequality in the criminal justice system. And it may also lead to erroneous outcomes: as with DNA evidence, IoT data may help exonerate criminals just as often as it implicates them. Indeed, in the Arkansas v. Bates murder case, the prosecution dismissed the charges against the defendant shortly after it obtained the Amazon Echo data, which apparently validated the defendant's alibi. Similarly, allegations of cheating against low-income students at Dartmouth Medical School were dismissed after IoT data brought into question potentially erroneous remote test monitoring that may have been skewed by poor internet.

So what can we do to reform or limit government use of IoT data? This talk aims to talk through ways in which both the infosec and legal communities can increase their mutual understanding and help drive reform. In the short term, the infosec community can increase security by minimizing, encrypting, or de-identifying data. This can reduce the amount of information that IoT devices collect and, thus, are required to turn over to law enforcement. Over the long-term, the best solution may be to pass new laws or drive new judicial precedent that incorporates an understanding as to what IoT data is, how it is changing expectations of privacy, and how it is being used by law enforcement. Such laws could either limit access to IoT data—enshrining a greater degree of privacy—or set forth procedures delineating when authorities may use it and guaranteeing defendants equal access. Of course, there are other potential solutions and we hope this talk will help launch a broader discussion on how to help the law interact with IoT technology.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 16:30-17:15 PDT

Title: IoT Testing Crash Course
When: Friday, Aug 6, 16:30 - 17:15 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Tim Jensen (EapolSniper)
Tim has 9 years of professional security experience, largely in network, IoT, and web application penetration testing. He ran a hack lab in Fargo, ND for 4 years where he taught hardware hacking and penetration testing on evenings and weekends. When not hacking, Tim enjoys cycling, walking, and live music.

Description:
In this IoT 101 level talk I provide practical instruction to security focused individuals who want to test IoT devices for critical vulnerabilities. Included will be basic network pentesting of the device, web app or other UI testing, extracting/downloading firmware, and using binwalk. This will also include reviewing binaries for potential backdoors, looking for hardcoded credentials, and whitebox code review of the UI interface to look for backdoors or other vulnerabilities. All testing will be done against publicly downloadable binaries.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 10:00-18:30 PDT

Title: IoT Village Capture the Flag (CTF)
When: Friday, Aug 6, 10:00 - 18:30 PDT
Where: IoT Village (Virtual + Paris Vendome A)

Description:
For more information, see https://www.iotvillage.org/defcon.html

IoT Village virtual events will be streamed to Twitch.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 10:00-18:30 PDT

Title: IoT Village Capture the Flag (CTF)
When: Saturday, Aug 7, 10:00 - 18:30 PDT
Where: IoT Village (Virtual + Paris Vendome A)

Description:

For more information, see https://www.iotvillage.org/defcon.html

IoT Village virtual events will be streamed to Twitch.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Sunday - 10:00-11:59 PDT

Title: IoT Village Capture the Flag (CTF)
When: Sunday, Aug 8, 10:00 - 11:59 PDT
Where: IoT Village (Virtual + Paris Vendome A)

Description:
For more information, see https://www.iotvillage.org/defcon.html

IoT Village virtual events will be streamed to Twitch.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 10:00-18:30 PDT

Title: IoT Village Labs
When: Friday, Aug 6, 10:00 - 18:30 PDT
Where: IoT Village (Virtual + Paris Vendome A)

Description:

For more information, see https://www.iotvillage.org/defcon.html

IoT Village virtual events will be streamed to Twitch.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 10:00-18:30 PDT

Title: IoT Village Labs
When: Saturday, Aug 7, 10:00 - 18:30 PDT
Where: IoT Village (Virtual + Paris Vendome A)

Description:

For more information, see https://www.iotvillage.org/defcon.html

IoT Village virtual events will be streamed to Twitch.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Sunday - 06:00-10:59 PDT

Title: IoT Village Labs
When: Sunday, Aug 8, 06:00 - 10:59 PDT
Where: IoT Village (Virtual + Paris Vendome A)

Description:

For more information, see https://www.iotvillage.org/defcon.html

IoT Village virtual events will be streamed to Twitch.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Friday - 15:30-15:59 PDT

Title: It Takes a Village (and a generous grant): Students Performing ICS Security Assessments
When: Friday, Aug 6, 15:30 - 15:59 PDT
Where: ICS Village (Virtual)
Speakers: Alexander Vigovskiy,Christopher Von Reybyton,Dennis Skarr

SpeakerBio: Alexander Vigovskiy
No BIO available

SpeakerBio: Christopher Von Reybyton
No BIO available

SpeakerBio: Dennis Skarr , Everett Community College
Dennis Skarr is tenured faculty at Everett Community College (EvCC) where he teaches Information Technology. His teaching endeavors resulted in receiving the 2019 Exceptional Faculty Award from EvCC. Dennis is currently building an Industrial Security Program for EvCC that includes classes, workshops, and Capture the Flag competitions.

Dennis has an extensive background in performing security assessments on a variety of industrial control systems. While Dennis was with the National Guard he created a two-week training program for cyber operators to receive special qualifications for missions involving cyber-physical systems. Dennis spent over 10 years performing assessments for the National Guard on critical systems that included building automation systems, electrical utilities, and voting systems. In 2016, Dennis' work at the Guard contributed to US Secretary of Defense Ash Carter visiting his unit for a briefing on their capabilities and achievements.

Twitter: @DennisSkarr

Description:
Everett Community College (EvCC) recently launched a 5 credit class titled "Assessing and Securing Control Systems" utilizing custom-developed ICS trainers by GRIMM. Performing a mock assessment on the nation's first 10 foot ICS wall at a community college, students completed their capstone exercise for the EvCC's first class dedicated to ICS security. This presentation has multiple students sharing their experiences related to why they chose this class, what they gained, and their career goals after the competition.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Sunday - 13:30-13:59 PDT

Title: It takes a village: Why you should join the Biohacking Village
When: Sunday, Aug 8, 13:30 - 13:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Rob Suárez , CISO, BD
Rob Suárez is a cybersecurity and privacy professional in the medical device and healthcare IT industry. At BD, Rob serves as Chief Information Security Officer and oversees cybersecurity across the company’s enterprise, IT and manufacturing systems. Rob currently chairs the Cybersecurity Steering Committee for the Medical Device Innovation Consortium and the Cybersecurity Working Group for AdvaMed. He was also one of three leaders to co-chair the public-private Healthcare and Public Health Sector Coordinating Council (HSCC) Med Tech Cybersecurity Risk Management Task Group, which issued the seminal Medical Device and Healthcare Information Technology Joint Security Plan (JSP) in 2019.

Description:
The Biohacking Village at DEF CON brings medical device manufacturers and security researchers together for one purpose: to strengthen medical device cybersecurity. In this presentation, BD CISO Rob Suárez will share his perspective on crowdsourcing cybersecurity and how creating a community of practice strengthens cybersecurity, promotes ethical coordinated vulnerability disclosure processes, and accelerates the application of emerging best practices across industries. Participants will also hear from Scott Shindledecker, Chief Product Security Officer for BD and Nastassia Tamari, Director of Information Security - Operations for BD, on practical tips for participating in events like the Biohacking Village Medical Device Lab and fostering collaborative relationships with security researchers and fellow medical device manufacturers.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

SEV - Friday - 12:30-13:30 PDT

Title: Judging by the Cover: Profiling & Targeting Through Social Media
When: Friday, Aug 6, 12:30 - 13:30 PDT
Where: Social Engineer Village (Virtual)

SpeakerBio: Christina Lekati
Christina Lekati is a psychologist, a social engineer and an open-source intelligence analyst.

She specializes in behavioral analysis and in intelligence collection and analysis through open source and human intelligence.

Christina has participated among other things in penetration tests, in trainings to companies and organizations, in vulnerability assessments, and in profiling and analysis of the modus operandi, and in the process of identifying personality traits, behavioral tendencies, and other variables of victims and offenders.

Christina is working with Cyber Risk GmbH as a social engineering specialist and an open source intelligence investigator for the vulnerability assessments conducted on corporations and high-value targets. She is the main developer of the social engineering training programs provided by Cyber Risk GmbH. Those programs are intertwining the lessons learned from real life cases and previous experiences with the fields of cybersecurity, psychology, and counterintelligence.

She is also an active Advisory Board Member at the OSINT Curious project.

Description:

While to the rest of the world social media are friendly platforms of communication and sharing, for the fellow social engineers and OSINT analysts, they are targeting and information harvesting platforms. Even though social media do not always demonstrate our true personalities, they do demonstrate the way we want to be viewed and treated by others – which can be a lot more useful for social engineers. They also “leak” behavioral tendencies and characteristics that provide significant intelligence for any type of operation targeting humans.

The talk covers the topic of information gathering through social media intelligence (SOCMINT), and explains how even seemingly innocent information can be used to manipulate or influence targets. Case studies will be provided.

It will also discuss the art & science of profiling, along with its limitations for social engineering engagements. A two-part demonstration is included on how a profiler’s mind works when harvesting information on social media:

The first part includes real examples of posts that expose vulnerabilities, attract attackers and ultimately can be exploited and lead to security breaches. The second part dives deeper and demonstrates how the information found on a social media profile (from their pictures to the words used by the individual) are gathered, categorized into a profiling matrix and then analyzed, bringing into the surface a personality profile. The target’s profile can then provide actionable intelligence that increases the success of attacks, or attack simulations.

Social Engineer Village will stream content to Twitch.

Twitch: https://www.twitch.tv/socialengineerllc

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Saturday - 12:00-12:30 PDT

Title: Keeping Your Information Security Policy Up to Date
When: Saturday, Aug 7, 12:00 - 12:30 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Sang-Oun Lee
Sang-Oun Lee is an IT Security Specialist-Compliance at the City of Chicago. Prior to his current position at the City, Mr. Lee served as a cybersecurity policy expert in both public and private sectors. In the public sector, Mr. Lee served two government agencies in the Republic of Korea, Korea Internet & Security Agency and National Security Research Institute respectively. In the private sector, Mr. Lee was a Chief Information & Financial Officer at EPIKAR Inc., a mobility start-up company based in Seoul, Korea. Mr. Lee holds Master of Public Policy from the University of Chicago, Master of Science in Engineering from Seoul National University, Seoul, Korea, and Bachelor's degree from Waseda University, Tokyo, Japan.

Description:

Information security policy (ISP) is the highest directive of the cybersecurity posture of an organization. ISPs play a role by providing a subset of administrative, operational, and technical controls to mitigate omnidirectional cyber risks. Local government, which provides a wide range of public services with various functions, is a double-edged sword.

On the one hand, its public impact on every activity is wide enough to influence a far broader audience with multiple interests. On the other hand, this wider audience than private organizations allows salient cyberattacks such as influence operations with social media, conveyance of wrongful policy information, a breach in personal health information (PHI) and privacy, and so forth - protecting a local government is both protection of an organization and its residents.

This presentation suggests a method to revise existing ISP to make contributions for ISP staying up-to-date, align to the latest industry standards and regulations to be compliant, and narrowing down newly identified gaps from the local government perspective.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Friday - 11:00-11:50 PDT

Title: Key Duplication - It's not just for the movies!
When: Friday, Aug 6, 11:00 - 11:50 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio: Tony Virelli
No BIO available

Description:

Have you ever seen someone just walking around with a key hanging on their belt? How about a wall of keys behind a security desk? Better yet, has anyone you know every posted a picture of the keys to the new home they just bought? Well, what if you could take a picture and easily duplicate that key with a 3D Printer? Sound like something from a James Bond film? Well it's not! Better yet, if you can just get a moment alone with a key, you can get an imprint of it in less than 2 minutes, return the key to the owner and then cast a duplicate of that key for later use.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Saturday - 10:15-11:30 PDT

Title: Key Note – The Three Amigos: Money Laundering, Cryptocurrencies, and Smart Contracts
When: Saturday, Aug 7, 10:15 - 11:30 PDT
Where: Blockchain Village / Paris Vendome B
Speakers: Daniel Garrie,David Cass

SpeakerBio: Daniel Garrie , Esq. (Law & Forensics)
No BIO available

SpeakerBio: David Cass , Federal Reserve
No BIO available

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Friday - 10:00-10:59 PDT

Title: Keynote - PW Singer
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: ICS Village (Virtual)

SpeakerBio:PW Singer
No BIO available

Description: No Description available

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Friday - 13:30-13:59 PDT

Title: Kickoff Remarks (recorded in-person in Las Vegas)
When: Friday, Aug 6, 13:30 - 13:59 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Harri Hursti
Co-Founder, DEF CON Voting Village; Founding Partner, Nordic Innovation Labs

Harri Hursti is considered one of the world’s foremost experts on the topic of electronic voting security, having served in all aspects of the industry sector. He is considered an authority on uncovering critical problems in electronic voting systems worldwide.

As a consultant, he has conducted and co-authored many studies, both academic and commercial, on various election systems’ data security and vulnerability. These studies have come at the request of officials, legislators and policy makers in 5 countries; including the U.S. government, at both the state and federal level.

Description:

Recorded live in Las Vegas this morning and rebroadcast.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 12:50-13:20 PDT

Title: Kubernetes Goat - Kubernetes Security Learning (Tool Demo)
When: Friday, Aug 6, 12:50 - 13:20 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Madhu Akula
Madhu Akula is the creator of Kubernetes Goat, an intentionally vulnerable by design Kubernetes Cluster to learn and practice Kubernetes Security. Also published author and Cloud Native security researcher with extensive experience. Also, he is an active member of the international security, DevOps, and Cloud Native communities (null, DevSecOps, AllDayDevOps, etc). Holds industry certifications like OSCP (Offensive Security Certified Professional), CKA (Certified Kubernetes Administrator), etc. Madhu frequently speaks and runs training sessions at security events and conferences around the world including DEFCON (24, 26 & 27), BlackHat USA (2018 & 19), USENIX LISA (2018 & 19), O'Reilly Velocity EU 2019, GitHub Satellite 2020, Appsec EU (2018 & 19), All Day DevOps (2016, 17, 18, 19 & 20), DevSecCon (London, Singapore, Boston), DevOpsDays India, c0c0n(2017, 18), Nullcon (2018, 19), SACON 2019, Serverless Summit, null and multiple others. His research has identified vulnerabilities in over 200+ companies and organizations including; Google, Microsoft, LinkedIn, eBay, AT&T, WordPress, NTOP and Adobe, etc, and credited with multiple CVE's, Acknowledgements, and rewards. He is co-author of Security Automation with Ansible2 (ISBN-13: 978-1788394512), which is listed as a technical resource by Red Hat Ansible. Also, technical reviewer of Learn Kubernetes Security book published by Packt. Also won 1st prize for building Infrastructure Security Monitoring solution at InMobi flagship hackathon among 100+ engineering teams.
Twitter: @madhuakula

Description:

Kubernetes Goat is "vulnerable by design" Kubernetes Cluster environment to practice and learn about Kubernetes Security. In this session, Madhu Akula will present how to get started with Kubernetes Goat by exploring different vulnerabilities in Kubernetes Cluster and Containerized environments. Also, he demonstrates the real-world vulnerabilities and maps the Kubernetes Goat scenarios with them. We will see the complete documentation and instruction to practice Kubernetes Security for performing security assessments. As a defender you will see how we can learn these attacks, misconfigurations to understand and improve your cloud native infrastructure security posture.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

Title: Kubernetes Goat
When: Saturday, Aug 7, 10:00 - 11:50 PDT
Where: DemoLab Video Channel 1

SpeakerBio: Madhu Akula
Madhu Akula is the creator of Kubernetes Goat, an intentionally vulnerable by design Kubernetes Cluster to learn and practice Kubernetes Security. Also published author and Cloud Native security researcher with extensive experience. Also, he is an active member of the international security, DevOps, and Cloud Native communities (null, DevSecOps, AllDayDevOps, etc). Holds industry certifications like OSCP (Offensive Security Certified Professional), CKA (Certified Kubernetes Administrator), etc. Madhu frequently speaks and runs training sessions at security events and conferences around the world including DEFCON (24, 26 & 27), BlackHat USA (2018 & 19), USENIX LISA (2018 & 19), O'Reilly Velocity EU 2019, GitHub Satellite 2020, Appsec EU (2018 & 19), All Day DevOps (2016, 17, 18, 19 & 20), DevSecCon (London, Singapore, Boston), DevOpsDays India, c0c0n(2017, 18), Nullcon (2018, 19), SACON 2019, Serverless Summit, null and multiple others. His research has identified vulnerabilities in over 200+ companies and organizations including; Google, Microsoft, LinkedIn, eBay, AT&T, WordPress, NTOP and Adobe, etc, and credited with multiple CVE's, Acknowledgements, and rewards. He is co-author of Security Automation with Ansible2 (ISBN-13: 978-1788394512), which is listed as a technical resource by Red Hat Ansible. Also, technical reviewer of Learn Kubernetes Security book published by Packt. Also won 1st prize for building Infrastructure Security Monitoring solution at InMobi flagship hackathon among 100+ engineering teams.
Twitter: @madhuakula

Description:
Tool or Project Name: Kubernetes Goat

Short Abstract:
Kubernetes Goat is “vulnerable by design” Kubernetes Cluster environment to practice and learn about Kubernetes Security. It has step by step detailed guide and digital book on how to get started with Kubernetes Goat by exploring different vulnerabilities in Kubernetes Cluster and Containerized environments. Also, it has scenarios taken from the real-world vulnerabilities and maps the Kubernetes Goat scenarios. The complete documentation and instruction to practice Kubernetes Security for performing security assessments, pentesting, and in general Kubernetes Security. As a defender you will see how we can learn these attacks, misconfigurations to understand and improve your cloud native infrastructure security posture.

Short Developer Bio:
Madhu Akula is the creator of Kubernetes Goat, an intentionally vulnerable by design Kubernetes Cluster to learn and practice Kubernetes Security. Also published author and Cloud Native security architect with extensive experience. Also, he is an active member of the international security, DevOps, and Cloud Native communities (null, DevSecOps, AllDayDevOps, etc). Holds industry certifications like OSCP (Offensive Security Certified Professional), CKA (Certified Kubernetes Administrator), etc.

Madhu frequently speaks and runs training sessions at security events and conferences around the world including DEF CON (24, 26, 27, 28), Black Hat USA (2018, 19, 21), USENIX LISA (2018, 19, 21), O’Reilly Velocity EU 2019, GitHub Satellite 2020, Appsec EU (2018 & 19), All Day DevOps (2016, 17, 18, 19 & 20), DevSecCon (London, Singapore, Boston), DevOpsDays India, c0c0n(2017, 18, 20), Nullcon (2018, 19, 21), SACON 2019, Serverless Summit, null and multiple others.

His research has identified vulnerabilities in over 200+ companies and organizations including; Google, Microsoft, LinkedIn, eBay, AT&T, WordPress, NTOP and Adobe, etc, and credited with multiple CVE’s, Acknowledgements, and rewards. He is co-author of Security Automation with Ansible2 (ISBN-13: 978-1788394512), which is listed as a technical resource by Red Hat Ansible. Also, technical reviewer of Learn Kubernetes Security book published by Packt. Won 1st prize for building Infrastructure Security Monitoring solution at InMobi flagship hackathon among 100+ engineering teams

URL to any additional information:
https://github.com/madhuakula/kubernetes-goat https://madhuakula.com/kubernetes-goat

Detailed Explanation of Tool:
Kubernetes Goat is designed to be an intentionally vulnerable cluster environment to learn and practice Kubernetes security. Some of the high-level scenarios include, but not limited to below: Sensitive keys in code bases
DIND (docker-in-docker) exploitation
SSRF in K8S world
Container escape to access host system
Docker CIS Benchmarks analysis
Kubernetes CIS Benchmarks analysis
Attacking private registry
NodePort exposed services
Helm v2 tiller to PwN the cluster
Analysing crypto miner container
Kubernetes Namespaces bypass
Gaining environment information
DoS the memory/cpu resources
Hacker Container preview
Hidden in layers
Supporting Files, Code, etc:
https://github.com/madhuakula/kubernetes-goat https://madhuakula.com/kubernetes-goat/

Target Audience:
Offense, Defense

The adoption of Kubernetes use in production has increased to 83% from a survey by CNCF. Still, most of the security teams struggle to understand these modern technologies. So this project helps and brings a completely new area of research to share with the community to learn and practice from years of experience.

This content will be presented on a Discord video channel.

#dl-video1-voice: https://discord.com/channels/708208267699945503/734027693250576505

Return to Index - Add to Google Calendar - ics Calendar file

Title: Kubernetes Security 101: Best Practices to Secure your Cluster (Workshop)
When: Friday, Aug 6, 14:35 - 16:59 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Magno Logan
Magno Logan works as an Information Security Specialist for Trend Micro. He specializes in Cloud, Container and Application Security Research, Threat Modelling and Red Teaming. He has been tapped as a resource speaker for numerous security conferences around the globe. He is the founder of the JampaSec Security Conference and the OWASP Paraiba Chapter and also an active member of the CNCF TAG-Security team.
Twitter: @magnologan

Description:

This workshop aims to give an overview about how Kubernetes works and provide some best practices to secure your cluster whenever you are deploying a new cluster on your own or via managed services such as GKE, EKS or AKS. We are going to cover everything from the Control Plane or the Master Node, starting with the API server, including etcd, RBAC and network policies. Then, we’ll cover the worker nodes, kubelet, audit logs and pods best practices. We'll talk about the CIS Benchmarks for Kubernetes and the default configurations you need to worry about when deploying a new cluster. We'll show how to use RBAC and assign roles and permissions to your cluster users. We'll demonstrate how to enable audit logs for better visibility and later we'll set up some network policies to avoid communication between pods and prevent any lateral movement from attackers. Are you starting to use Kubernetes for container orchestration? Do you need guidelines on how to start securing Kubernetes in your organization? Do you want to find a way to increase the protection of your Kubernetes clusters without increasing the complexity of the infrastructure? Do you need to use Kubernetes clusters in a safe, efficient and affordable way? Everything in a practical way with a focus on security best practices? Then this is the workshop for you! Outline:

- Kubernetes
    - ♦ What is Kubernetes?
    - ♦ Why should I use it?
    - ♦ What is the CNCF?
    - ♦ What are cloud native applications?
- K8s Architecture
    - ♦ Control Plane (API Server, etcd, scheduler, controller-manager)
    - ♦ Worker Nodes (kubelet, kube-proxy and CRE)
- Cluster, Nodes, Pods and Namespaces
- K8s API Objects
- kubectl
- Setting up your first cluster
- Deploying your web app as a pod
- Using services and load balancers
- Hardening K8s
    - ♦ API Server
    - ♦ Image Scanning
    - ♦ Runtime Protection
    - ♦ Network Policy
    - ♦ Pod Security Policy (PSP) - Deprecated
    - ♦ PSP Alternatives
    - ♦ Audit Logs

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Title: Kubestriker
When: Friday, Aug 6, 14:00 - 15:50 PDT
Where: DemoLab Video Channel 1

SpeakerBio: Vasant Chinnipilli
Vasant is a security enthusiast and speaker, currently working as a Security Architect and DevSecOps Practitioner.

His technical abilities span a wide range of technologies across various domains of information security including cloud and container security and penetration testing. He is passionate about cloud and cloud native security, devsecops and security automation.

Description:

Tool Name: Kubestriker - a blazing fast security auditing tool for kubernetes

Short Abstract:
Kubestriker is a platform-agnostic tool designed to tackle Kuberenetes cluster security issues due to misconfigurations and will help strengthen the overall IT infrastructure of any organization.

It performs numerous in depth checks on a range of services and open ports on Kubernetes platform to identify any misconfigurations which make organisations an easy target for attackers. In addition, it helps safeguard against potential attacks on Kubernetes clusters by continuously scanning, monitoring and alerting of any anomalies.

Furthermore, it comprises the ability to see some components of kubernetes infrastructure and provides visualised attack paths of how hackers can advance their attacks.

Short Developer Bio:
Vasant is a security enthusiast and speaker, currently working as a Security Architect and DevSecOps Practitioner. His technical abilities span a wide range of technologies across various domains of information security including cloud and container security and penetration testing. He is passionate about cloud and cloud native security, devsecops and security automation.

URL to any additional information:
https://github.com/vchinnipilli/kubestriker

Detailed Explanation of Tool:
The tool is open source and platform-agnostic making it compatible with various platforms such as self-hosted kubernetes, Amazon EKS, Azure AKS and Google GKE.

Current capabilities include performing in-depth reconnaissance and automated enumeration for a range of services and open ports. It also scans for a wide range of IAM misconfigurations, misconfigured containers and misconfigured pod security and network policies. It can also assess the excessive privileges of subjects in the cluster and generate an elaborative report with detailed explanation of the findings.

It also incorporates security for containers running in the cluster by continuously discovering, tracking, scanning, and reporting them, along with the ability to see some of the components of kubernetes infrastructure and provide visualised attack paths of how hackers can advance their attacks by chaining different misconfigured components in the kubernetes cluster.

Target Audience:
Offensive and Defensive Security Professionals Security Auditors
Developers, Devops, Sysadmins, Devsecops and SRE professionals The aim of the presentation is to demonstrate the kind of

attacks that are possible due to misconfigurations. In particular, through the use of Kubestriker, I will demonstrate how misconfigured cluster privileges can compromise the kubernetes platform and its underlying infrastructure, along with showing backdooring cloud environments, avoid detection by manipulating logging controls and access sensitive information and trade secrets due to IAM, pod security policy and webhook misconfigurations.

This content will be presented on a Discord video channel.

#dl-video1-voice: https://discord.com/channels/708208267699945503/734027693250576505

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Friday - 17:00-17:45 PDT

Title: Law School for Lockpickers
When: Friday, Aug 6, 17:00 - 17:45 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio: Preston Thomas
No BIO available

Description:
No, Virginia, lockpicks aren't "illegal". Like lockpicking itself, the law of lockpicking is esoteric, widely misunderstood, and occasionally a source of hilarity when interpreted by outsiders. Class is in session as practicing attorney and former TOOOL Board member Preston Thomas hosts a lighthearted law school for locksporters, laying out the legal logic, busting myths, and telling stories. Expect raucous Q&A, real talk, and absolutely zero legal advice.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 18:00-19:59 PDT

Title: Lawyers Meet
When: Friday, Aug 6, 18:00 - 19:59 PDT
Where: Bally's Pool Cabana

Description:

If you're a lawyer (recently unfrozen or otherwise), a judge or a law student please make a note to join Jeff McNamara at 18:00 on Friday in a poolside cabana, look for the sign, for a friendly get-together, drinks, and conversation.

Return to Index - Add to Google Calendar - ics Calendar file

WS - Friday - 15:00-18:59 PDT

Title: Learning to Hack Bluetooth Low Energy with BLE CTF
When: Friday, Aug 6, 15:00 - 18:59 PDT
Where: Workshops - Las Vegas 3+4 (Onsite Only)

SpeakerBio: Ryan Holeman , Global Security Overlord
Ryan Holeman resides in Austin Texas where he works as the Global Security Overlord on Atlassian's Security team. He is also an advisor for the endpoint security software company Ziften Technologies. He received a Masters of Science in Software Engineering from Kent State University. His graduate research and masters thesis focused on C++ template metaprograming. He has spoken at many respected venues such as Black Hat, DEF CON, Lockdown, BSides, Ruxcon, Notacon, and Shmoocon. He has also published papers though venues such as ICSM and ICPC . You can keep up with his current activity, open source contributions and general news on his blog. His spare time is mostly spent digging into various network protocols, random hacking, creating art, and shredding local skateparks.

Description:

BLE CTF is a series of Bluetooth low energy challenges in a capture the flag format. It was created to teach the fundamentals of interacting with and hacking Bluetooth Low Energy services. Each exercise, or flag, aims to interactively teach a new concept to the user. For this workshop, we will step through a series of exercises to teach beginner students new concepts and allow more seasoned users to try new tools and techniques. After completing this workshop, you should have a good solid understanding of how to interact with and hack on BLE devices in the wild.

If you have done BLE CTF in the past, this class is still valuable. For advanced users we offer BLE CTF Infinity which is a sequel to BLE CTF. BLE CTF Infinity offers new exercises where each flag challenge is hosted in a completely separate GATT service. The new version allows for more advanced challenges which were not possible in the past.

To prepare for the workshop, please follow the setup documentation located at
https://github.com/hackgnar/ble_ctf/blob/master/docs/workshop_setup.md

Registration Link:
https://www.eventbrite.com/e/learning-to-hack-bluetooth-low-energy-with-ble-ctf-las-vegas-3-4-tickets-162217343441

Prerequisites

> To prepare for the workshop, please follow the setup documentation located at
> https://github.com/hackgnar/ble_ctf/blob/master/docs/workshop_setup.md

Materials needed:
Preferably a Linux box with a bluetooth controller or a bluetooth usb dongle. An OSX or Windows machine with a Linux VM and usb passthough works as well but should be setup and tested before the workshop.

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 12:45-13:15 PDT

Title: LED Light Lunacy!
When: Friday, Aug 6, 12:45 - 13:15 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Victor Hanna
Security Researcher at SpiderLabs

Description:
All your LEDs are mine ... How a case of lockdown boredom turned into led lights for everyone !

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 10:00-15:59 PDT

Title: Lego Spike Hub
When: Friday, Aug 6, 10:00 - 15:59 PDT
Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:

Participants will be given the opportunity to program a Lego Spike Hub to perform a space mission of transporting and sorting valuable minerals. The workshop is intended to be an introductory workshop to give participants an appreciation for the operation of autonomous space vehicles and an understanding of finite state machines and hardware limitations. There will be 4 prebuilt Lego robots, 2 will be for tracing a line while the other 2 will be for color sorting. The scenario presented to the participant is that they are on a foreign planet and need to transport minerals along a predefined path to safely arrive at the sorting facility and as such will program in Scratch code code for the transport shuttle to execute. Participants will also have a chance to program in Scratch the code to execute on the color sorting robot, thus demonstrating the ability to correctly sort the minerals in appropriate colors.

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 10:00-15:59 PDT

Title: Lego Spike Hub
When: Saturday, Aug 7, 10:00 - 15:59 PDT
Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:

Participants will be given the opportunity to program a Lego Spike Hub to perform a space mission of transporting and sorting valuable minerals. The workshop is intended to be an introductory workshop to give participants an appreciation for the operation of autonomous space vehicles and an understanding of finite state machines and hardware limitations. There will be 4 prebuilt Lego robots, 2 will be for tracing a line while the other 2 will be for color sorting. The scenario presented to the participant is that they are on a foreign planet and need to transport minerals along a predefined path to safely arrive at the sorting facility and as such will program in Scratch code code for the transport shuttle to execute. Participants will also have a chance to program in Scratch the code to execute on the color sorting robot, thus demonstrating the ability to correctly sort the minerals in appropriate colors.

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Sunday - 10:00-10:55 PDT

Title: Less Jaw Work, More Paw Work: Why We Need to Start “Doing” Cyber
When: Sunday, Aug 8, 10:00 - 10:55 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: Cliff Neve
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Saturday - 12:00-12:45 PDT

Title: Let the bugs come to me - how to build cloud-based recon automation at scale
When: Saturday, Aug 7, 12:00 - 12:45 PDT
Where: Recon Village (Virtual)

SpeakerBio: Ryan Elkins
No BIO available
Twitter: @ryanelkins

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Friday - 17:00-17:30 PDT

Title: Lets Get Real About The Future State of Healthcare
When: Friday, Aug 6, 17:00 - 17:30 PDT
Where: Biohacking Village (Talk - Virtual)
Speakers: Christian Dameff,Jeff 'R3plicant' Tully

SpeakerBio: Christian Dameff , Medical Director of Cybersecurity at UCSD
No BIO available

SpeakerBio: Jeff 'R3plicant' Tully
No BIO available

Description:
Taking the lessons of COVID-19 and the healthcare response, how can we create an improved state of resilience in healthcare?

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 13:45-14:15 PDT

Title: Leveraging NGFWs for Threat Hunting
When: Saturday, Aug 7, 13:45 - 14:15 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Drimacus
Drimacus is a veteran in the security focusing around Network Security, Emerging Threats, and Innovation.

Description:

Sharing research and details around running passive NGFWs to complement threat hunting tools. This talk will walk through sharing why, how, and what I learned about these to share with the community and the value that can be gained by leveraging NGFWs for threat hunting.

With the introduction of NGFWs came new operational risk in the form of application ID. After taking a path down to mitigate this risk by implementing passive NGFWs, it also become an opportunity to leverage them for threat hunting.

This talk will review research over the past 5 years of running such passive NGFWs. The pros/cons of the environment over exiting threat hunting tools, review of architecture, and a deep dive into the various functionality will be discussed.

Talk presented by - Shawn Wallis (Drimacus) - Cyber Security Research Strategiest

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Saturday - 14:30-14:59 PDT

Title: Leveraging SBOMs to Enhance ICS Security
When: Saturday, Aug 7, 14:30 - 14:59 PDT
Where: ICS Village (Virtual)

SpeakerBio: Thomas Pace , NetRise
Thomas is currently the co-founder and CEO of NetRise, a cybersecurity company focusing on securing firmware across a heterogenous device set. Prior to NetRise, Thomas served as the Global Vice President of Enterprise Solutions at Cylance where his responsibilities ranged from conducting incident response investigations, product marketing, public speaking and analyst relations. Thomas was also responsible for ICS security at the DOE for 3 years and served in the United States Marine Corps serving in both Iraq and Afghanistan. Thomas has spoken at Black Hat, RSA, and was interviewed on 60 Minutes for his efforts related to ransomware."
Twitter: @tommypastry

Description:
In this talk Tom Pace will discuss how SBOMs (Software Bill of Materials) can be leveraged to enhance ICS security. The recent executive order and guidance from the NTIA have reignited the SBOM discussion and its importance, especially to critical assets such as ICS devices. Tom will explain what an SBOM is, how they can be generated and consumed as well as the vale of the data once an SBOM has been generated. This will include but not be limited to use cases such as known vulnerabilities, integrity verification, provenance and license compliance. Tom will further explain the value an SBOM can have to various stakeholders, from ICS device manufacturers to end-users of the devices themselves. Tom will highlight how significant time savings can be realized once SBOMs are in place, while at the same time provide commentary on the challenges of generating an SBOM especially for devices deemed "legacy" or out of support.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 18:15-18:45 PDT

Title: Lightning talk: Autonomous lateral movement
When: Saturday, Aug 7, 18:15 - 18:45 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Stephan Wampouille , Cyber Security Engineer (Intern), Prelude Research
Stephan is a Cyber Security Engineering intern at Prelude Research, where he uses his mechanical engineering background to construct realistic adversary profiles which are runnable within the Prelude Operator application or on their own. Stephan works on attacks which are designed to bypass detection through creative measures.
https://www.linkedin.com/in/stephan-wampouille

Description:

See autonomous lateral movement in a live environment. In this Linux-based attack, multiple benign behaviors - each designed not to be detected - are chained together to complete a lateral movement action. Using a creative approach to parsing indicators of compromise out of RAT responses and injecting them automatically into commands later down the kill chain, this lateral movement demonstration will be fully hands-off. The techniques and TTPs in this demonstration will be made open-source following the talk.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Friday - 14:45-14:59 PDT

Title: Lightning Talk: Differential Privacy and Census Data
When: Friday, Aug 6, 14:45 - 14:59 PDT
Where: Crypto & Privacy Village (Virtual)

SpeakerBio: Wendy Edwards
Wendy is a software developer interested in the intersection of cybersecurity and data science. She's involved in the NASA Datanauts program and participated in the SANS Women's Academy, earning GIAC GSEC, GCIH, and GCIA certifications. She has masters degrees in computer science and library and information science from the University of Illinois. She has spoken at Summercon, BSides Chicago, The Diana Initiative, Hackfest Canada, Circle City Con, and DEFCON Ethics Village. In her spare time, she enjoys Scrabble and swimming and has a lively flat-coated retriever named Ciaran.
Twitter: @wayward710

Description:
The U.S. Constitution requires that a Census be conducted every 10 years. In addition to counting populations, the Census also collects personal data that's legally required to be kept private. This presents a growing challenge: how can the Census provide accurate statistical data without revealing information that would allow others to piece together someone's data? For example, what if you had a very small census block with only one member of a particular ethnicity? Without any privacy measures, it might be possible to figure out who the person was. Big data also increases privacy risks. What if it was possible to deidentify Census data and then combine it with social media big data?

The Census Bureau has developed a Disclosure Avoidance System that uses differential privacy to introduce noise into results. Essentially, the goal of differential privacy is to give each person the same amount of privacy they would have if their data was removed. Differential privacy has a number of implications for redistricting; for example, it may make gerrymandering more difficult since fine-grained data is obscured.

This talk will discuss Census privacy challenges, and provide an overview of differential privacy.

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Saturday - 11:00-11:59 PDT

Title: Linux Binary Analysis w/ Strace
When: Saturday, Aug 7, 11:00 - 11:59 PDT
Where: Packet Hacking Village - Talks (Virtual)

SpeakerBio: Jared Stroud , LACEWORK
Jared Stroud (Twitter: @DLL_Cool_J) is a Cloud Security Researcher at Lacework where he focuses on emerging Linux and Cloud platform threats. Previously, he worked at The MITRE Corporation where he contributed Unix and Windows tooling for the ATT&CK Fin7/CARBANAK Evaluation and the Open Source adversary emulation utility CALDERA.
Twitter: @DLL_Cool_J

Description:

The strace utility allows for deep insight into what an application is doing on a nix host. While the amount of data produced can be overwhelming, in this video I'll demonstrate how to filter, log and obtain relevant information for a wide variety of use cases around file analysis. From diagnosing a bisheaving application, to revealing a malware's secrets. This video will give a practical introduction in using strace to spy on *nix applications at the syscall level. All resources can be found here: https://www.github.com/lacework-dev/strace_lab_PUBLIC

All Packet Hacking Village talks will stream on YouTube, Twitch, Facebook, and Periscope.

YouTube: https://youtube.com/wallofsheep

Twitch: https://twitch.tv/wallofsheep

Facebook: https://www.facebook.com/wallofsheep/

Periscope: https://www.periscope.tv/wallofsheep

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 13:00-13:45 PDT

Title: Look at me, I'm the Adversary now: Introduction to Adversary Emulation and its place in Security Operations
When: Friday, Aug 6, 13:00 - 13:45 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Samuel Kimmons
Samuel Kimmons is Red Teamer at Cognizant. He is responsible for researching, planning, and developing full scope Red Team engagements. Samuel got is start in Information Security during his time in the United States Air Force (USAF). While in the USAF he stood up the first interal red team at the United States Air Force Computer Emergency Response Team (AFCERT). His team's primary purpose was to emulate threat actors in order to increase the accuracy of detection capabilities.
https://www.linkedin.com/in/kimmons

Description:
Adversary Emulation is quickly becoming a hot topic in information security, and there is a good reason for it. Security analysts, threat hunters, and incident responders are constantly facing an onslaught of old and new threats. How can defenders properly prepare for the ever-changing threat landscape, improve their skill set, and improve the security posture of their organization? In this presentation I'll answer those questions by covering: The various forms of Adversary Emulation, where/how it fits into Security Operations, Threat Intelligence, the benefits of using it as a Blue Team training tool, and how to get started!

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 12:30-13:20 PDT

Title: Lost In Space: No-one Can Hear Your Breach (Choose Wisely)
When: Saturday, Aug 7, 12:30 - 13:20 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Elizabeth Wharton
Liz, a cybersecurity-focused business and public policy attorney, has advised researchers, startups, and policymakers at the federal, state, and local level. Currently SCYTHE's Chief of Staff, she was the World's (second) Busiest Airport's technology attorney and hosts the CISO Stressed podcast.

Description:
Navigating the space race is difficult enough with privately sponsored flights, internationally owned stations, and interplanetary destinations. Supply-chain vulnerabilities, ransomware threats, and other cybersecurity challenges are magnified when the galactic rules are still being written. Join an interactive adventure dodging malicious attackers, signal and software glitches, and potential liabilities trekking to Mars, highlighting cybersecurity pitfalls and pending policy issues.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=TEUgTF5zDHA

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part 2
When: Saturday, Aug 7, 14:00 - 17:59 PDT
Where: Blue Team Village - Workshop Track 1 (Virtual)
Speakers: Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges

SpeakerBio: Cat Self , Lead Cyber Adversarial Engineer – The MITRE Corporation
Cat Self is a Lead Cyber Adversarial Engineer working on MITRE ATT&CK· and ATT&CK Evaluations teams at MITRE. Cat previously worked at Target as a red team operator, threat hunter, and developer. Cat is an Army Military Intelligence veteran with a passion for mentorship, hiking in foreign lands, and finding opportunities to give back.

SpeakerBio:plug
Plug started his journey in computer security back in 1996 when he discovered a 2600 magazine that eventually lead him to his first LA2600 meeting in 1998. From that point forward, he has been involved in computer security. Plug currently leads the Threat Hunting Program for a Fortune 20 organization. In his free time he enjoys building Legos, playing with synthesizers, and when possible, he volunteers his time to computer security events.

SpeakerBio: Ben Bornholm
Ben (@CptOfEvilMinion) is not new to creating workshops as this is his second time creating a DEFCON workshop, yet he has never actually been to DEFCON in person! Ben crafted his whimsical presenting style from being President of RIT's security club previously known as RC3.

During the day Ben fights off cyber criminals as a DART engineer at Dropbox.com. At night Ben is the author of his blog HoldMyBeerSecurity.com where he discusses topics in security that interest him such as incident response, threat hunting, Osquery, and DevSecOps.

Twitter: @CptOfEvilMinion

SpeakerBio: Tilottama Sanyal
Tilottama Sanyal (wildphish) has a degree in Information technology from India and has almost 8 years of combined experience across DevOps and Cybersecurity. She holds certifications like the GCIH and currently works as an Incident Response Team member at Verizon Media (Yahoo!). Her areas of expertise include risk assessments, vulnerability analysis, and incident response. Her current interests include threat hunting and this is her first-ever workshop.
Twitter: @wildphish

SpeakerBio: Dan Borges
A core member of the National CCDC red team and a director for the Global CPTC. Recently wrote a book on deception applied to infosec and attack-defense competitions: https://ahhh.github.io/Cybersecurity-Tradecraft/

Description:
The Hunt for Red Apples workshop guides participants through emulation walkthroughs, hunting playbooks, & hunting exercises around an Ocean Lotus intrusion, an established threat actor targeting macOS. The workshop is broken into sections using both the attack lifecycle & Mitre ATT&CK knowledge base.

For each phase in the attack live cycle participants learn about one particular tactic, relevant macOS data sources, how to build a hunting plan, practice hunting, & how the red team emulated the tactic using open source intelligence.

This workshop is a resource on how to threat hunt, emulate, & use open source threat intelligence on a specific threat actor.

The Hunt for Red Apples workshop guides participants through emulation walkthroughs, hunting playbooks, and hunting exercises around an Ocean Lotus intrusion, an established threat actor targeting macOS. The workshop is broken into sections using both the attack lifecycle and Mitre ATT&CK knowledge base. For each phase in the attack live cycle participants learn about one particular tactic, relevant macOS data sources, how to build a hunting plan, practice hunting, and how the red team emulated the tactic using open source intelligence.

The objective of this workshop is to provide a balanced approach that showcases both hunting and adversary actions. This workshop is a resource on how to threat hunt, emulate, and use open source threat intelligence on a specific threat actor.

The Hunt for Red Apples workshop is broken into two four hour sessions over two days. As a bonus, we are releasing a second data set for a different scenario on day two for more advanced hunters with no playbooks or walkthroughs. Participants will get to test their macOS Threat Hunting skills! And it's all FREE!

Return to Index - Add to Google Calendar - ics Calendar file

Title: MacOs Workshop - Hunt for Red Apples: Ocean Lotus Edition Part1
When: Friday, Aug 6, 14:00 - 17:59 PDT
Where: Blue Team Village - Workshop Track 1 (Virtual)
Speakers: Cat Self,plug,Ben Bornholm,Tilottama Sanyal,Dan Borges

SpeakerBio: Cat Self , Lead Cyber Adversarial Engineer – The MITRE Corporation
Cat Self is a Lead Cyber Adversarial Engineer working on MITRE ATT&CK· and ATT&CK Evaluations teams at MITRE. Cat previously worked at Target as a red team operator, threat hunter, and developer. Cat is an Army Military Intelligence veteran with a passion for mentorship, hiking in foreign lands, and finding opportunities to give back.

SpeakerBio:plug
Plug started his journey in computer security back in 1996 when he discovered a 2600 magazine that eventually lead him to his first LA2600 meeting in 1998. From that point forward, he has been involved in computer security. Plug currently leads the Threat Hunting Program for a Fortune 20 organization. In his free time he enjoys building Legos, playing with synthesizers, and when possible, he volunteers his time to computer security events.

SpeakerBio: Ben Bornholm
Ben (@CptOfEvilMinion) is not new to creating workshops as this is his second time creating a DEFCON workshop, yet he has never actually been to DEFCON in person! Ben crafted his whimsical presenting style from being President of RIT's security club previously known as RC3.

During the day Ben fights off cyber criminals as a DART engineer at Dropbox.com. At night Ben is the author of his blog HoldMyBeerSecurity.com where he discusses topics in security that interest him such as incident response, threat hunting, Osquery, and DevSecOps.

Twitter: @CptOfEvilMinion

SpeakerBio: Tilottama Sanyal
Tilottama Sanyal (wildphish) has a degree in Information technology from India and has almost 8 years of combined experience across DevOps and Cybersecurity. She holds certifications like the GCIH and currently works as an Incident Response Team member at Verizon Media (Yahoo!). Her areas of expertise include risk assessments, vulnerability analysis, and incident response. Her current interests include threat hunting and this is her first-ever workshop.
Twitter: @wildphish

SpeakerBio: Dan Borges
A core member of the National CCDC red team and a director for the Global CPTC. Recently wrote a book on deception applied to infosec and attack-defense competitions: https://ahhh.github.io/Cybersecurity-Tradecraft/

Description:
The Hunt for Red Apples workshop guides participants through emulation walkthroughs, hunting playbooks, & hunting exercises around an Ocean Lotus intrusion, an established threat actor targeting macOS. The workshop is broken into sections using both the attack lifecycle & Mitre ATT&CK knowledge base.

For each phase in the attack live cycle participants learn about one particular tactic, relevant macOS data sources, how to build a hunting plan, practice hunting, & how the red team emulated the tactic using open source intelligence.

This workshop is a resource on how to threat hunt, emulate, & use open source threat intelligence on a specific threat actor.

The Hunt for Red Apples workshop guides participants through emulation walkthroughs, hunting playbooks, and hunting exercises around an Ocean Lotus intrusion, an established threat actor targeting macOS. The workshop is broken into sections using both the attack lifecycle and Mitre ATT&CK knowledge base. For each phase in the attack live cycle participants learn about one particular tactic, relevant macOS data sources, how to build a hunting plan, practice hunting, and how the red team emulated the tactic using open source intelligence.

The objective of this workshop is to provide a balanced approach that showcases both hunting and adversary actions. This workshop is a resource on how to threat hunt, emulate, and use open source threat intelligence on a specific threat actor.

The Hunt for Red Apples workshop is broken into two four hour sessions over two days. As a bonus, we are releasing a second data set for a different scenario on day two for more advanced hunters with no playbooks or walkthroughs. Participants will get to test their macOS Threat Hunting skills! And it's all FREE!

Return to Index - Add to Google Calendar - ics Calendar file

SEV - Saturday - 14:30-15:30 PDT

Title: Make Them Want To Tell You: The Science of Elicitation
When: Saturday, Aug 7, 14:30 - 15:30 PDT
Where: Social Engineer Village (Virtual)

SpeakerBio: Christopher Hadnagy
Christopher Hadnagy is the founder and CEO of Social-Engineer, LLC. During Chris' 18 years in the information security industry, he created the world's first social engineering framework and newsletter, as well as hosted the first social engineering based podcast.

Chris is also a well-known author, having written five books on social engineering. Chris' new book, "Human Hacking: Win Friends, Influence People and Leave Them Better Off for Having Met You", released January 5, 2021.

Learn more about the book: https://humanhackingbook.com/

Chris is an Adjunct Professor of Social Engineering for the University of Arizona's NSA designated Center of Academic Excellence in Cyber Operations (CAE-CO). He also lectures and teaches about social engineering around the globe. Moreover, he's been invited to speak at the Pentagon, as well as other high secure facilities. Additionally, as the creator of the world's first Social Engineering Capture the Flag (SECTF), Chris leads the way in educating people on this serious threat.

Chris works with some of the world's leaders in scientific research for the purpose of acquiring a deeper understanding of social engineering. Notably, Chris authored a book with Dr. Paul Ekman regarding the use of nonverbal communication by social engineers.

Description:
What is elicitation? Can it be brought to a science and taught? This talk dives deep into the principles of elicitation and how to use them as an SE, also in every day life.

Social Engineer Village will stream content to Twitch.

Twitch: https://www.twitch.tv/socialengineerllc

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 09:00-09:59 PDT

Title: Making the DEF CON 29 Badge
When: Friday, Aug 6, 09:00 - 09:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Katie Whiteley,Michael Whiteley

SpeakerBio: Katie Whiteley
Katie is a wife, mother, and graphic designer. She likes long walks on the beach because there's no internet connection.

Together with Michael, they are MK Factor, a husband/wife badgemaker team. They've created badges for many conferences and groups like OpenWest, Saintcon, DC801, Car Hacking Village, and many unofficial DEF CON badges. Together they earned a black badge for Car Hacking at DEF CON 24.

Twitter: @ktjgeekmom

SpeakerBio: Michael Whiteley
Michael is a husband, father, and electronics geek. He doesn't like long walks on the beach, but prefers to be indoors with a fast internet connection.

Together with Katie, they are MK Factor, a husband/wife badgemaker team. They've created badges for many conferences and groups like OpenWest, Saintcon, DC801, Car Hacking Village, and many unofficial DEF CON badges. Together they earned a black badge for Car Hacking at DEF CON 24.

Twitter: @compukidmike

Description:

Come meet the new badge makers and hear the story of how this year's badge was created amidst a global pandemic. We'll share tales of chip shortages, delayed parts, and late nights, as well as discuss how the badge works and what you can do with it. Maybe even some hints about the challenges within...

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=H3kdq40PY3s

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20M

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

CAHV - Friday - 14:00-14:59 PDT

Title: Making the Leap - Changing Careers
When: Friday, Aug 6, 14:00 - 14:59 PDT
Where: Career Hacking Village (Talk)

SpeakerBio: Danyelle Davis
No BIO available

Description:
Cyber Security, Research, H4x0r, or that stuff in the place with the thing. Regardless of what you call it, many people end up here after starting down a different career path. I was one of those people. I found myself, a 26 year old, black, female, manual software tester with learning disabilities, in an automated world. I refused to be stuck in a dead end job for the rest of my life. I decided it was time for a switch. Like any transition - some things worked well and some needed improvement. My challenges in maintaining one career while transitioning to another can provide insights as you plan your own.

This talk will be available on YouTube: https://www.youtube.com/watch?v=0mFw0fXia58

Career Hacking Village content will be available on YouTube.

YouTube: https://youtube.com/careerhackingvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: MAVSH> Attacking from Above
When: Friday, Aug 6, 14:00 - 14:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio:Sach

Sach is a self taught developer, an aspiring pentester, and a drone enthusiast. In his spare time he enjoys playing chess, reading Sci-Fi novels, learning about cryptocurrencies, and flying drones.
Twitter: @0xkayn

Description:

Over the course of 2020 and 2021, drone enthusiasts and the FAA have been locked in a series of legal battles over the future of unmanned aviation.

New regulations and restrictions, such as Remote Identification, aim to leave drone and model aviation hobbyists with a grim choice: incur countless financial costs, or lose the ability to fly freely.

Not only do these regulations impact hobbyists, they also restrict our ability to use drones as recon and payload delivery tools, but the FAA gave us a loophole.

In this talk, I'll share my knowledge of the MAVLink protocol and how it can be modified to take advantage of that loophole. I'll also show you how to build a drone capable of 20+ minute flights, potentially multiple miles of range, and hosting a Raspberry Pi 0 W onboard, enabling remote command execution without the use of onboard WiFi or cellular networks ALL while exploiting that loophole.

Come learn how and why the FAA "Can't Stop the Signal"!

REFERENCES

Ardupilot
    https://ardupilot.org/ https://github.com/ArduPilot/ardupilot
MAVLink
    https://mavlink.io/en/

Danger Drone and Defense Measures:
https://resources.bishopfox.com/files/slides/2017/DEF_CON_25_(2017)-Game_of_Drones-Brown_Latimer-29July2017.pdf
https://resources.bishopfox.com/resources/tools/drones-penetration-testers/attack-tools/

Watch Dogs Drone:
https://hackaday.com/2018/05/27/watch-dogs-inspired-hacking-drone-takes-flight/

FAA vs RDQ:
https://www.racedayquads.com/pages/rdq-vs-faa
https://www.gofundme.com/f/savefpv?utm_campaign=p_cp_url&utm_medium=os&utm_source=customer
https://www.suasnews.com/2021/03/racedayquads-com-vs-faa-court-case-in-defense-of-all-drone-pilots-and-model-aviators/

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 16:00-16:30 PDT

Title: Meetup: Certification Processes (UL, FCC, etc.)
When: Saturday, Aug 7, 16:00 - 16:30 PDT
Where: Hardware Hacking Village (Virtual Meetup)

SpeakerBio: ShortTie
No BIO available

Description:
A place to meet people with the same interests or challenges and discuss. The meetup is a nexus for finding and starting the conversation. Bring your expertise and your questions.

#hhv-meetups-A: https://discord.com/channels/708208267699945503/739567085004521533

#hhv-meetups-A-voice: https://discord.com/channels/708208267699945503/739571117756383333

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 15:30-15:59 PDT

Title: Meetup: Legacy Hardware

When: Friday, Aug 6, 15:30 - 15:59 PDT

Where: Hardware Hacking Village (Virtual Meetup)

SpeakerBio:K

No BIO available

Description:

A place to meet people with the same interests or challenges and discuss. The meetup is a nexus for finding and starting the conversation. Bring your expertise and your questions.

#hhv-meetups-A: https://discord.com/channels/708208267699945503/739567085004521533

#hhv-meetups-A-voice: https://discord.com/channels/708208267699945503/739571117756383333

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 15:00-15:30 PDT

Title: Meetup: OSS ASIC
When: Saturday, Aug 7, 15:00 - 15:30 PDT
Where: Hardware Hacking Village (Virtual Meetup)

SpeakerBio: Josh Marks
No BIO available

Description:
Come geek out about ASICs! No ASIC knowledge? No problem — casual conversation about transistor structures, and basic circuit architectures included.

#hhv-meetups-A: https://discord.com/channels/708208267699945503/739567085004521533

#hhv-meetups-A-voice: https://discord.com/channels/708208267699945503/739571117756383333

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 14:30-14:59 PDT

Title: Meetup: PCB Proto and Rework
When: Friday, Aug 6, 14:30 - 14:59 PDT
Where: Hardware Hacking Village (Virtual Meetup)

SpeakerBio:K
No BIO available

Description:
A place to meet people with the same interests or challenges and discuss. The meetup is a nexus for finding and starting the conversation. Bring your expertise and your questions.

#hhv-meetups-A: https://discord.com/channels/708208267699945503/739567085004521533

#hhv-meetups-A-voice: https://discord.com/channels/708208267699945503/739571117756383333

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 17:30-17:59 PDT

Title: Meetup: Some HHV challenges
When: Friday, Aug 6, 17:30 - 17:59 PDT
Where: Hardware Hacking Village (Virtual Meetup)

SpeakerBio:rehr
Rehr is an electrical engineering, and long-time Hardware Hacking Village volunteer. He enjoys teaching and creating challenges that help grow and challenge the hardware hacking community.
Twitter: @mediumrehr

Description:
HHV members have created a few challenges for this year's DEF CON. Come learn and chat about those challenges, or bring new challenges to share with the community. This time will start with an introduction to this year's HHV challenges, but the remaining time will be open to community questions and conversations

#hhv-challenge: https://discord.com/channels/708208267699945503/739567199647301702

#hhv-meetups-A-voice: https://discord.com/channels/708208267699945503/739571117756383333

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 13:00-13:30 PDT

Title: Meetup: Some HHV challenges
When: Saturday, Aug 7, 13:00 - 13:30 PDT
Where: Hardware Hacking Village (Virtual Meetup)

SpeakerBio:rehr
Rehr is an electrical engineering, and long-time Hardware Hacking Village volunteer. He enjoys teaching and creating challenges that help grow and challenge the hardware hacking community.
Twitter: @mediumrehr

Description:

HHV members have created a few challenges for this year's DEF CON. Come learn and chat about those challenges, or bring new challenges to share with the community. This time will start with an introduction to this year's HHV challenges, but the remaining time will be open to community questions and conversations

#hhv-challenge: https://discord.com/channels/708208267699945503/739567199647301702

#hhv-meetups-A-voice: https://discord.com/channels/708208267699945503/739571117756383333

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 09:30-09:59 PDT

Title: Meetup: Some HHV challenges
When: Friday, Aug 6, 09:30 - 09:59 PDT
Where: Hardware Hacking Village (Virtual Meetup)

SpeakerBio:rehr
Rehr is an electrical engineering, and long-time Hardware Hacking Village volunteer. He enjoys teaching and creating challenges that help grow and challenge the hardware hacking community.
Twitter: @mediumrehr

Description:
HHV members have created a few challenges for this year's DEF CON. Come learn and chat about those challenges, or bring new challenges to share with the community. This time will start with an introduction to this year's HHV challenges, but the remaining time will be open to community questions and conversations

---

#hhv-challenge: https://discord.com/channels/708208267699945503/739567199647301702

#hhv-meetups-A-voice: https://discord.com/channels/708208267699945503/739571117756383333

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 14:00-14:30 PDT

Title: Meetup: Sourcing Parts & The Global Parts Shortage
When: Saturday, Aug 7, 14:00 - 14:30 PDT
Where: Hardware Hacking Village (Virtual Meetup)

SpeakerBio:bombnav
No BIO available

Description:
Sourcing parts in the COVID involves new challenges due to supply chain issues. Counterfeiting continues to be an problem with out of production parts. This meetup is designed to share ideas and sources for acquiring parts for electronic hobbyists.

#hhv-meetups-A: https://discord.com/channels/708208267699945503/739567085004521533

#hhv-meetups-A-voice: https://discord.com/channels/708208267699945503/739571117756383333

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 12:30-12:59 PDT

Title: Microsoft ML Security Evasion Competition Details
When: Friday, Aug 6, 12:30 - 12:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Hyrum Anderson
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

Title: Mind the Gap - Managing Insecurity in Enterprise IoT
When: Saturday, Aug 7, 13:45 - 14:30 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Cheryl Biswas , Threat Intel Specialist, TD
Cheryl Biswas is a Threat Intelligence Specialist with TD Bank in Toronto, Canada, where she produces and delivers annual cyber threat forecasts, and has experience in security audits and assessments, privacy, disaster recovery and change management. She holds an ITIL certification and a specialized honours degree in Political Science. Cheryl is actively engaged in the security community as a conference speaker and volunteer, mentors those entering the field, and champions women and diversity in cyber security as a founding member of "The Diana Initiative".
Twitter: @3ncr1pt3d

Description:

IoT is an ever-expanding attack surface about which we have many misconceptions and assumptions but for which we have very few policies, regulations or security. These are devices built for one purpose, not meant to be upgraded and rarely if ever patched. As more devices are enabled to connect and communicate online, in the relentless pursuit of innovation, we've put the cart before the horse and failed to construct a framework to effectively control and secure the capability created. Consider this: over 90% of the data in the world was created over the past two years, and current output is roughly 2.5 quintillion bytes per day. As IoT moves into a range of enterprise environments, driven by consumer demand and BYOD desire, Shadow IT becomes Shadow ET, bringing new challenges and risks that our existing compliance and security don't address or regulate. Misconfiguration usurps any benefits of eroding segregation as online exposure of both sensitive data and critical systems increases. Adversaries at all levels have been watching, waiting and are making their moves because ignorance isn't an excuse – it's an invitation to exploitation.

Introduction: (2 min)
• A deluge of data
• So many devices and growing

I have a dream: (5 min)
• Perceived benefits of IoT
• Improved efficiency, innovation, collaboration • We don't know what we're doing
• The dangers of upholding a Utopian ideal as reality • "The cost of breaches will be viewed like the toll taken by car crashes, which have not persuaded very many people not to drive."

Defining IoT: (10 min)
• Our assumptions: what we think IoT is • What is and isn't IoT. Adding intelligence to devices that are normally "dumb", enabling them to communicate without human involvement • Failure to inventory IoT devices because no centralized control over what IoT devices and applications are in the workplace • Me and My Shadow IoT
o An open invitation to Shadow IoT through increasing unmonitored, unsanctioned BYOD • Recent statistics on IoT cyberattacks on organizations o "82% of organizations that manufacture IoT devices are concerned that the devices they develop are not adequately secured from a cyberattack." (Irdeto Global Connected Industries Cybersecurity Survey 2019) • Insecure third parties and Shadow IoT risks - what the party of your third party allows without your knowledge or consent • Different flavors – ET, IIoT, IoHT, OT Takeaways:
Attendees will understand what makes IoT/ET different from standard equipment we connect, and why we cannot secure them the same way. Attendees will be alerted to the ongoing and increasing risk of Shadow IT within their networks so they can take action on it

Understanding IoT Architecture: (5 min) • Sensors working overtime - Sensors and actuators connecting the digital and physical realms • Internet gateway
• The Edge
• Managing, securing and storing all the data • Communication architectures

- What is Enterprise Architecture
- Understanding IoT in the Enterprise
- Enterprise Architecture and IoT: How to build IoT into Enterprise Architecture

How IoT Attacks are Different: (5 min)
• A lack of awareness around the motivation, perpetrators, attacks • Different threat dynamic: industrial espionage, damage, destruction. • Geopolitics and the games nationstates play. After Stuxnet - Iran and Shamoon wiper malware. • Threat actors seek something more than just monetary gain. Triton destructive malware. • How sanctions drive retaliation. What could we expect in the current climate? Takeaway: Attendees will understand IoT/ET as a potential threat, who attackers are and how to evaluate what they have in place to improve their security It Only Takes One: Analysis of Attacks (15 min) • It only takes ONE exposed, misconfigured system to spread the infection. • Think ransomware: an increase in targeted ransomware attacks on industry in 2019 using LockerGoga and MegaCortex. Norsk Hydro • Think NotPetya. Targeted attack that spread from one laptop globally bringing Maersk down. • How cryptominers are increasingly leveraging exploits on critical vulnerabilities in enterprise realms and spreading via EternalBlue. Targets include Docker containers, and container escapes. • Compromised conference equipment. Examine the attack on Polycom HDX video conferencing systems. Thousands exposed externally, many more deployed internally. Polycom systems are linked to each other across different corporate offices globally. Takeaway: Attendees will be able to understand how an attack could be leveraged against IoT/ET in their enterprise environments

Making it Better: (5 min)
• IoT policy and compliance
• Strong authentication: what do we do better when we know that passwords and certs have failed us • Automating the identification of IoT – no more hide and seek • Network segmentation - it only works if we do it • Automatically securing IoT devices before something happens, not after • The need for Unified Endpoint Management over Enterprise Mobility Management.

Takeaways: Attendees will have recommendations to bring back they they can action within their environments for increased security posture

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 12:45-13:30 PDT

Title: MIPS-X - The next IoT Frontier
When: Saturday, Aug 7, 12:45 - 13:30 PDT
Where: IoT Village (Talk - Virtual)
Speakers: Patrick Ross,Zoltán Balázs

SpeakerBio: Patrick Ross
Patrick (0xn00b), a DEF CON 26 Black Badge holder, is the co-founder of Village Idiot Labs which helps run IoT Village across the globe. Patrick has created a fully immersible/virtual web-based lab environment that people can learn how to hack IoT without the need for their own tools, equipment or even prior knowledge.

SpeakerBio: Zoltán Balázs
Zoltan (@zh4ck) is the Head of Vulnerability Research Lab at CUJO AI, a company focusing on smart home security. Before joining CUJO AI he worked as a CTO for an AV Tester company, as an IT Security expert in the financial industry, and as a senior IT security consultant. He is also the developer of the Hardware Firewall Bypass Kernel Driver (HWFWBypass), the Encrypted Browser Exploit Delivery tool (#IRONSQUIRREL) and the Sandbox tester tool to test Malware Analysis Sandboxes. He found and disclosed a vulnerability in IP cameras, and this vulnerability was exploited by the Persirai botnet, running on ˜600 000 cameras.
Twitter: @zh4ck

Description:

IoT vulnerability research usually involves both static and dynamic analysis of the target device. To aid in this task, researchers typically perform some sort of emulation to enumerate the filesystem as well as run the respective binaries. Luckily, there are tools like QEMU and/or Buildroot to guide our path on the way, but this does not mean the way is smooth.

Our main goal was to create a framework and documentation suitable for MIPS (LE/BE) device research, which can be used in a Dockerized environment to set up as many emulated IoT devices as desired. The goal was to create the least amount of pain and effort to set up the emulation infrastructure. This means, you will have a target MIPS architecture virtual machine running natively with all the binaries, full network stack, debugging tools, and other useful tools. Let the pwning begin!

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: MITRE Engage: A Framework for Adversary Engagement Operations
When: Friday, Aug 6, 11:00 - 11:59 PDT
Where: Packet Hacking Village - Talks (Virtual)
Speakers: Stan Bar,Gabby Raymond,Maretta Morovitz

SpeakerBio: Stan Bar
Dr. Stanley Barr is a three-time graduate of University of Massachusetts Lowell. He has a BS in Information Sciences, an MS in Mathematics, and a PhD in Computer Science. He has coauthored papers in malware analysis, barrier coverage problems, expert systems for network security, and robotic manufacturing. He has spoken at MILCOM and been a panelist for several conferences. Additionally, he has appeared on several podcasts on adversary engagement and presented at TEDx. Currently, he is a Principal Scientist at The MITRE Corporation. He currently is the Capability Area Leader for Cyber Denial, Deception, and Adversary Engagement. Stan lives with his wife, 5 rescue dogs, and 15 chickens.

SpeakerBio: Gabby Raymond , CO-CAPABILITY AREA LEAD, CYBER DENIAL, DECEPTION, AND ADVERSARY ENGAGEMENT, THE MITRE CORPORATION
Gabby Raymond is a two-time graduate from Tufts University. She holds a B.S. in Mathematics and Computer Science and a M.S. in Computer Science. Her research has spanned topics in intrusion detection, cyber-physical systems, and machine learning applications for security. Gabby recently co-authored a Choose Your Own Adventure style book called "The Toolbox of Innovation" with members of MITRE's Innovation Toolkit team. Outside of work, Gabby enjoys knitting and judging science fairs. Gabby is the Co-Capability Area Lead for Cyber Deception and Adversary Engagement at The MITRE Corporation.

SpeakerBio: Maretta Morovitz , SENIOR CYBER SECURITY ENGINEER, THE MITRE CORPORATION
Maretta Morovitz is a graduate of Tufts University School of Engineering, where she graduated with a degree in Computer Science. She is a Senior Cyber Security Engineer at the MITRE Corporation where she works in the areas of adversary engagement, malware analysis, and reverse engineering. She is a founding member of MITRE's Cyber Deterrence and Adversary Management (CDAM) team and has helped shape MITRE's adversary engagement work for the last two years. She was recently named as one fo the AFCEA 40 Under 40 Awardees for 2021. Outside of work you can find her nerding out about the latest Brandon Sanderson novel, still anxiously awaiting her letter from Hogwarts, or snuggling with her dog and hedgehog.

Description:
For 10+ years MITRE has been engaged in denial, deception, and adversary engagement operations for internal defense and research purposes. We have created MITRE Engage as a framework for planning and communicating about adversary engagement operations. In our talk we include:

- A brief overview of what we mean when we say denial, deception, and adversary engagement
- Our vision for the future and why we think this technology matters
- A brief history of our past experiences (and failures) in this space and how that shaped where we are today
- The official release of MITRE Engage 0.9 Beta and ask for community feedback
- A fictional walkthrough of how you can use Engage to get started in adversary engagement operations

All Packet Hacking Village talks will stream on YouTube, Twitch, Facebook, and Periscope.

YouTube: https://youtube.com/wallofsheep

Twitch: https://twitch.tv/wallofsheep

Facebook: https://www.facebook.com/wallofsheep/

Periscope: https://www.periscope.tv/wallofsheep

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 14:30-15:30 PDT

Title: Modern Authentication for the Security Admin
When: Saturday, Aug 7, 14:30 - 15:30 PDT
Where: Blue Team Village - Main Track (Virtual)
Speakers: Bailey Bercik,Mark Morowczynski

SpeakerBio: Bailey Bercik
Bailey Bercik (@baileybercik on Twitter) is a Program Manager in the customer facing arm of the Identity Engineering division at Microsoft. As part of the “Get-To-Production” team, she acts as a trusted advisor to Fortune 500 enterprises deploying Azure Active Directory. She's previously spoken about Azure AD customer stories and security recommendations at Microsoft Ready & Ignite, Blue Team Con, The Diana Initiative, and BSides Portland. Prior to this role, Bailey worked on Microsoft's incubation team for Decentralized Identity and volunteered as a computer science teacher at Warden High School.
Twitter: @BaileyBercik

SpeakerBio: Mark Morowczynski
Mark Morowczynski (@markmorow) is a Principal Program Manager on the customer success team in the Microsoft Identity division. He spends most of his time working with customers on their deployments of Azure Active Directory. He's spoken at various industry events such as Black Hat 2019, Defcon Blue Team Village, GrayHat, several BSides, Microsoft Ignite, Microsoft Inspire, Microsoft MVP Summits, The Experts Conference (TEC), The Cloud Identity Summit, SANs Security Summits and TechMentor. He can be frequently found on Twitter as @markmorow arguing about baseball and making sometimes funny gifs.
Twitter: @markmorow

Description:
Modern authentication protocols such as SAML, OAuth and OpenID Connect. Claims, bearer tokens and JWT tokens are traversing various authentication flow paths in your environment today. In this session we will break down these authentication concepts and common flows for the non-identity admin. We will also discuss some common attacks and defenses the security team should be monitoring for and implementing in their environment.

Many organization's applications are moving to modern authentication protocols such as SAML, OAuth and OpenID Connect. Claims, bearer tokens and JWT tokens are traversing various authentication flow paths in your environment today. Security teams need to be just as familiar with how these work, the risks and the benefits they provide, as they are with Kerberos tickets and NTLM hashes (please stop btw). In this session we will break down these authentication concepts and common flows for the non-identity admin. We will also discuss some common attacks and defenses the security team should be monitoring for and implementing in their environment.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Modern Malware Analysis for Threat Hunters

When: Sunday, Aug 8, 10:00 - 13:59 PDT

Where: Workshops - Las Vegas 1+2 (Onsite Only)

Speakers: Aaron Rosenmund,Ryan Chapman

SpeakerBio: Aaron Rosenmund , Security Researcher

Aaron M. Rosenmund is a cyber security operations subject matter expert, with a background in federal and business defensive and offensive cyber operations and system automation. Leveraging his administration and automation experience, Aaron actively contributes to multiple open and closed source security operation platform projects and continues to create tools and content to benefit the community. As an educator & cyber security researcher at Pluralsight, he is focused on advancing cyber security workforce and technologies for business and national enterprises alike. In support of the Air National Guard, he contributes those skills part time in various initiatives to defend the nation in cyberspace. Certifications: GIAC GCIA, GIAC GCED, CCNA Cyber Operations, Pentest+, CySa+ www.AaronRosenmund.com @arosenmund "ironcat"

Twitter: @arosenmund

SpeakerBio: Ryan Chapman , Principal IR Consultant

Ryan is an experienced incident response practitioner, malware analyst, and trainer. He is a Principal IR Consultant for BlackBerry, the lead organizer of CactusCon, a SANS trainer for FOR610: Reverse Engineering Malware, and a Pluralsight author. Ryan strives to imbue comedy into his trainings and loves being able to teach others while learning from them at the same time. He is a veteran speaker having presented talks and/or workshops at conferences including DefCon, SANS Summits, BSides events, CactusCon, and more. Prior to working in IR, Ryan worked as a technical trainer for over five years. "We must not teach people how to press buttons to get results. We must teach people what happens when these buttons are clicked, such that they fully understand the processes occurring in the background," says Ryan.

Description:

Malware authors go to great lengths to bypass enterprise security to deliver malware, avoid detection after the initial intrusion and maintain persistence to compromise an organization. To achieve this, malware authors employ a wide variety of obfuscation and anti-analysis techniques at each phase of an attack. In this workshop, you will get hands-on with real-world malware and learn how to identify key indicators of compromise (IOCs)/indicators of attack (IOAs), apply analysis to enhance security products to protect users and infrastructure and gain a deeper understanding of malware behavior through reverse engineering.

This workshop will utilize open-source and limited use tools such as Ghidra, IDA Pro Free/Demo, Oledump/OleVBA, PE Studio, and Suricata to perform deep technical analysis of malware, focusing on developing effective strategies to maximize your time spent. By the end of this workshop, you will be able to analyze malicious office documents, identify signs of packing, defeat obfuscation and other anti-analysis techniques and use traffic analysis to aid in detection and identifying of prevalent malware families. These skills ultimately allow you to generate valuable threat intelligence to aid in your efforts to defend your organization or respond to an incident.

This is a fast-paced course designed to take you deep into malware operations – from delivery methods to payloads! Numerous labs will reinforce key learning objectives throughout the workshop and each lab comes with a detailed lab guide. Comprehensive analysis activities and exercises are used to to test and reaffirm key learning objectives and ensure attendees have a start-to-finish understanding of the material.

Attendees will be provided with all the lab material used throughout the course in a digital format. This includes all lab material, lab guides and virtual machines used for training. This workshop will also utilize several live classroom sharing resources, such as chat and notes to ensure that attendees have access to all material discussed throughout the training. All the material provided will help to ensure that students have the ability to continue learning well after the course ends and maximize the knowledge gained from this course.

Registration Link:
https://www.eventbrite.com/e/modern-malware-analysis-for-threat-hunters-las-vegas-1-2-tickets-162214781779

Prerequisites

The primary requirement for this course is a desire to learn and the determination to tackle challenging problems. In addition, having some familiarization with the following topics will help students maximize their time in this course:

- ◊ Basic familiarity with Linux and the terminal
- ◊ An understanding of programming languages such as control structures (IF statements, loops and functions), data structures (objects, structures, arrays) and variable usage will be helpful

Materials needed:

- Linux/Windows/Mac desktop environment
- A laptop with the ability to run virtualization software such as VMWare or VirtualBox
- Access to the system BIOS to enable virtualization, if disabled via the chipset
- Ability to temporarily disable anti-virus or white-list folders/files associated with lab material
- A laptop that the attendee is comfortable handling live malware on
- Enough disk space to store at least a single 40 GB VM, although multiple VMs may be used

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Saturday - 17:00-17:15 PDT

Title: Monero After Party
When: Saturday, Aug 7, 17:00 - 17:15 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Monero Sound
No BIO available

Description:

Quick reminder for the Monero Party that will begin later that evening. Previous Monero parties have been so excellent that they made the news. Tickets available at monerosound.com

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Saturday - 13:00-13:15 PDT

Title: Monero Scaling Opportunities and Challenges
When: Saturday, Aug 7, 13:00 - 13:15 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Francisco Cabañas
No BIO available

Description:
This is a short 15 minute talk followed by an open Q&A session. We will cover the impact of technology, business models and protocols on payment ledgers starting with the advent of general purpose payment, credit and debit cards since the 1940's followed by the advent of de centralized blockchain based ledgers such as Bitcoin (2009) and Monero (2014). The critical distinction between technological limitations and protocol / business model limitations and the impact of technological limitations at a given point in time on the development of protocols and business models. We will consider how various protocols and business models can compete with each other and in particular what the Monero scaling protocol has to tell us about the limitations of scaling in Bitcoin and similar cryptocurrencies.

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

Title: Mooltipass
When: Friday, Aug 6, 10:00 - 11:50 PDT
Where: DemoLab Video Channel 2

SpeakerBio: Mathieu Stephan
Mathieu Stephan is an electronics engineer who is actively involved in the open source movement. He specializes in designing devices from the ground up and alternates between full-time positions in the security and communication industries and contracting jobs in other sectors – from quantum physics to Formula E cars. He has been a writer for Hackaday and has a personal website filled with electronics projects.

Description:
Tool or Project Name: Mooltipass

Short Abstract: The Mooltipass project is a completely open-source ecosystem aimed at providing hardware-based authentication solutions. Its latest family member, the Mooltipass Mini BLE, features a dual microcontroller architecture aimed at separating the communications and security domains, together with an OLED screen and dedicated flash memories for credentials and graphics storage. The Mooltipass project is an ongoing 7-year adventure with contributors from around the globe. It has produced 3 hardware devices, multiple browser extensions, a cross-platform user interface and software daemon, an SSH agent and a python library.

Short Developer Bio: Mathieu Stephan is an electronics engineer who is actively involved in the open source movement. He specializes in designing devices from the ground up and alternates between full-time positions in the security and communication industries and contracting jobs in other sectors – from quantum physics to Formula E cars. He has been a writer for Hackaday and has a personal website filled with electronics projects.

URL to any additional information: https://github.com/mooltipass/minible

Detailed Explanation of Tool: The Mooltipass project is an authentication ecosystem centered around several open source devices, the Mooltipass Standard, Mini and BLE.

Among its many features, it offers:
Files, notes and credentials storage
FIDO2 (WebAuthn), TOTP and SSH support
Native credentials recall into browser login fields On-device language and security parameter customization Standalone credential typing using the device's standard USB or Bluetooth Keyboard HID channels Cross-platform tools allowing device database management and synchronization Its latest family addition, the Mini BLE, includes the following hardware features: A dual microcontroller architecture: the 'auxiliary' ATSAMD21E18 takes care of USB (HID, FIDO2, custom HID) and Bluetooth Low Energy (HID and custom HID) communications while the 'main' ATSAMD21G18 takes care of the rest. A dedicate hardware line for the main MCU to hard-disable BLE communications A 256x64x4bpp 2.08" OLED screen
A clickable scroll wheel for fast user interaction A smartcard connector to interface with secure elements storing the encryption keys A dedicated flash memory for graphics, strings and signed firmware updates A dedicated flash memory for users' encrypted databases Purpose-built charging electronics for the NiMH battery The firmware running on the ATSAMD21E18 and on ATSAMD21G18 was built from scratch, except the crypto routines which are from the open source BearSSL library, and the BLE features which are from the Atmel-proprietary library. The firmware provides the following features: A fully-fledged graphical library that handles compressed bitmaps and font rendering, using an internal frame buffer as needed A custom-made database model allowing storage of credentials, files, notes and WebAuthn secrets while still allowing ease-of-use features such as favorites A read-only file system library allowing fetching of graphical data, user-selected language strings, firmware updates and keyboard HID lookup tables A dedicated abstraction layer allowing the device to send unicode text using simulated key presses through BLE & USB HID, with support for dozens of keyboard layouts Graphical and database storage support of the Unicode Basic Multilingual Plane Time based One Time Password (TOTP) and FIDO2 (WebAuthn) support On-device password generation and credential display To facilitate our development

process and to allow device testing by everyone, we developed device emulators for Windows and Linux. These emulators also enable testing most of the Mooltipass ecosystem open-source software components:

1. Moolticute, a Qt-based cross-platform software tool composed of a daemon & user interface allowing the user to: customize device behavior (more than 30 settings, requested by our beta testers and users of previous generations of the Mooltipass) manage, modify, import and export a user's database directly view and edit notes stored on the device upload and download files to and from the device manage FIDO2 credentials
2. mc-agent, an SSH agent running on the OS side allowing password-less SSH authentication, written in Go
3. mooltipy, a python library to recall credentials stored on the Mooltipass
4. mc-cli, a command line tool written in Go to interact with the device

Supporting Files, Code, etc: https://github.com/mooltipass

Target Audience:
Hardware, Defense

How will you or your Demo Lab contribute a new perspective to the content at DEF CON? The Mooltipass project takes a fundamentally different approach from the commonly used software-based security solutions that require non-compromised systems to run on. We want to show that there are open source hardware solutions out there that do not sacrifice security for ease-of-use and while reducing the attack surface to a very strict minimum.

This content will be presented on a Discord video channel.

#dl-video2-voice: https://discord.com/channels/708208267699945503/734027778646867988

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Thursday - 22:00-22:59 PDT

Title: Music - Abstrct
When: Thursday, Aug 5, 22:00 - 22:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Abstrct
Abstrct has spent his quarantine bringing dirty progressive and dancey funk to your living rooms, kitchens, patios, and pools each weekend, but holy heck is he ready to bring the party back to DEF CON proper.

https://soundcloud.com/abstrct/saturday-morning-quarantoons-ep46 https://imgur.com/m5Jcql2
https://twitter.com/Abstr_ct
https://www.twitch.tv/abstr_ct

Twitter: @Abstr_ct

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Friday - 01:00-01:59 PDT

Title: Music - Acid T
When: Friday, Aug 6, 01:00 - 01:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Acid T
Prepare for some Post Pandemic Pandemonium!

https://www.facebook.com/dj.sm0ke
https://www.twitch.tv/studio_sm0ke
https://www.youtube.com/channel/UC55xsENb9PKz-IKB5zodYGA https://soundcloud.com/acid_t
https://twitter.com/DJ_Sm0ke
https://youtu.be/3lIhyGU4uB4
https://soundcloud.com/acid_t/liquid-feeling

Twitter: @DJ_Sm0ke

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Thursday - 21:00-21:59 PDT

Title: Music - CTRL/RSM

When: Thursday, Aug 5, 21:00 - 21:59 PDT

Where: Bally's Silver Ballroom

SpeakerBio:CTRL/rsm
an audio / visual bombardment of your cerebral cortex

https://www.instagram.com/ctrlrsm
https://www.facebook.com/ctrlrsm
https://www.twitch.tv/ctrlrsm

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Sunday - 01:00-01:59 PDT

Title: Music - CTRL/rsm
When: Sunday, Aug 8, 01:00 - 01:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio:CTRL/rsm
an audio / visual bombardment of your cerebral cortex

https://www.instagram.com/ctrlrsm
https://www.facebook.com/ctrlrsm
https://www.twitch.tv/ctrlrsm

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Thursday - 21:00-21:59 PDT

Title: Music - Deep Therapy
When: Thursday, Aug 5, 21:00 - 21:59 PDT
Where: Bally's Pool

SpeakerBio: Deep Therapy
Deep Therapy, the duo based out of South Florida began by hosting and DJ'n their own college radio shows. Constantly achieving new heights of dancefloor energy and pushing the boundaries of convention, Deep Therapy is recognized as one of South Florida’s essential DJ’s. Deep Therapy has been featured on Sirius XM radio in Ultra Music Festival Radio, opening up for Infected Mushroom as well as performing at Ultra Music Festival Miami three years, featured across Miami Music Week events, and has performed / held residencies at Space Miami and Treehouse Miami.

https://www.mixcloud.com/SoundboxMiami/deep-therapy-defcon-conference-2020-wall-of-sheep/
https://imgur.com/ylG9jDo
https://www.facebook.com/deeptherapy

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Friday - 00:00-00:59 PDT

Title: Music - DJ St3rling
When: Friday, Aug 6, 00:00 - 00:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio:DJ St3rling
L33t Hacker by day, DJ by night- DJ St3rling brings those dirty ass bass wobbles and loads of remixed electronic house music. Together, let's Drink all the booze and Hack all the things! Let's Rock <3

https://www.facebook.com/photo?fbid=1277406085958716&set=a.116333305399339 https://www.youtube.com/c/DJSt3rling
https://www.facebook.com/OfficialDjSt3rling https://www.instagram.com/theycallmest3r
https://soundcloud.com/theycallmest3r
https://www.twitch.tv/theycallmest3r

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Thursday - 23:00-23:59 PDT

Title: Music - Dr. McGrew
When: Thursday, Aug 5, 23:00 - 23:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Dr. McGrew
By day, Dr. McGrew serves as Senior Cyber Fellow for MartinFederal. By night he spins a curated collection of house and more.

https://pbs.twimg.com/profile_images/1319660847069802497/g9z15y61_400x400.jpg https://twitter.com/McGrewSecurity

Twitter: @McGrewSecurity

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Friday - 22:00-22:59 PDT

Title: Music - FuzzyNop
When: Friday, Aug 6, 22:00 - 22:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: FuzzyNop
FuzzyNop is a computer, raised by computers that told him to computer, now he knows how to computer.

https://www.youtube.com/watch?v=dqtTPco4_v8
https://drive.google.com/drive/folders/1DJDbugX8FfhyeZ8AZhemEYrb86qbmGJ2?usp=sharing https://twitter.com/fuzzynop
https://www.vjdj.io

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Thursday - 23:00-23:59 PDT

Title: Music - FuzzyNop
When: Thursday, Aug 5, 23:00 - 23:59 PDT
Where: Bally's Pool

SpeakerBio: FuzzyNop
FuzzyNop is a computer, raised by computers that told him to computer, now he knows how to computer.

https://www.youtube.com/watch?v=dqtTPco4_v8
https://drive.google.com/drive/folders/1DJDbugX8FfhyeZ8AZhemEYrb86qbmGJ2?usp=sharing https://twitter.com/fuzzynop
https://www.vjdj.io

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Saturday - 22:00-22:59 PDT

Title: Music - Icetre Normal
When: Saturday, Aug 7, 22:00 - 22:59 PDT
Where: Bally's Pool

SpeakerBio: Icetre Normal
Sometime in 1975, a fissure in the time-space continuum, allowed for only briefest of moments the possibility of time travel. A young iconoclast first born in 2275 took advantage of this brief opportunity.

He traveled with only his knowledge of the art of party creation, ability to bend space and time, and supreme skill of serving the masses with only the smallest pool of available alcohol.

First appearing at Defcon X, since then Icetre can always be found somehow making the impossible possible, and bringing the funk while doing so.

https://photos.app.goo.gl/tUi8xmRuKpLCuVC16 https://www.facebook.com/icetre.normal
https://www.twitter.com/aniabeenz
https://www.youtube.com/channel/UCVY8zEm23QFbO-7LfWLR6xg

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Saturday - 22:00-22:59 PDT

Title: Music - Krisz Klink
When: Saturday, Aug 7, 22:00 - 22:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Krisz Klink
No BIO available

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Saturday - 01:00-01:59 PDT

Title: Music - Magik Plan
When: Saturday, Aug 7, 01:00 - 01:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Magik Plan
Magik Plan was founded in 2008 by Garrett Jones. Originally getting his start in electronic music by setting up projections for underground parties, he carved his way through the early days of the dance music scene while making a name for himself as Magik Plan. His obsession with guitars and live instrumentals lead him into diving into the world of sound design. After graduating college in 2009, Garrett began releasing music on online platforms such as SoundCloud.

Fast forward 10 years later, Magik Plan has become a growing name in PsyTrance, Progressive House, Drum n Bass, Chillout and more flavors of electronica.

https://drive.google.com/file/d/1Mj2TAyZdj5tZljcK3oTzg-5lSNpZh5pg/view?usp=sharing https://soundcloud.com/magikplan
https://instagram.com/magikplan
https://facebook.com/magikplan
https://spoti.fi/3jBy8ko

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Saturday - 21:00-21:59 PDT

Title: Music - mattrix

When: Saturday, Aug 7, 21:00 - 21:59 PDT

Where: Bally's Pool

SpeakerBio:mattrix
https://1drv.ms/v/s!AKEhFmBpC9cHimI
https://twitter.com/mattrix_
Insta @mattrixla
Twitter: @mattrix_

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Saturday - 23:00-23:59 PDT

Title: Music - Miss Jackalope
When: Saturday, Aug 7, 23:00 - 23:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Miss Jackalope
Miss Jackalope is DEF CON's resident community DJ who has a Threat Intel $day job, makes a ton of awesome Jackalope Army swag (see the DC Vendor area), hosts a goofy DJ steam on Twitch, herds Ingress cats, and says silly things on Twitter. She plays drum and bass and techno and is known for playing so hard the ceiling caves in. Long live the Jackalope Army!

http://www.dj-jackalope.com/appearence.html https://Twitch.tv/missjackalope
https://twitter.com/djjackalope
https://instgram.com/djjackalope
https://missjackalope.com
https://mixcloud.com/djjackalope
https://missjackalope.square.site

Twitter: @djjackalope

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Friday - 23:00-23:59 PDT

Title: Music - n0x08

When: Friday, Aug 6, 23:00 - 23:59 PDT

Where: Bally's Silver Ballroom

SpeakerBio:n0x08

n0x08 has been obliterating eardrums with filthy drum&bass since he first played the Seattle club scene in the early 2000's. A staunch advocate against laptop DJ's and for getting TF off his lawn, the pandemic finally made him break down & switch to digital. He rides to Valhalla, shiny & chrome!

https://media.wired.com/photos/5f726156dc40abe2b60138b1/master/w_1600%2Cc_limit/backchannel_cti_seattle.jpg
https://twitter.com/n0x08
https://soundcloud.com/n0x08

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Saturday - 23:00-23:59 PDT

Title: Music - Nina Lowe
When: Saturday, Aug 7, 23:00 - 23:59 PDT
Where: Bally's Pool

SpeakerBio: Nina Lowe
Nina fights crime as a cyber threat analyst, defending global, diverse environments. She's most passionate about food, science fiction, music, and kicking all the @ss.

Genres: DnB, Tech House, Techno, Psytrance

https://imgur.com/a/bSyxPzE
https://twitter.com/PacketTorta
https://soundcloud.com/ninalowe
https://www.twitch.tv/packettorta

Twitter: @PacketTorta

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Saturday - 21:00-21:59 PDT

Title: Music - Ohm-i
When: Saturday, Aug 7, 21:00 - 21:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Ohm-i
Ohm-I is known for his music that primarily focuses on storytelling and comedy from a nerdy perspective. He is a Navy veteran and currently a red teamer with a strong penchant for causing you to involuntarily dance and sing along. He has performed at several major anime/gaming conventions and heavily supports spreading awareness of information security careers to kids in underrepresented communities. Ohm-I has performed at DEF CON NYE, Sony Online Entertainment Live, Otakon, SXSW, various PAX venues, and various other cons and venues all over the country as part of the Nerdy People of Color Collective.

https://mcohmi.com/photos
https://twitter.com/mcohmi
https://www.instagram.com/mcohmi/
https://twitter.com/NPCCollective
https://www.twitch.tv/mcohmi

Twitter: @mcohmi

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Saturday - 00:00-00:59 PDT

Title: Music - Scotch & Bubbles
When: Saturday, Aug 7, 00:00 - 00:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Scotch & Bubbles
Scotch and Bubbles have a long history of brining the untz, unce, and wub to nursing homes, children's hospitals, and employee sexual harassment training (giggity). When not running her NFT side hustle with Ken in her dreamhouse, the Barbie has kept playing on during COVID at “it’s not you it’s the virus” break-ups, awkward coworker Zoom game nights, background music for Floyd Mayweather’s Cameo videos, and private pool cocktail deliveries for the at-home cabana experience. Previous tik-tock and YouTube vloggers have said about Zack " it’s better than still being stuck at home", "definitely some value as a free show", and "he’s better off backstage".

Fan [girls|boys] can find Erin on-the-line as @secbarbie on Twitter and Erin's Secret Society of Stalkers at secbarbie.com. Interested peeps, stalkers, and midget strippers can join Zack's A++ #1 Fan club @ zfasel.com on Twitter or unliking/unsubscribing/refusing to comment as zfasel here.

http://scotchandbubbles.club/wp-content/uploads/2021/05/profile_zack-barbie.png https://www.twitch.tv/secbarbie
https://soundcloud.com/secbarbie
https://twitter.com/secbarbie
https://twitter.com/zfasel

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Thursday - 22:00-22:59 PDT

Title: Music - Tense Future
When: Thursday, Aug 5, 22:00 - 22:59 PDT
Where: Bally's Pool

SpeakerBio: Tense Future
Los Angeles, CA. Trapped in an autonomous car during a solar flare. Anxiety attack over spying home appliances that tip their hand. General AI caretaker grappling over competing logical fallacies. Dark techno sounds from the tense future that was once distant.

https://soundcloud.com/tensefuture/d...years-eve-2020 https://soundcloud.com/tensefuture/live-def-con-27-phv https://www.dropbox.com/s/nhwpfpule1...pdate.jpg?dl=0 https://soundcloud.com/tensefuture https://twitter.com/tensefutur3

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Friday - 22:00-22:59 PDT

Title: Music - Terrestrial Access Network
When: Friday, Aug 6, 22:00 - 22:59 PDT
Where: Bally's Pool

SpeakerBio: Terrestrial Access Network
If packets were to dance, they would surely dance to this.

https://soundcloud.com/collinsulliva...mix-07-06-2019 https://www.mediafire.com/view/g31mc...PRESS.png/file
https://soundcloud.com/collinsullivan
https://www.instagram.com/terrestrialaccessnetwork/

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Friday - 21:00-21:59 PDT

Title: Music - Thaad

When: Friday, Aug 6, 21:00 - 21:59 PDT

Where: Bally's Silver Ballroom

SpeakerBio: Thaad

Lead DJ and Promoter at Malevolent-Las Vegas. Founder of Anti-Klub.
Power Noise Movement Original.
Klub Terminal Resident DJ.

https://facebook.com/djTotalHarmonDistortion https://www.twitch.tv/djthaad
https://www.mixcloud.com/DJ_ThAAd
https://soundcloud.com/d-j-th-d

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Friday - 21:00-21:59 PDT

Title: Music - Yesterday & Tomorrow
When: Friday, Aug 6, 21:00 - 21:59 PDT
Where: Bally's Pool

SpeakerBio: Yesterday & Tomorrow
Yesterday & Tomorrow believes in DJing as an art form, seeking to establish a deep connection with listeners through rhythm and sound.

Influenced heavily by legendary DJs such as John Digweed and Hernan Cattaneo, his musical selections showcase the latest in underground dance music from all corners of the globe, from Argentina to Berlin and beyond.

Y&T has performed at various DEF CON venues and events for several years running and showcases the latest releases weekly on select streaming platforms.

https://www.mixcloud.com/yesterdayan...-showcase-mix/ https://imgur.com/sHtxfyv
Mixcloud: https://www.mixcloud.com/yesterdayandtomorrow Twitch: https://twitch.tv/yesterdayandtomorrow Additional: https://linktr.ee/yesterdayandtomorrow

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Friday - 23:00-23:59 PDT

Title: Music - Z3NPI
When: Friday, Aug 6, 23:00 - 23:59 PDT
Where: Bally's Pool

SpeakerBio:Z3NPI
Z3Npi is the culmination of over 2 decades of writing, recording, and performing electronic music from many genres. Originally known as dj:devoid, Chris Schmidt has spent over half his life creating music and is bringing to bear the experience he’s gained to a new project. With Z3Npi, the concept is clear:

“Music is the glue that holds us togethers, it can heal our hearts and minds in ways that nothing else can”.

Collaboration is an important aspect of the Z3Npi sound, so you can expect a wide variety of featured artists in his catalog. More than anything music is best when it’s combined with performances that accentuate the sounds – Z3Npi delivers not just a unique recorded sound but performances that take the music to the next level.

https://www.youtube.com/watch?v=NeDqEGUrRcg https://i0.wp.com/z3npi.com/wp-conte...74961283_n.jpg https://i0.wp.com/z3npi.com/wp-conte...1/02/image.png https://i2.wp.com/z3npi.com/wp-conte.../12/Church.jpg

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

MUS - Sunday - 00:00-00:59 PDT

Title: Music - Zebbler Encanti Experience
When: Sunday, Aug 8, 00:00 - 00:59 PDT
Where: Bally's Silver Ballroom

SpeakerBio: Zebbler Encanti Experience
Zebbler Encanti Experience (aka “ZEE”) is an audio/visual collaboration between video artist Zebbler and electronic music producer Encanti, based out of Boston, Massachusetts and Valencia, Spain. The Experience is an immersive performance of mapped visuals on three custom winged projection screens, synchronized with heavy peak-hour psychedelic bass music, resulting in the creation of a fantasy world for audiences to lose themselves in.

Zebbler Encanti Experience released a critically-acclaimed EP, End Trance, on standout bass label Wakaan, coupled with a performance at the inaugural Wakaan Festival. Coming out of the pandemic, ZEE released Syncorswim on longtime label Gravitas Recordings, which is a full audio-visual album exploring the ambient, glitchy, and IDM side of the project. Beautiful natural visuals accompany gorgeous, synth-heavy grooves. This different perspective gives fans a whole new look at what an A/V project can be.

ZEE have seen a considerable amount of road time in the last few years, serving as integral members of multiple tour teams. The architect behind the projection mapped projects for Shpongle and EOTO, and assisting with Infected Mushroom’s stage construction, Zebbler has toured the United States nonstop producing visual shows and performing as a VJ at hundreds of high profile events. In addition to ZEE performing as direct touring support for EOTO in venues throughout the country, and performing in the Shpongle Live band during their first few shows in the United States and final appearance at Red Rocks, Encanti has carved out some time to teach electronic music production to graduate students in the Valencia, Spain wing of Berklee College of Music.

https://zebblerencantiexperience.com/
https://facebook.com/zebblerencantiexperience https://instagram.com/zebblerencantiexperience
https://soundcloud.com/zebblerencantiexperience

Description: No Description available

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Saturday - 11:00-11:59 PDT

Title: My other car is your car: compromising the Tesla Model X keyless entry system
When: Saturday, Aug 7, 11:00 - 11:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Lennert Wouters
No BIO available

Description:

This talk covers a practical security evaluation of the Tesla Model X keyless entry system. We will cover the internal workings of the system, including the key fob, the body control module and the pairing protocol. Additionally, we detail our reverse engineering techniques and document several security issues. The identified issues in the key fob firmware update mechanism and the key fob pairing protocol allow us to bypass all of the cryptographic security measures put in place. Our proof-of-concept attack allows to unlock and start a Model X in a matter of minutes. The vulnerability in the key fob firmware update mechanism was fixed by Tesla using an OTA update.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=36AvYW48JtQ

Return to Index - Add to Google Calendar - ics Calendar file

CAHV - Saturday - 12:00-12:59 PDT

Title: National Service Panel
When: Saturday, Aug 7, 12:00 - 12:59 PDT
Where: Career Hacking Village (Talk)
Speakers: Amelie Koran,Elizabeth Schweinsberg,Joe Billingsley,Teri Williams

SpeakerBio: Amelie Koran , Senior Technology Advocate, Splunk
No BIO available

SpeakerBio: Elizabeth Schweinsberg
No BIO available

SpeakerBio: Joe Billingsley
No BIO available

SpeakerBio: Teri Williams
No BIO available

Description:
What background do you need to work with different federal agencies? Which ones have authorities for enforcing regulations, protecting different areas, or engaging adversaries? How do you get hired into the organization? Whether someone is just entering the workforce or wants to consider the options as part of career planning, our panel helps provide the insights and answer the questions you have. We draw from the US Digital Service, DHS CISA, NASA, Marine Corps Cyber Auxiliary, NSA, and other federal agencies. Join us on the Defcon Forums and let us know what questions you have for our panel.

This talk will be available on YouTube: https://www.youtube.com/watch?v=PqLEFsaFWes

Career Hacking Village content will be available on YouTube.

YouTube: https://youtube.com/careerhackingvillage

Return to Index - Add to Google Calendar - ics Calendar file

WS - Saturday - 15:00-18:59 PDT

Title: Network Analysis with Wireshark
When: Saturday, Aug 7, 15:00 - 18:59 PDT
Where: Workshops - Jubilee 2 (Onsite Only)
Speakers: Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman

SpeakerBio: Sam Bowne , Proprietor, Bowne Consulting
Sam Bowne has been teaching computer networking and security classes at CCSF since 2000. He has given talks and hands-on trainings at DEF CON, DEF CON China, HOPE, BSidesSF, BSidesLV, RSA, and many conferences and colleges.

SpeakerBio: Elizabeth Biddlecome , Consultant and Part-Time Instructor
Elizabeth Biddlecome is a consultant and a part-time instructor at City College San Francisco, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

SpeakerBio: Irvin Lemus , Cybersecurity Professor
Irvin Lemus has been in the industry for 10+ years as an MSP technician, consultant, instructor and coordinator. He is currently the cybersecurity professor at Cabrillo College in Santa Cruz, CA. He also is the Bay Area Cyber Competitions Regional Coordinator as well as the contest creator for SkillsUSA CA and FL. Irvin has spoken at various cybersecurity and educational conferences. Irvin holds a CISSP and a Bachelor's Degree in Information Security.

Irvin Lemus is an instructor at Cabrillo College, teaching cyber security courses for 3 years. Irvin runs the cybersecurity competition program for the Bay Area Community Colleges. He also creates the SkillsUSA Cybersecurity contests for California and Florida. He has Security+, CySA+, WCNA, CISSP.

SpeakerBio: Kaitlyn Handelman , Hacker
I like to hack stuff, and I'm like really good at computers.

Description:

Summarize what your training will cover, attendees will read this to get an idea of what they should know before training, and what they will learn after. Use this to section to broadly describe how technical your class is, what tools will be used, and what materials to read in advance to get the most out of your training. This abstract is the primary way people will be drawn to your session.

This workshop will introduce participants to Network Analysis by understanding Wireshark. Participants will learn to understand packet activity, abnormalities and anomalies to detect attacks, troubleshoot network problems, and perform network forensics. This workshop is structured as a CTF.

Registration Link: https://www.eventbrite.com/e/network-analysis-with-wireshark-tickets-162219979325

Prerequisites
Basic networking knowledge

Materials needed:
Any laptop with Wireshark installed.

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 12:00-12:30 PDT

Title: Never a dill moment: Exploiting machine learning pickle files
When: Saturday, Aug 7, 12:00 - 12:30 PDT
Where: AI Village (Virtual)

SpeakerBio: Suha Sabi Hussain
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Friday - 10:00-10:59 PDT

Title: New Face, Who Dis? Protecting Privacy in an Era of Surveillance
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: Crypto & Privacy Village (Virtual)

SpeakerBio: Mike Kiser
Mike Kiser is insecure. He has been this way since birth, despite holding a panoply of industry positions over the past 20 years—from the Office of the CTO to Security Strategist to Security Analyst to Security Architect—that might imply otherwise. In spite of this, he has designed, directed, and advised on large-scale security deployments for a global clientele. He is currently in a long-term relationship with fine haberdashery, is a chronic chronoptimist (look it up), and delights in needlessly convoluted verbiage. He speaks regularly at events such as the European Identity Conference and the RSA Conference, is a member of several standards groups, and has presented identity-related research at Black Hat and Def Con. He is currently a Senior Identity Strategist for SailPoint Technologies.

Description:

While it has its potential benefits, facial recognition is eroding privacy and other human rights. Over the past year, several organizations have acknowledged that they have “scraped” social media and similar sites for photos to build their biometric databases, and photos intended for personal use only have now been potentially weaponized.

Industry and government have ethical responsibilities to prevent this, but what if there were a way to enhance privacy for individuals without waiting for the cavalry? Adversarial technology can provide a way to protect this biometric, but it must be as easy to use as picking up their mobile device and taking a photo.

We’ll cover the last year in adversarial research, examining the pros and cons of each and working towards the introduction of a new open-source mobile app, “Ruse," that seeks to use adversarial strategies to make personal photos less useful for commercial facial recognition systems while retaining a (relatively) low impact on human usefulness.

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Saturday - 13:00-13:30 PDT

Title: New Hampshire SB43 Forensic Audit
When: Saturday, Aug 7, 13:00 - 13:30 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Harri Hursti
Co-Founder, DEF CON Voting Village; Founding Partner, Nordic Innovation Labs

Harri Hursti is considered one of the world’s foremost experts on the topic of electronic voting security, having served in all aspects of the industry sector. He is considered an authority on uncovering critical problems in electronic voting systems worldwide.

As a consultant, he has conducted and co-authored many studies, both academic and commercial, on various election systems’ data security and vulnerability. These studies have come at the request of officials, legislators and policy makers in 5 countries; including the U.S. government, at both the state and federal level.

Description:

Election security expert Harri Hursti will explain the process and findings from the 2020 post-election audit conducted in Windham, NH.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

Title: New Phishing Attacks Exploiting OAuth Authentication Flows
When: Saturday, Aug 7, 16:00 - 16:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Jenko Hwong
Jenko Hwong is on the Netskope Threat Research team, focusing on cloud threats/vectors. He's spent time in engineering and product roles at various security startups in vulnerability scanning, AV/AS, pen-testing/exploits, L3/4 appliances, threat intel, and windows security.
Twitter: @jenkohwong

Description:

OAuth 2.0 device authentication gives users on limited-input devices like TVs an easier way to authenticate against a cloud website/app by entering a code on a computer/phone. This authentication flow leads to new phishing attacks that: - do not need server infrastructure--the login page is served by the authorization provider using their domain and cert - do not require a client application--application identities can be reused/spoofed - do not require user consent of application permissions

Since the phish attacks hijack oauth session tokens, MFA will be ineffective as the attacker does not need to reauthenticate. The ability to defend against these attacks is hindered by limited info and functionality to detect, mitigate, and prevent session token compromise.

I'll demonstrate these new phishing attacks, access to sensitive user data, and lateral movement.

Defensive measures against these phishing attacks will be discussed, specifically the challenges in detection, mitigation, and prevention, and the overall lack of support for managing temporary credentials.

Open-source tools have been developed and will be used to demonstrate how users can: - self-phish their organizations using these techniques - audit security settings that help prevent/mitigate the attacks

REFERENCES

> 1.0 Evolving Phishing Attacks 1.1 A Big Catch: Cloud Phishing from Google App Engine and Azure App Service: https://www.netskope.com/blog/a-big-catch-cloud-phishing-from-google-app-engine-and-azure-app-service 1.2 Microsoft Seizes Malicious Domains Used in Mass Office 365 Attacks: https://threatpost.com/microsoft-seizes-domains-office-365-phishing-scam/157261/ 1.3 Phishing Attack Hijacks Office 365 Accounts Using OAuth Apps: https://www.bleepingcomputer.com/news/security/phishing-attack-hijacks-office-365-accounts-using-oauth-apps/ 1.4 Office 365 Phishing Attack Leverages Real-Time Active Directory Validation: https://threatpost.com/office-365-phishing-attack-leverages-real-time-active-directory-validation/159188/ 1.5 Demonstration - Illicit Consent Grant Attack in Azure AD: https://www.nixu.com/blog/demonstration-illicit-consent-grant-attack-azure-ad-office-365 https://securecloud.blog/2018/10/02/demonstration-illicit-consent-grant-attack-in-azure-ad-office-365/ 1.6 Detection and Mitigation of Illicit Consent Grant Attacks in Azure AD: https://www.cloud-architekt.net/detection-and-mitigation-consent-grant-attacks-azuread/ 1.7 HelSec Azure AD write-up: Phishing on Steroids with Azure AD Consent Extractor: https://securecloud.blog/2019/12/17/helsec-azure-ad-write-up-phishing-on-steroids-with-azure-ad-consent-extractor/ 1.8 Pawn Storm Abuses OAuth In Social Engineering Attack: https://www.trendmicro.com/en_us/research/17/d/pawn-storm-abuses-open-authentication-advanced-social-engineering-att

2.0 OAuth Device Code Flow
2.1 OAuth 2.0 RFC:
https://tools.ietf.org/html/rfc6749#page-24 2.2 OAuth 2.0 for TV and Limited-Input Device Applications: https://developers.google.com/identity/protocols/oauth2/limited-input-device 2.3 OAuth 2.0 Scopes for Google APIs:

https://developers.google.com/identity/protocols/oauth2/scopes 2.2 Introducing a new phishing technique for compomising Office 365 accounts: https://o365blog.com/post/phishing/#oauth-consent 2.3. Office Device Code Phishing: https://gist.github.com/Mr-Un1k0d3r/afef5a80cb72dfeaa78d14465fb0d333

3.0 Additional OAuth Research Areas
3.1 Poor OAuth implementation leaves millions at risk of stolen data: https://searchsecurity.techtarget.com/news/450402565/Poor-OAuth-implementation-leaves-millions-at-risk-of-stolen-data 3.2 How did a full access OAuth token get issued to the Pokémon GO app?: https://searchsecurity.techtarget.com/answer/How-did-a-full-access-OAuth-token-get-issued-to-the-Pokemon-GO-app

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=9slRYvpKHp4

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20J

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Friday - 16:00-16:59 PDT

Title: No Aggregation Without Representation
When: Friday, Aug 6, 16:00 - 16:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Andrea Downing , Light Collective, Co-Founder
Andrea Downing is a BRCA Community Data Organizer and an ePatient security researcher. In 2018, Andrea discovered a security vulnerability (SICGRL) which affected the privacy and safety of all closed groups on Facebook and launched a congressional inquiry.
Twitter: @BraveBosom

Description:
As we emerge from a pandemic and a year where we all became at risk of developing COVID, many of us have become patients and caregivers navigating a healthcare system under siege. With the rise in ransomware attacks on hospitals, disinformation campaigns from state actors on social media, and new biosecurity threats there has never been a greater need to develop capacity for a new kind of immune response to emerging threats in digital health. Representation matters. During this talk, BRCA mutant turned Security Researcher share how patient communities - namely "the ePatient movement" - holds potential to bring a new type of representation to the field of cybersecurity. ePatients with disabilities have superpowers to co-design and co-production of new technologies with fresh eyes - and to help us protect the emerging technologies that have the power to cure or kill.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 12:00-12:45 PDT

Title: No Key? No PIN? No Combo? No Problem! P0wning ATMs For Fun and Profit
When: Sunday, Aug 8, 12:00 - 12:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Roy Davis
Roy Davis is a security researcher and engineer with 15 years of pentesting, security research and programming experience. He has worked on security teams at Zoom, Salesforce, Apple, Barclays Bank, and Thomson Reuters. He holds a B.S. degree in Computer Science from Purdue University and an M.S. in Cybersecurity and Digital Forensics from WGU. Roy has presented at several security conferences from 2008 to his most recent talk at the "HackerOne Security@" conference in San Francisco.

https://www.linkedin.com/in/roy-davis/

Twitter: @hack_all_things
https://www.davisinfosec.com

Description:

Since the late great Barnaby Jack gave us "Jack Potting" in the late 2000s, there have been several talks on ATM network attacks, USB port attacks, and digital locks attacks which apply to several brands of ATM safes. In this session, I'll discuss and demonstrate how most of these known attack vectors have been remediated, while several fairly simple attacks against the machine and the safe still remain. We'll dive into how ATMs work, the steps I went through to become a "licenced ATM operator" which enabled my research, and how I identified the vulnerabilities. I'll show how, with very little technical expertise and 20 minutes, these attacks lead directly past "secure" and allow attackers to collect a lot more than $200.

REFERENCES
Barnaby Jack - "Jackpotting Automated Teller Machines" - (2010) from DEFCON - https://www.youtube.com/watch?v=FkteGFfvwJ0 Weston Hecker - "Hacking Next-Gen ATM's From Capture to Cashout" - (2016) from DEFCON - https://www.youtube.com/watch?v=1iPAzBcMmqA Trey Keown and Brenda So - "Applied Cash Eviction through ATM Exploitation" (2020) from DEFCON - https://www.youtube.com/watch?v=dJNLBfPo2V8 Triton - "Terminal Communications Protocol And Message Format Specification" (2004) from Complete ATM Services - tinyurl.com/7nf2fdy5 Rocket ATM - "Hyosung ATM Setup Part 1 - Step by Step" (2018) from Rocket ATM - https://www.youtube.com/watch?v=abylmrBkOGM&t=3s Rocket ATM - "Hyosung ATM Setup Part 2 - Step by Step" (2018) from Rocket ATM - https://www.youtube.com/watch?v=IM9ZG46fwL8 Hyosung - "NH2600 Service Manual v1.0" (2013) From Prineta - https://tinyurl.com/c6jd4hd9 Hyosung - "NH2700 Operator Manual v1.2" (2010) From AtmEquipment.com - https://tinyurl.com/rp2cad8

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=9cG-JL0LHYw

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20R

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Saturday - 12:00-12:59 PDT

Title: Not so Passive: Vehicle Identification and Tracking via Passive Keyless Entry
When: Saturday, Aug 7, 12:00 - 12:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Nick Ashworth
No BIO available
Twitter: @zeetw11

Description:
Attacks on the passive keyless entry system have been around for a while, with most focused on gaining physical access to the vehicle. We have developed a new attack, Marco, that instead focuses on identifying and tracking vehicles by exploiting weaknesses in passive keyless entry systems. This attack works similar to a cooperative radar system, where the attacker transmits an interrogation message, and any nearby key fob will automatically respond. The attacker can then use these responses to identify and track key fobs either generically, such as all fobs of the same make and model of vehicle, or specifically, such as a key fob with a specific identifier.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=aiSA4QdF4m8

Return to Index - Add to Google Calendar - ics Calendar file

Title: Offensive Golang Bonanza: Writing Golang Malware

When: Saturday, Aug 7, 18:00 - 18:45 PDT

Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Benjamin Kurtz , Hacker
Ben Kurtz is a hacker, a hardware enthusiast, and the host of the Hack the Planet podcast (https://symbolcrash.com/podcast). After his first talk, at DefCon 13, he ditched development and started a long career in security. He has been a pentester for IOActive, head of security for an MMO company, and on the internal pentest team for the Xbox One at Microsoft. Along the way, he volunteered on anti-censorship projects, which resulted in his conversion to Golang and the development of the ratnet project (https://github.com/awgh/ratnet). A few years ago, he co-founded the Binject group to develop core offensive components for Golang-based malware, and Symbol Crash, which focuses on sharing hacker knowledge through trainings for red teams, a free monthly Hardware Hacking workshop in Seattle, and podcasts. He is currently developing a ratnet-based handheld device for mobile encrypted mesh messenging, planned for release next year.
Twitter: @symbolcrash1
symbolcrash.com

Description:

The past two years have seen the rise of Golang-based malware from its beginnings as a way to win at CCDC and red team engagements to its current use by actual threat actors. This talk will break down why Golang is so useful for malware with a detailed tour through the available components used for exploitation, EDR and NIDS evasion, and post-exploitation, by one of the main authors of the core components. Although focused on the offensive perspective, there will be valuable insights into the challenges in detecting Golang malware. Interested in learning Golang? Interested in writing or detecting malware? This is your invitation into the weird and wonderful world of Golang malware.

REFERENCES

List of Golang Security Tools:
https://github.com/Binject/awesome-go-security

C-Sto:
https://github.com/c-sto/goWMIExec
https://github.com/C-Sto/BananaPhone
https://github.com/C-Sto/gosecretsdump

capnspacehook
https://github.com/capnspacehook/pandorasbox https://github.com/capnspacehook/taskmaster

Vyrus / gscript crew:
https://github.com/gen0cide/gscript
https://github.com/vyrus001/go-mimikatz https://github.com/vyrus001/msflib

secretsquirrel / Josh Pitts:
https://github.com/secretsquirrel/the-backdoor-factory https://github.com/Genetic-Malware/Ebowla
https://github.com/secretsquirrel/SigThief https://github.com/golang/go/issues/16292

malwareunicorn on OSX loading:
https://malwareunicorn.org/workshops/macos_dylib_injection.html

Misc
https://github.com/sassoftware/relic https://github.com/EgeBalci/sgn https://github.com/moonD4rk/HackBrowserData
https://github.com/emperorcow/go-netscan https://github.com/CUCyber/ja3transport

https://github.com/swarley7/padoracle

Command and Control:
https://github.com/BishopFox/sliver
https://github.com/DeimosC2/DeimosC2
https://github.com/t94j0/satellite

Obfuscation/RE:
https://github.com/unixpickle/gobfuscate https://github.com/mvdan/garble
https://github.com/goretk/redress

Of interest for defense, but breaks Docker & Terraform: https://github.com/unsecureio/gokiller

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=3RQb05ITSyk

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20E

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 14:00-14:45 PDT

Title: Old MacDonald Had a Barcode, E-I-E-I CAR
When: Sunday, Aug 8, 14:00 - 14:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Richard Henderson
Richard Henderson is a writer, researcher, and ham radio/electronics nerd who has worked in infosec and technology for almost two decades. Richard has taught multiple times at DEF CON and leads the annual DEF CON Ham Radio Fox Hunt Contest. Richard is currently co-authoring a book on cybersecurity for ICS/Scada systems.
Twitter: @richsentme

Description:

For decades, the EICAR test string has been used by antivirus and security vendors to safely test their detection engines without having to use live virulent samples which could cause harm. What would happen if you took that string, encoded it into a machine readable format like a QR code and started scanning various devices with the QR code? This talk shows how there are a lot of systems out there that aren't expecting an input string like EICAR and how many of them just collapse when shown the code. We will also discuss the types of systems you can target and how you may be able to extend this to more than a nuisance attack.

REFERENCES

> EICAR test string: https://www.eicar.org/?page_id=3950 EICAR wikipedia entry: https://en.wikipedia.org/wiki/EICAR_test_file QR codes: https://en.wikipedia.org/wiki/QR_code Risks surrounding QR codes: https://en.wikipedia.org/wiki/QR_code#Risks

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=cIcbAMO6sxo

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20R

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Saturday - 14:35-16:59 PDT

Title: Onions In the Cloud Make the CISO Proud (Workshop)
When: Saturday, Aug 7, 14:35 - 16:59 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Wes Lambert
Wes Lambert is the Director of Support and Professional Services at Security Onion Solutions, where he helps customers to implement enterprise security monitoring solutions and understand their computer networks. A huge fan of OSS projects, Wes loves to solve problems and enhance security using completely free and easily deployable tools.
Twitter: @therealwlambert

Description:

It's been said that 94% of enterprises already use a cloud service, and that 30% of all IT budgets are allocated to cloud computing. What does this mean for network defenders? It means that many organizations are invested in the cloud, and unfortunately, many organizations still have little visibility into inter-instance, instance-to-internet, and control plane activity, as well as management functions and bucket access within the cloud. While some of this activity may be logged, it may not be analyzed or aggregated for quick review. In this workshop, we'll cover how Security Onion, a completely free and open platform for intrusion detection, enterprise security monitoring, and log management can be leveraged to increase visibility in the cloud. By using Security Onion, defenders can facilitate effective threat detection and ease compliance efforts. Attendees should walk away with an understanding of how they can utilize Security Onion to find evil in their cloud environments and make their adversaries cry. Outline:

- Introduction to the Cloud
    - Asset/Threats
    - Monitoring Challenges
- Introduction to Security Onion
    - Components and Data Collected
- Security Onion in the Cloud
    - Traffic Mirroring
    - Cloud Telemetry
    - Deployment

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

Title: Open Bridge
When: Friday, Aug 6, 14:00 - 15:50 PDT
Where: Palace 1+2

SpeakerBio: Constantine Macris
No BIO available

Description:
Tool or Project Name: Open Bridge Simulator

Short Abstract:
Open Bridge Simulator provides a platform to explore the NMEA 2000 protocol, maritime electronics and CAN interfaces in a cost effective (under $50) software/hardware suite.

Short Developer Bio:
Constantine is an instructor at the US Coast Guard Academy where he teaches Cyber Systems. On the side he breaks things...

URL to any additional information: https://github.com/thedini/openBridge

Detailed Explanation of Tool:
Over the years I have built various tools that pull data from and put data on the NMEA 2000 maritime electronics bus. From talking boats (Twitter @CES_bigAl) to a network of connected recreational vessels. It was always a struggle because of the somewhat obscure nature of the application (boats/yachts/ships) and the difficulty and cost in obtaining hardware and tools to learn about the systems. Open Bridge Simulator is an open source project (software and eventually hardware) that aims to make this process more cost effective and obtainable to individuals without $10,000 laying around to purchase expensive maritime electronics.

The demo lab will involve:
Reviewing the NMEA 2000 protocol
Seeing the simulator and estimated cost of the system produced by the US Coast Guard Academy Capstone team (an example of an expensive solution) Reviewing the architecture of a standard NMEA 2000 network (with live devices) The traditional means of interacting with the NEMA 2000 network An introduction and demo of the Open Bridge Simulator software and hardware I also intend to cover some of the challenges we faced in developing this project as well as ways we can work together to make learning about NMEA 2000 more inclusive.

The general project will be using off the shelf hardware (Teensy 4.1, WCMCU-230 Can Transceiver) to interface with Docker containers that simulate different marine electronics so a user with less than $50 in hardware can simulate an entire bridge system on almost any computer. The project is designed to be a framework to allow individuals to share the devices they build and create a library of bridge systems that can be connected to simulate industry accurate systems.

This project can stand alone or interface with an existing system and can act as an educational tool, defense and simulation tool or prove out attacks.

The overall goal of Open Bridge Simulator is to make playing with NMEA 2000 easier!

Target Audience: Hardware, Education, Defense

The purpose of this project is to make learning and playing with NMEA2000 more reasonable and affordable for beginners and those without access to expensive hardware (like GPS head units). I think that reducing the cost and barrier to entry will bring more people into the space and shine a light onto a somewhat obscure and difficult area to get started.

BHV - Friday - 14:30-14:59 PDT

Title: Open-Source Vaccine Developer Kits (VDKs) with RaDVaC
When: Friday, Aug 6, 14:30 - 14:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Alex Hoekstra
No BIO available

Description:
Vaccine development has traditionally been an expensive and thus primarily proprietary endeavor. Tools to decrease costs, increase adaptability, speed of production, speed of testing, and expand access to could help increase participation, collaboration, innovation, infectious disease biosecurity, and equity in vaccine development and ultimately vaccine deployment globally. Open-Source VDKs could fill a vital and underserved niche in the ecosystem or vaccine development.

RaDVaC is building tools to increase participation in vaccine development. Key features of a useful vaccine developer kit (VDK) include technical specs for vaccine candidate design, production, testing, adaptation, and collaboration. The ecosystem of vaccine development is weaker for a lack of open-source toolkits (open-source infrastructure is an investment in anti-fragility).

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-17:30 PDT

Title: OpenSOC Blue Team CTF
When: Friday, Aug 6, 10:00 - 17:30 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/238017

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 09:00-15:59 PDT

Title: OpenSOC Blue Team CTF
When: Saturday, Aug 7, 09:00 - 15:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/238017

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 14:00-14:59 PDT

Title: Operation Bypass: Catch My Payload If You Can
When: Saturday, Aug 7, 14:00 - 14:59 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Matthew Eidelberg , Technical Manager, Optiv
Matthew Eidelberg is a Technical Manager in Optiv’s Threat Management Team (Attack and Penetration specialization). Matthew has over 8 years’ experience in both consulting and information security. Matthew’s primary role is focused on leading Threat Management’s Adversary Simulation Services which focus on physical, red/purple team, and other advanced assessments.

Matthew’s expertise also involves research development, focusing on developing new techniques and tooling for endpoint security bypass and evasion. Matthew’s experience working in enterprise networks has also given him a deep understanding of the business operations.

https://ca.linkedin.com/in/matthew-eidelberg-b0422997/

Description:

Endpoint Detection and Response (EDR) have become the punching bags of the security world. Attackers employ sophisticated techniques to circumvent these controls and as a result, there has been a driving need for defenders to detect and prevent these attacks... but are they sufficient? This talk will go over all the operational considerations and tradecraft theory I've developed over the past few years when evading EDRs and other endpoint controls. This will primarily focus on techniques to ensure command and controls servers are not easily detected and contain virtually no Indicators of Compromise. This talk will then deep dive into the inner workings of the EDR bypassing framework ScareCrow,highlighting some of the lesser-known techniques and new features that are available to red teamers and pentesters. By the end of this talk, the audience should walk away with a detailed understanding of how to use ScareCrow and other opsec considerations to avoid being detected by endpoint controls and blue teams.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Friday - 12:15-12:59 PDT

Title: OSINT and the Hermit Kingdom. Leveraging online sources to learn more about the worlds most secret nation
When: Friday, Aug 6, 12:15 - 12:59 PDT
Where: Recon Village (Virtual)

SpeakerBio: Nick Roy
Nick Roy (Twitter: @superducktoes) currently works for a global security vendor creating training content and researching new attacker patterns and techniques. Previously he worked at an automation platform startup teaching people about the joys and benefits of automation. While not working he lives in Boston with his wife and two cats hunting out the best dive bars in Boston and solving math problems on college chalkboards overnight.
Twitter: @superducktoes

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Saturday - 15:20-16:05 PDT

Title: OSINT for Sex Workers
When: Saturday, Aug 7, 15:20 - 16:05 PDT
Where: Recon Village (Virtual)

SpeakerBio: Kala Kinyon
No BIO available
Twitter: @TankKala

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Saturday - 10:00-10:55 PDT

Title: OSINT Tales: What the Public Knows About Russia’s New Mega-Submarine
When: Saturday, Aug 7, 10:00 - 10:55 PDT
Where: Hack the Sea (Virtual)

SpeakerBio:H I Sutton
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 14:00-14:45 PDT

Title: Over-the-air remote code execution on the DEF CON 27 badge via Near Field Magnetic Inductance or World's first NFMI exploitation, sorta or OTARCEDC27NFMIOMGWTFBBQ

When: Saturday, Aug 7, 14:00 - 14:45 PDT

Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Seth Kintigh
Seth Kintigh learned to program at age 12 on an IBM PC jr and his grandmother taught him how to crack ciphers. His first hack was to get infinite lives and beat the Atari 2600 game Solaris. He earned a BS EE with minors in CS and physics and a MS EE with concentration in cryptography and information security from WPI. He worked 6 years as a hardware engineer and 17 in security. Hobbies include cracking historical ciphers and restoring a Victorian home

Description:

The DEF CON 27 badge employed an obscure form of wireless communication: Near Field Magnetic Inductance (NFMI). The badges were part of a contest and while poking through the firmware for hints I noticed a buffer overflow flaw. All it required to exploit it was an oversized packet… via a chip with no datasheet and no documentation on the proprietary protocol. Thus started a 2 year odyssey.

I used Software Defined Radio tools to study the signal's modulations. I built a receiver in GNURadio and Python to convert signals into symbols, symbols obfuscated by a pattern that I had to deduce while only controlling a fraction of the bytes. Data was encoded in those symbols using proprietary convolution for even bits and Trellis Code Modulation for odd bits. I then reversed their bizarre CRC and wrote tools to craft and send packets. Using those tools I chained bugs in 2 chips and remotely crashed the badge. However, limitations in the NFMI protocol made more sophisticated attacks impossible.

But after a year and a half invested, I was not about to give up. I soldered leads to middle layer traces, extracted and reverse engineered the NFMI firmware, fixed their protocol, and patched a badge FW to patch the NFMI FW. At long last I achieved what may be the world's first, over-the-air, remote code exploit via NFMI.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=sDCIjcUEFj0&

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20S

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 15:00-16:45 PDT

Title: OWASP & CSA IoT: Impacting Medical Security
When: Saturday, Aug 7, 15:00 - 16:45 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Aaron Guzman , OWASP Project Leader
Aaron Guzman is co-author of IoT Penetration Testing Cookbook and Product Security Lead with Cisco Meraki. He spends his days building security into IoT products and crafting designs that keep users safe from compromise. A co-chair of Cloud Security Alliance's IoT Working Group and a technical reviewer for several published security books, he also spearheads many open-source initiatives, raising awareness about IoT hacking and proactive defensive strategies under OWASP's IoT and Embedded Application Security projects. He has extensive public speaking experience, delivering conference presentations, training, and workshops globally. Follow Aaron on Twitter @scriptingxss.
Twitter: @scriptingxss

Description:

The Open Web Application Security Project (OWASP) IoT Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things as well as enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies. Similarly, CSA's IoT Working group is dedicated to understanding IoT deployments and defining actionable guidance to secure ecosystems. Their efforts are often used to develop medical security guidelines for developers and manufacturers alike but also to influence IoT security assessment methodologies for later use on commercial IoT certification schemes. This session will provide insights into current project initiatives, including those that directly impact medical devices and how you can save lives by getting involved.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Friday - 20:00-20:59 PDT

Title: Panel discussion: Adversary simulation, emulation or purple teaming - How would you define it?
When: Friday, Aug 6, 20:00 - 20:59 PDT
Where: Adversary Village (Virtual)
Speakers: Tomer Bar,Samuel Kimmons,Anant Shrivastava,Vincent Yiu,Martin Ingesen,Joe Vest

SpeakerBio: Tomer Bar
Tomer Bar is hands-on security researcher and head of research manager with ~20 years of unique experience in the cyber security. In the Past, he ran research groups for the Israeli government and then lead the endpoint malware research for Palo Alto Networks. Currently, he leads the SafeBreach Labs research which is the research and development arm of SafeBreach.

His main interest is focused on Windows vulnerability research, reverse engineering and APT research.

His recent discoveries are vulnerabilities in the Windows Spooler mechansim and a research on the most persistent Iranian APT campaign. He is a contributor to Mitre Attack framework and a Speaker at BlackHat, Defcon and Sector conferences.

SpeakerBio: Samuel Kimmons
Samuel Kimmons is Red Teamer at Cognizant. He is responsible for researching, planning, and developing full scope Red Team engagements. Samuel got is start in Information Security during his time in the United States Air Force (USAF). While in the USAF he stood up the first interal red team at the United States Air Force Computer Emergency Response Team (AFCERT). His team's primary purpose was to emulate threat actors in order to increase the accuracy of detection capabilities.
https://www.linkedin.com/in/kimmons

SpeakerBio: Anant Shrivastava
No BIO available

SpeakerBio: Vincent Yiu
No BIO available

SpeakerBio: Martin Ingesen
No BIO available

SpeakerBio: Joe Vest
No BIO available

Description: No Description available

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 20:30-21:30 PDT

Title: Panel discussion: Is Adversary Emulation Too ___ For You?
When: Saturday, Aug 7, 20:30 - 21:30 PDT
Where: Adversary Village (Virtual)
Speakers: Jamie Williams,Cat Self,Tim Schulz,Michael Long,Frank Duff,Jose Barajas

SpeakerBio: Jamie Williams , Principal Adversary Emulation Engineer – The MITRE Corporation
Jamie Williams is an engineer at MITRE where he works on various exciting efforts involving security operations and research, specializing in adversary emulation and behavior-based detections. He also leads teams that help shape and deliver the “adversary-touch” within MITRE ATT&CK· and ATT&CK Evaluations.

SpeakerBio: Cat Self , Lead Cyber Adversarial Engineer – The MITRE Corporation
Cat Self is a Lead Cyber Adversarial Engineer working on MITRE ATT&CK· and ATT&CK Evaluations teams at MITRE. Cat previously worked at Target as a red team operator, threat hunter, and developer. Cat is an Army Military Intelligence veteran with a passion for mentorship, hiking in foreign lands, and finding opportunities to give back.

SpeakerBio: Tim Schulz , Adversary Emulation Lead - SCYTHE
Tim Schulz is SCYTHE’s Adversary Emulation Lead. He has been helping organizations build and train teams to understand and emulate cyber threats for the last seven years while working at multiple FFRDCs. He is the author of the Purple Maturity Model, and has given talks on purple teaming, adversary emulation, security testing, and technical leadership.

SpeakerBio: Michael Long , Capability Area Lead for Cyber Adversary Emulation – The MITRE Corporation
Michael Long is a Principal Adversary Emulation Engineer at the MITRE Corporation and a former U.S. Army Cyber Operations Specialist. Michael has over 10 years’ experience in offensive and defensive cyber operations. With MITRE, Michael leads adversary emulation activities for ATT&CK Evaluations. Michael is also an instructor for MITRE ATT&CK Defender’s upcoming ATT&CK Adversary Emulation course.

SpeakerBio: Frank Duff , Director of ATT&CK Evaluations - MITRE Engenuity
Frank Duff is the General Manager for MITRE Engenuity's ATT&CK Evaluations. Frank has spent over 15 years at the MITRE Corporation, starting in radar signal analysis and then transitioning to cyber security. He was on the forefront of early endpoint detection and response research, before leading a team responsible for developing and executing test methodologies. He now leverages this experience to foster public-private partnerships to drive organizational security and product improvement.

SpeakerBio: Jose Barajas
No BIO available

Description: No Description available

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Sunday - 10:00-10:59 PDT

Title: Panel discussion: Resilient cyber space: The role of hacker and security communities

When: Sunday, Aug 8, 10:00 - 10:59 PDT

Where: Adversary Village (Virtual)

Speakers: Abhijith B R,Jay Turla,Manu Zacharia,Aseem Jakhar,Omar Santos,Dave Lewis,Dhillon 'L33tdawg' Kannabhiran

SpeakerBio: Abhijith B R
No BIO available

SpeakerBio: Jay Turla , Manager, Security Operations at Bugcrowd
Jay Turla is a Manager, Security operations at Bugcrowd Inc., and one of the goons of ROOTCON. He has been acknowledged and rewarded by Facebook, Adobe, Yahoo, Microsoft, Mozilla, etc. for his responsible disclosures. He has also contributed auxiliary and exploit modules to the Metasploit Framework: Host Header Injection Detection, BisonWare BisonFTP Server Buffer Overflow, Zemra Botnet CnC Web Panel Remote Code Execution, Simple Backdoor Shell Remote Code Execution, w3tw0rk / Pitbul IRC Bot Remote Code Execution, etc. He used to work for HP Fortify where he performs Vulnerability Assessment, Remediation and Advance Testing.

SpeakerBio: Manu Zacharia , President at ISRA, Founder of c0c0n International Hacking & Information Security Conference
Information Security evangelist with more than 23 years of professional experience. CEO – HackIT Technology and Advisory Services (Singapore, India, UAE) - www.hackit.co. External Consultant to Kerala State IT Mission / Computer Emergency Response Team (Kerala) – CERT-K from Feb 2016 to Jul 2016. Awarded the prestigious Microsoft Most Valuable Professional - MVP award consecutively for four years (2009, 2010, 2011 and 2012) in Enterprise Security stream. Also honored with the prestigious Asia Pacific Information Security Leadership Achievements Award for 2010 from (ISC) under Senior Information Security Professional Category. Awarded the Nullcon Black Shield Awards for 2014 under the Community Star category for contribution to community in terms of knowledge sharing, administration, communication, proliferation. Founder of c0c0n International Hacking & Information Security Conference and also Information Security Day Initiatives.

SpeakerBio: Aseem Jakhar , Co-founder/Director R&D - Payatu, Nullcon, Hardwear.io, EXPLIoT
Aseem Jakhar is the Director, research at Payatu Software Labs http://payatu.com a boutique security testing company specializing in IoT, Embedded, cloud, mobile security testing. He is the founder of null-The open security community, registered not-for-profit organization http://null.co.in and also the founder of nullcon security conference http://nullcon.net and hardwear.io security conference. He has worked on various security software including UTM appliances, messaging/security appliances, anti-spam engine, anti-virus software, bayesian engine to name a few. He currently spends his time researching on IoT security and hacking things. He is an active speaker and trainer at security conferences like AusCERT, Black Hat, Brucon, Defcon, Hack.lu, Hack in Paris, Hack In The Box, PHDays and many more. He has authored various open source security software including - ExplIoT - IoT Exploitation Framework - DIVA (Damn Insecure and Vulnerable App) for Android - Jugaad/Indroid - Linux Thread injection kit for x86 and ARM - Dexfuzzer - Dex file format fuzzer

SpeakerBio: Omar Santos , Principal Engineer, Cisco PSIRT, DEF CON Red Team Village
Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure. Omar is the author of over 20 books and video courses; numerous white papers, articles, and security configuration guidelines and best practices. Omar is a Principal Engineer of Cisco's Product Security Incident Response Team (PSIRT) where he mentors and lead engineers and incident managers during the investigation and resolution of security vulnerabilities.

Omar has been quoted by numerous media outlets, such as TheRegister, Wired, ZDNet, ThreatPost, CyberScoop, TechCrunch, Fortune Magazine, Ars Technica, and more.

SpeakerBio: Dave Lewis , Global Advisory CISO for CISCO
Dave Lewis has twenty five years+ of industry experience. He has extensive experience in IT security operations and management including a decade dealing with critical infrastructure security. Lewis is a Global Advisory CISO for Cisco. He is the founder of the security site Liquidmatrix Security Digest and cohost of the Liquidmatrix podcast as well as the host of the Plaintext and Murder Board podcasts. Lewis serves on the advisory boards for several firms. He is currently enrolled in a graduate program at Harvard University. Lewis has written columns for Daily Swig, Forbes and several other publications

SpeakerBio: Dhillon ‘L33tdawg’ Kannabhiran , Founder, CEO at Hack In The Box
Dhillon Andrew Kannabhiran (@l33tdawg on Twitter) is the Founder and Chief Executive Officer of Hack in The Box, organiser of the HITBSecConf series of network security conferences which has been held annually for over a decade in various countries including Malaysia, The Netherlands, The UAE and now China!

Description:
How do security communities help the information security industry and professionals? Why does the security industry need open security communities and forums? The relevance of such communities in standardizing Vulnerability disclosures Building frameworks and tools etc

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

Title: ParseAndC
When: Saturday, Aug 7, 14:00 - 15:50 PDT
Where: DemoLab Video Channel 1

SpeakerBio: Parbati Kumar Manna
Parbati Kumar Manna got his Bachelor of Technology from Indian Institute of Technology, Kharagpur in 1997. After spending a bit of time in the software industry, he went back to school to earn his MS and PhD in Computer Science from University of Florida in 2008. His dissertation involved the creation and detection of some of the smartest malware (particularly internet worms) that leave minimal footprint during their spread yet propagate at the maximal speed. After his PhD he joined the premier security group within Intel, working with other like-minded security researchers looking over the security of various Intel products, including hardware, firmware and software. He has published and reviewed in eminent conferences and journals.

Description:

ParseAndC - A Universal Parser and Data Visualization Tool for Security Testing

Short Abstract:
Parsing is the process of extracting the data values of various fields by mapping the data format (known) onto the datastream (known) from a certain offset (known). Parsing is often an integral part of hacking - even when we do not know the exact format of the data, we still have some vague idea, and we want to parse the data based on our assumed data format to see if our hunch is true. While it is trivial to write a parser that will output the values corresponding to the fields of a single C structure, that parser becomes useless if now we have to deal with a different C structure. A parser that can handle any and all C structures as its input is essentially a compiler, since even C header files contain enough complexity (#define constants, macros calling macros, variadic macros, conditional code via **if-**else etc., included files, packed/aligned attributes, pragmas, bitfield, complex variable declarations, nested and anonymous structure declaration etc.). This tool is capable of mapping any C structure(s) to any datastream from any offset, and then visually displaying the 1:1 correspondence between the variables and the data in a very colorful, intuitive display so that it becomes very easy to understand which field has what value.

This tool is extremely portable - it is a single 800KB Python text file, supports all versions of Python, is cross-platform (Windows/Mac/Unix), and also works in the terminal /batch mode without GUI. For multi-byte datatypes (e.g. integer or float) it supports both endianness (little/big) and displays value in both decimal and Hex formats. The tool needs no internet connection and works fully offline. It is self-contained - it doesn't import almost anything, to the extent that it implements its own C compiler (front-end) from scratch!!

This tool is useful for both security- and non-security testing alike (reverse engineering, network traffic analyzing, packet processing etc.). It is currently being widely used at Intel, and in the users' own words, this tool has reduced their days' work into minutes. The author of this tool led many security hackathons at Intel and there this tool was found to be very useful.

Short Developer Bio:
Parbati Kumar Manna got his Bachelor of Technology from Indian Institute of Technology, Kharagpur in 1997. After spending a bit of time in the software industry, he went back to school to earn his MS and PhD in Computer Science from University of Florida in 2008. His dissertation involved the creation and detection of some of the smartest malware (particularly internet worms) that leave minimal footprint during their spread yet propagate at the maximal speed. After his PhD he joined the premier security group within Intel, working with other like-minded security researchers looking over the security of various Intel products, including hardware, firmware and software. He has published and reviewed in eminent conferences and journals.

URL to any additional information:
The tool has just been open-sourced, but no public announcement has been made (don't want to steal the thunder from DEFCON) https://github.com/intel/ParseAndC

Detailed Explanation of Tool:
If one knows the data format of any datastream (basically, if you have access to the source code), parsing is easy since it takes <5 minutes to write a parser for a C structure. However, if one's job involves looking at many different datastreams, each with a different data format (basically, a different C structure), then this process becomes very tedious as you have to write a fresh parser for every new structure. As part of the Intel's in-house core hacking team, this author faced this very problem where he had to parse many different datastreams based on their individual data formats. So, to rid himself of the trouble of writing a new parser every time, he chose to write a tool that can parse any datastream with any data format (a C structure) with just two clicks.

The other big problem that this tool handles is the data visualization. The problem is, not every time we have a 1:1 mapping between code and data - we can have one-to-many relationship (for arrays), and can have many-to-one relationship (many union members pointing to same chunk of data). For example, if we have a single line of code like int a[30][40][50];, suddenly for a single line of code we have sixty thousand chucks of 4-byte data. This tool handles these many-to-one and one-to-many relationships between code and data very gracefully (just try hovering your cursor over the variables in the Interpreted code window or the data windows, and you will see). Also, if you double-click on any variable, it will re-display the datastream centered around the place where the variable maps to. Similarly, if you double-click on any data byte, it will scroll the Interpreted code window to pinpoint to the variable(s) that map to that data.

You can see all that just by clicking the "Run Demo" button on the tool. :-)

Supporting Files, Code, etc:
The tools needs no supporting file to run. To show its capability, just run the Demo (see below how). There is a huge README explaining everything right at the top of the script itself (the same README is also available in the Open Source repo https://github.com/intel/ParseAndC), but in case you don't have time to read that, below is a TL;DR version.

Just download the tool source (a single Python file) anywhere (Windows/Linux/Mac), run it using Python 2 or 3, and click on the "Run Demo" button on top right corner. It will load a datafile (the tool script itself), choose a builtin data format (expressed via C structures and variable declarations), compile/Interpret that code and finally map the variables in the data format onto the data file. Once this happens, the Interpreted code window and the Data window will contain colorful items. Just hover your cursor over those colorful items (or double-click) and see the magic happen!

There is also a bottom window which lays out a Tree-like view of the data format. You can expand/collapse all the structures and arrays in the data format here using left/right arrows (or mouse click).

It also creates a snapshot.csv file with all the data format variables with their values. It also prints the same in the background (console).

The tool is currently in Beta stage (a lot of new features have been added lately), but it will absolutely be mature during the actual conference time.

Target Audience:
The target audience for this tool is pretty broad - it involves both White Hat and Black Hat researchers alike. Basically, anybody who tests C programs, or reverse engineers any datastream produced from a C program will find this tool extremely useful. Examples of actual usage of this tool are noted below.

White Hat Testing (has access to source code): At Intel, of course we have access to our own source code, so we do not need to speculate about the data format of Intel products. In Intel, this tool has found its wide usage in driver testing, network packet analyzing, firmware reversing etc. where the testers use this tool to confirm that we are indeed observing the intended value in the datastream.

Black Hat Testing (no access to source code): An example of how this tool is useful for even Black Hat hackers is as follows. Suppose you believe that a certain executable or datastream should begin with a certain magic number, followed by version number, followed by a header, followed by data etc. So, you can just write a C structure corresponding to your "hunch", and then use this tool to map that hypothetical structure onto the datastream to see if the values corresponding to the fields "make sense" visually. This is where the visualization part of this tool comes as immensely useful - you can hover your cursor on top of any variable and see its corresponding data value, or hover your cursor over any data byte and see its corresponding variable(s). If some of the supposed fields in the structure make sense but others do not, you know for which fields you have hit the jackpot, and for which you didn't. So, you modify your structure accordingly and just two more clicks will give you the new visualization of the mapped data with the new structure. This way, you can use this tool iteratively to figure out the format of the datastream.

To summarize, this is a tool that has been widely used at Intel for both security testing and regular non-security testing for the last two years.

This tool, per se, is not targeted ONLY for security, but it has been proven to be extremely useful for security research (just like the case of a binary disassembler).

For the past couple of years, it has been used at Intel for both kinds of testers: Security researchers and regular non-security folks. Both groups of people found the tool to be extremely useful.

To the best of the author's knowledge, no such hacking tool currently exists. Thus, this tool can definitely contribute to a new perspective to DEF CON.

This content will be presented on a Discord video channel.

#dl-video1-voice: https://discord.com/channels/708208267699945503/734027693250576505

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 10:00-18:30 PDT

Title: Pentesting 101
When: Friday, Aug 6, 10:00 - 18:30 PDT
Where: IoT Village (Onsite)

Description:
For more information, see https://www.iotvillage.org/defcon.html

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 10:00-18:30 PDT

Title: Pentesting 101
When: Saturday, Aug 7, 10:00 - 18:30 PDT
Where: IoT Village (Onsite)

Description:

For more information, see https://www.iotvillage.org/defcon.html

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Friday - 16:15-16:45 PDT

Title: People Hunting: A Pentesters Perspective
When: Friday, Aug 6, 16:15 - 16:45 PDT
Where: Recon Village (Virtual)

SpeakerBio: Mishaal Khan
No BIO available
Twitter: @mish3alkhan

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Phantom Attack: Evading System Call Monitoring
When: Friday, Aug 6, 17:00 - 17:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded
Speakers: Junyuan Zeng,Rex Guo

SpeakerBio: Junyuan Zeng
Junyuan Zeng is Senior Software Engineer at Linkedin. Before Linkedin, he was Staff Security Architect at JD.com where he designed and architected container security monitoring solutions. Before that he was Staff Software Engineer for mobile payment security at Samsung and a security researcher at FireEye where he worked on mobile malware analysis. He has published in ACM CCS, USENIX ATC, and other top academic conferences. He obtained his PhD in Computer Science from The University of Texas at Dallas.
https://www.linkedin.com/in/junyuanzeng/

SpeakerBio: Rex Guo
Rex Guo works as Head of Research at Confluera where he leads the security research and development of the cloud XDR product which includes the real-time threat storyboarding capabilities (a.k.a. attack narrative). Before joining Confluera, he was an engineering manager at Cisco Tetration where his team bootstrapped the server EDR product deployed on millions of cloud endpoints. Before that, Rex worked at both Intel Security and Qualcomm. In these positions, he has worked on application security, infrastructure security, malware analysis, and mobile/ IoT platform security. He has presented at Blackhat multiple times. He has 30+ patents and publications. He received a PhD from New York University.
Twitter: @Xiaofei_REX
https://www.linkedin.com/in/xiaofeiguo/

Description:

Phantom attack is a collection of attacks that evade Linux system call monitoring. A user mode program does not need any special privileges or capabilities to reliably evade system call monitoring using Phantom attack by exploiting insecure tracing implementations.

After adversaries gain an initial foothold on a Linux system, they typically perform post-exploitation activities such as reconnaissance, execution, privilege escalation, persistence, etc. It is extremely difficult if not impossible to perform any non-trivial adversarial activities without using Linux system calls.

Security monitoring solutions on Linux endpoints typically offer system call monitoring to effectively detect attacks. Modern solutions often use either ebpf-based programs or kernel modules to monitor system calls through tracepoint and/or kprobe. Any adversary operations including abnormal and/or suspicious system calls reveal additional information to the defenders and can trigger detection alerts.

We will explain the generic nature of the vulnerabilities exploited by Phantom attack. We will demonstrate Phantom attack on two popular open source Linux system call monitoring solutions Falco (Sysdig) and Tracee (Aquasecurity). We will also explain the differences between Phantom v1 and v2 attacks. Finally, we will discuss mitigations for Phantom attack and secure tracing in the broader context beyond system call tracing.

REFERENCES

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33505
https://i.blackhat.com/USA-20/Thursday/us-20-Lee-Exploiting-Kernel-Races-Through-Taming-Thread-Interleaving.pdf
https://www.youtube.com/watch?v=MIJL5wLUtKE
https://dl.packetstormsecurity.net/1005-advisories/khobe-earthquake.pdf

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=yaAdM8pWKG8

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20R

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 15:45-16:30 PDT

Title: Phish Like An APT
When: Saturday, Aug 7, 15:45 - 16:30 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Sanne Maasakkers , Security Expert, Fox-IT
Sanne Maasakkers works as a security expert in the Red Team and Strategic Threat Intelligence team at Fox-IT in the Netherlands. Next to her focus on pentesting and threat analysis (which was recently demonstrated by ‘being’ the attacking APT during the biggest Dutch cyber crisis exercise), she loves to perform social engineering attacks and has a strong expertise on getting initial access by using this technique. In addition to her work, she contributes to "a more secure society" by providing awareness training, guest lectures and hack demos in both professional and educational environments and as team captain of the European team during the International Cyber Security Challenge (ICSC).
https://nl.linkedin.com/in/sannemaasakkers/

Description:

Have you ever wondered what phishing strategy real world APTs use? And how these compare with the scenarios that you use during your Red Team / social engineering activities? If you did, you probably found out that there's a lot of research about APT techniques, tactics and procedures, like the use of specific malware or attack vectors, but there are not many public resources on which techniques those attackers actually use to convince a non-suspecting person to aid them in their operation. In this talk an analysis is presented of hundreds of phishing emails that were used in real campaigns. All characteristics of an email, like the method of influence, tone of speech and used technologies are classified and measures how well a phishing campaign is designed, scoring from “obvious spam” to “near-realistic original mail”. By comparing and measuring the state of these phishing emails,we can learn more about how certain groups operate and how much “effort” they put into their scenarios. This is important knowledge for both attackers and defenders. If you want to know how to phish like you’re an APT, then this talk is for you. Spoiler alert: you might already be a better phisher than these groups.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Friday - 16:30-17:30 PDT

Title: Piecing Together Your Personal Privacy Profile
When: Friday, Aug 6, 16:30 - 17:30 PDT
Where: Crypto & Privacy Village (Virtual)

SpeakerBio: Margaret Fero
Margaret leads security at a small startup, and loves information security, learning and education, and interdisciplinary connections. Before transitioning to a career in security, Margaret was a Technical Writer and independent security researcher. Margaret has spoken at conferences including ToorCon, Write The Docs Day: Australia, the O'Reilly Open Source Convention (OSCON), and Abstractions II.

Description:
In finance, analysts combine seemingly-insignificant information to constitute useful information that a company didn't intend to reveal. This is called mosaic theory. This talk applies the concepts of mosaic theory to a personal privacy audit.

Many details, like those you might post to social media or include on a public resume, can be combined to deduce significant aspects of your private data. Small divergences from your usual patterns can, when combined together, also reveal information that you may not intend to disclose. Often, this information includes your physical location, vacation dates, or current employer.

After this talk, you should be able to apply the concepts of mosaic theory to evaluate the data that is publicly available about you, including combinations of small details that you may have considered insignificant on their own.

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 13:00-13:45 PDT

Title: PINATA: PIN Automatic Try Attack
When: Saturday, Aug 7, 13:00 - 13:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Salvador Mendoza
Salvador Mendoza is a Metabase Q security researcher and member of the Ocelot Offensive Security Team.

Salvador focuses on tokenization processes, payment systems, mag-stripe information and embedded prototypes. He has presented on tokenization flaws and payment methods in different conferences such as Black Hat USA, DEF CON, HITB, Troopers and many others. Also, Salvador designed different tools to pentest mag-stripe information and tokenization processes.

Author of “Show me the (e-) money Hacking a sistemas de pagos digitales: NFC. RFID, MST y Chips EMV“. A Spanish-written book with a collection of different attacks against payment systems.

Twitter: @Netxing
salmg.net

Description:
A brute force attack is a trial-and-error method used to obtain information such as user passwords or personal identification numbers (PINs). This attack methodology should be impossible to apply to the actual secured EMV bank cards. In this talk, we will analyze how an inadequate implementation could rely on an extreme and sophisticated PIN brute force attack against 10,000 combinations from 4 digit PIN that could affect millions of contact EMV cards.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=VOIvEqjJNOY

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20S

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Sunday - 12:00-12:20 PDT

Title: PK-WHY
When: Sunday, Aug 8, 12:00 - 12:20 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Kevin Chen
Kevin Chen was the first Developer Advocate at the now-unicorn open source company Kong and currently works at smallstep, an early stage open source startup. When not developing tech and demos for the PKI space, he likes to bake, travel, and tend to his motorcycle.
Twitter: @devadvocado

Description:
Certificates and public key infrastructure (PKI) are hard. No shit, right? I know a lot of smart people who’ve avoided this particular rabbit hole. Personally, I avoided it for a long time and felt some shame for not knowing more. The obvious result was a vicious cycle: I was too embarrassed to ask questions so I never learned. Well, now everything needs a certificate so let's be embarrassed together and learn they why.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Friday - 14:00-14:45 PDT

Title: Playing God: How ambiguities in state and federal breach notification laws give lawyers too much discretion in deciding whether or not to disclose potential data breaches

When: Friday, Aug 6, 14:00 - 14:45 PDT

Where: Crypto & Privacy Village (Virtual)

Speakers: Anthony Hendricks,Jordan Sessler

SpeakerBio: Anthony Hendricks

Anthony Hendricks is an attorney who advises clients as the chair of Crowe & Dunlevy’s Cybersecurity & Data Privacy Practice Group. In that role, he frequently analyzes and litigates legal issues related to IoT devices. Prior to beginning his practice, he studied as Howard University's first Marshall Scholar and later graduated from Harvard Law School. He now teaches cybersecurity law as an adjunct professor at Oklahoma City University School of Law.

SpeakerBio: Jordan Sessler

Jordan Sessler is an attorney who advises clients on data security as a member of Crowe & Dunlevy’s Cybersecurity & Data Privacy Practice Group. In that role, he regularly engages with legal issues related to IoT devices and has represented companies in disputes with law enforcement regarding the discoverability of user- and device-generated data. Prior to beginning his practice, he graduated from Harvard Law School and clerked for U.S. District Court Judge D.P. Marshall Jr.

Description:

There is often ambiguity as to whether a security incident qualifies as a data breach and, thus, needs to be reported to authorities or disclosed to affected individuals. This means that, despite efforts to pass breach notification laws in all fifty states, there is little consistency in what actually gets reported and disclosed. Some companies disclose data breaches where there is no evidence of data access, while others decline to do so even when there is a substantial possibility of access. Under current law, both courses of action are generally acceptable given latent ambiguity in what triggers a “reasonable belief” that data has been accessed or acquired by an unauthorized party. However, this legal grey area often leaves individual lawyers to make a massive ethical decision: does our client need to tell you that your data may have been stolen, even when the law does not necessarily require that they do so?

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 17:30-17:59 PDT

Title: Playing with FHIR: hacking and securing healthcare APIs
When: Saturday, Aug 7, 17:30 - 17:59 PDT
Where: Biohacking Village (Talk - Virtual)
Speakers: Alissa Knight,Mitch Parker

SpeakerBio: Alissa Knight , Content Creator | Hacker
Alissa Knight is a recovering hacker of 20 years, blending hacking with a unique style of written and visual content creation for challenger brands and market leaders in cybersecurity. Alissa is a cybersecurity influencer, content creator, and community manager as a partner at Knight Ink (http://www.knightinkmedia.com/) that provides vendors go-to market and content strategy for telling brand stories at scale in cybersecurity. Alissa is also the principal analyst in cybersecurity at Alissa Knight & Associates.

Alissa is a published author through her publisher at Wiley, having published the first book on hacking connected cars (https://www.amazon.com/Hacking-Connected-Cars-Techniques-Procedures/dp/1119491800/ref=sr_1_1?crid=X8OQ88MUEP4T& and recently received two new book contracts to publish her autobiography and a new book on hacking APIs.

As a serial entrepreneur, Alissa has started and sold two cybersecurity companies to public companies in international markets and also sits as the group CEO of Brier & Thorn, a managed security service provider (MSSP).

https://www.alissaknight.com/

https://www.alissaknight.com/

SpeakerBio: Mitch Parker , CISO, Indiana University Health
No BIO available

Description:
Hear from renowned bank, automotive, and healthcare API Hacker Alissa Knight on her tactics and techniques in hacking mHealth and FHIR APIs. Alissa walks through the tactics and techniques she uses in her API kill chain. Mitch, IU Health CISO, follows up with tactical and strategic maneuvers to maintain the integrity of the data.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

Title: PMapper
When: Saturday, Aug 7, 10:00 - 11:50 PDT
Where: Palace 1+2

SpeakerBio: Erik Steringer
Erik Steringer is a Senior Security Consultant with NCC Group.

Description:

Tool or Project Name: Principal Mapper (PMapper) - Mapping Privilege Escalation and More in AWS IAM

Short Abstract:
Principal Mapper (PMapper) is an open-source tool and library for assessing AWS IAM and AWS Organizations for security concerns, such as privilege escalation and resource isolation. It tracks and identifies the different ways that one given IAM User/Role (Principal) could pivot to other IAM Users or Roles by reviewing all applicable IAM Policies. After gathering this data, PMapper can perform additional analysis, querying, and visualization.

The querying and analysis systems of PMapper goes beyond checking if a principal is authorized to make a specific AWS API call. It will check if the principal can go through other principals to make a specified AWS API call. In a real-world example: if a user is not authorized to get an S3 object, PMapper also checks if the user can run an EC2 instance with a role as a means of bypassing that restriction. This means that PMapper tells you the effective permissions of each IAM User and Role, and the impact of the extra access you may inadvertently grant to those principals.

Short Developer Bio:
Erik Steringer is a Senior Security Consultant with NCC Group.

URL to any additional information:
https://github.com/nccgroup/PMapper/wiki

Detailed Explanation of Tool:
PMapper is a free and open source project written in Python 3. The v1.1.X release added support for resource policies, SCPs, permission boundaries, and session policies, which means it now works for cross-account scenarios. Additionally, it can now map and handle AWS Organizations.

At a high level, the different operations of PMapper include gathering data (account or organization), querying, analysis, and visualization. All work typically starts with gathering data. When gathering an account's data, PMapper composes a graph to represent the account. The graph includes different IAM Users/Roles, represented as nodes. The graph also tracks how nodes can access each other, as edges. One example of an edge is when a principal can call sts:AssumeRole to access an IAM Role.

The account graph is used by the query component. During all queries, PMapper checks the specified principal and then other principals that can be pivoted to by the specified principal. This catches risks where a given user or role can bypass their own limited permissions with other users or roles. This is also the root of the privilege escalation detection. The different users and roles are marked as administrators if they can effectively call any API operation with any resource, and the privilege escalation detection finds non admins that can pivot to admins through an edge.

The authorization simulator of PMapper runs completely locally, with no calls to the AWS IAM Policy Simulation APIs. It can handle the most complex types of IAM Policies, and other types of policies that even the simulation APIs don’t include (SCPs, Session Policies).

The graph data, query component, and underlying authorization simulator enable PMapper to catch risks that other tools (ScoutSuite, awspx, Cartography, Aaia, CloudMapper, AWS IAM Access Analyzer) cannot. A lot of those risks are covered with the analysis component of PMapper. It can also be extended through the `principalmapper` package to check for even more specific needs.

Supporting Files, Code, etc:
https://github.com/nccgroup/PMapper

Target Audience:
Defense, Cloud

As a consultant, I've had the opportunity to work in a variety of AWS environments across a range of clients and requirements. I think PMapper reflects a lot of the lessons learned during these last few years. Some of the recent work I've put into PMapper helps show where I think the future is (infrastructure as code analysis) for tools in this space.

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 14:00-14:30 PDT

Title: Poking bots for fun and profit in the age of asynchronous stuff
When: Friday, Aug 6, 14:00 - 14:30 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Emanuel Rodrigues
No BIO available

Description:

What Slack, Telegram, Discord, and a ton of other messaging platforms have in common ? Messaging of course ! :) ... but also Bots/apps which are used to enrich the experience of messaging and collaboration environments. Bots are extremely popular now and are very easy to create. The App markets are full of Bots/Apps both free and paid. Let's take a look at these technologies, how it works and how to approach them from a security testing perspective.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 14:30-15:30 PDT

Title: Policy Debrief - Global Cyber Capacity Building - triple challenge or triple opportunity?

When: Friday, Aug 6, 14:30 - 15:30 PDT

Where: Policy (Onsite - SkyView 5/6)

Description:

One thing government worldwide agree upon is that raising defenses helps us all, but also that poorer countries need a lot of help to do so. In recent years the term “cyber capacity building” (CCB) has been used to describe large-scale development assistance programs that help build CERTs, train infosec professionals, but also educate on global cybersecurity issues. Often hackers from DEF CON can find themselves offered lucrative engagements in e.g. the Balkans or Sub-Saharan Africa towards this end. But are programs really global, or more a new type of big power competition? How much can they really deliver both for those societies, but also the rest of the world? And what is the best way to get involved?

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 13:00-13:59 PDT

Title: Policy Debrief - Myths and Legends of Section 230
When: Friday, Aug 6, 13:00 - 13:59 PDT
Where: See Description

Description:

LOCATION TBD

It seems like everyone's talking about Section 230 these days, and keen to change it, without really knowing what it says and does. Don't let this happen to you! Come to this crash course in Section 230 given by Cathy Gellis, a lawyer who regularly litigates (and pontificates) about the statute to learn the truth about this crucial law that enables our online world. We'll talk about why we have Section 230, what it does, why it works, its relationship with the First Amendment, and some of the common misperceptions about it, including why getting rid of it might not make the Internet any better (and will probably make it worse).

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Friday - 12:00-12:30 PDT

Title: Polyswarm Talk
When: Friday, Aug 6, 12:00 - 12:30 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Kevin Leffew
No BIO available

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Sunday - 11:00-11:30 PDT

Title: Potential Pitfalls Protecting Patient Privacy
When: Sunday, Aug 8, 11:00 - 11:30 PDT
Where: AI Village (Virtual)

SpeakerBio: Brian Martin
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 21:00-20:59 PDT

Title: Preventing Sandwich Attacks on DeFi Protocols using Recurrent and Recursive Zero Knowledge Proofs
When: Thursday, Aug 5, 21:00 - 20:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Gokul Alex
"Gokul Alex is an Engineer, Economist and Educator experimenting with emerging and exponential technologies. He loves the creative convergence of programming, philosophy, poetry, psychology, physics with passion and perspectives. He is one of the global 100 Blockchain Experts selected by LATTICE80 Network. He is a top 20 Global thought leader on AI, Analytics, Big Data, Blockchain, Cloud, Cybersecurity, Cryptography, Data Science, Design Thinking, Enterprise Architecture, Quantum Computing and EduTech, FinTech, GovTech, HealthTech as ranked by Thinkers360 Platform.

Smart Contract Auditor | QuillAudits
- Penetration Tester
- Blockchain Security Researcher
- Founder | CipherShastra
- Founder | RazzorSec
- Malware Analyst
- Adversarial ML Researcher"

Description:

We would like to present a session on the most recent attack vector in the DeFi space - Sandwich Attack. Essentially Sandwich attacks creates an imbroglio in the information space of a blockchain by concurrent execution of front running and back running attacks. We have come up with a solution for this problem by leveraging hash time locks implemented as verifiable delay functions coupled with recursive and recurrent combination of zkSNARKS and zkSTARKS. We will also use Polynomial Rings to obfuscate the accounts, transactions and receipts with addition of Identity Mixers.

This talk is now available on YouTube: https://www.youtube.com/watch?v=nEkEsZ0zjkY

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Friday - 12:30-12:59 PDT

Title: Privacy on Public Blockchains with SGX
When: Friday, Aug 6, 12:30 - 12:59 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Secret Network Team
No BIO available

Description:
Bringing privacy to smart contracts by leveraging intel SGX to compute over data without node operators seeing the underlying information.

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

Title: Privacy Without Monopoly: Paternalism Works Well, But Fails Badly
When: Saturday, Aug 7, 10:00 - 10:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Cory Doctorow
Cory Doctorow (craphound.com) is a science fiction novelist, journalist and technology activist. He is a contributor to many magazines, websites and newspapers. He is a special consultant to the Electronic Frontier Foundation (eff.org), a non-profit civil liberties group that defends freedom in technology law, policy, standards and treaties. He holds an honorary doctorate in computer science from the Open University (UK), where he is a Visiting Professor; he is also a MIT Media Lab Research Affiliate and a Visiting Professor of Practice at the University of North Carolina’s School of Library and Information Science. In 2007, he served as the Fulbright Chair at the Annenberg Center for Public Diplomacy at the University of Southern California.

His novels have been translated into dozens of languages and are published by Tor Books, Head of Zeus (UK), Titan Books (UK) and HarperCollins (UK). He has won the Locus, Prometheus, Copper Cylinder, White Pine and Sunburst Awards, and been nominated for the Hugo, Nebula and British Science Fiction Awards.

His recent books include ATTACK SURFACE (2020), a standalone sequel to LITTLE BROTHER intended for adults, POESY THE MONSTER SLAYER, a picture book for young children (2020), the nonfiction tech/politics book HOW TO DESTROY SURVEILLANCE CAPITALISM (2020), RADICALIZED (2019) and WALKAWAY (2017), science fiction for adults; and IN REAL LIFE, a young adult graphic novel created with Jen Wang (2014).

His latest young adult novel is HOMELAND, the bestselling sequel to 2008’s LITTLE BROTHER. His New York Times Bestseller LITTLE BROTHER was published in 2008. His latest short story collection is WITH A LITTLE HELP, available in paperback, ebook, audiobook and limited edition hardcover. In 2011, Tachyon Books published a collection of his essays, called CONTEXT: FURTHER SELECTED ESSAYS ON PRODUCTIVITY, CREATIVITY, PARENTING, AND POLITICS IN THE 21ST CENTURY (with an introduction by Tim O’Reilly) and IDW published a collection of comic books inspired by his short fiction called CORY DOCTOROW’S FUTURISTIC TALES OF THE HERE AND NOW. THE GREAT BIG BEAUTIFUL TOMORROW, a PM Press Outspoken Authors chapbook, was also published in 2011.

LITTLE BROTHER was nominated for the 2008 Hugo, Nebula, Sunburst and Locus Awards. It won the Ontario Library White Pine Award, the Prometheus Award as well as the Indienet Award for bestselling young adult novel in America’s top 1000 independent bookstores in 2008; it was the San Francisco Public Library’s One City/One Book choice for 2013. It has also been adapted for stage by Josh Costello.

He co-founded the open source peer-to-peer software company OpenCola, and serves on the boards and advisory boards of the Participatory Culture Foundation, the Clarion Foundation, the Open Technology Fund and the Metabrainz Foundation. He maintains a daily blog at Pluralistic.net.

Twitter: @doctorow

Description:

Governments around the world (US, UK, EU) are planning to force interoperability on the biggest tech platforms. Companies like Facebook say that this is a privacy disaster because it would hurt their ability to keep us safe from privacy invasions. Yeah, I know. But even if you DO think Facebook has our best interests at heart, monopoly is a deeply stupid way protect privacy. I will present "Privacy Without Monopoly," a major EFF white paper I co-authored with Bennett Cyphers, which sets out a framework for understanding how privacy and interop aren't just compatible - they rely on one another!

https://www.eff.org/wp/interoperability-and-privacy

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=deRRR5B1hwI

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20C

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

Title: ProxyLogon is Just the Tip of the Iceberg, A New Attack Surface on Microsoft Exchange Server!
When: Friday, Aug 6, 15:00 - 15:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Orange Tsai
Cheng-Da Tsai, aka Orange Tsai, is the principal security researcher of DEVCORE, CHROOT security group member, and captain of HITCON CTF team in Taiwan. He is the Pwn2Own 2021 "Master of Pwn" champion and also as the speaker in conferences such as Black Hat USA/ASIA, DEF CON, HITCON, HITB GSEC/AMS, CODE BLUE, and WooYun!

Orange participates in numerous CTF and won second place in DEF CON CTF 22/25/27 as team HITCON. Currently, Orange is a 0day researcher focusing on web/application security, his research is not only the Pwnie Awards 2019 winner for “Best Server-Side Bug” but also the first place in "Top 10 Web Hacking Techniques" of 2017/2018. Orange also enjoys bug bounties in his free time. He is enthusiastic about the RCE bugs and uncovered RCEs in numerous vendors such as Twitter, Facebook, Uber, Apple, GitHub, Amazon, and so on.

Twitter: @orange_8361
https://blog.orange.tw/

Description:
Microsoft Exchange Server is an email solution widely deployed within government and enterprises, and it is an integral part of both their daily operations and security. Needless to say, vulnerabilities in Exchange have long been the Holy Grail for attackers, hence our security research on Exchange. Surprisingly, we’ve found not only critical vulnerabilities such as ProxyLogon, but a whole new attack surface of Exchange.

This new attack surface is based on a significant change in Exchange Server 2013, where the fundamental protocol handler, Client Access Service (CAS), splits into frontend and backend. In this fundamental change of architecture, quite an amount of design debt was incurred, and, even worse, it introduced inconsistencies between contexts, leading us to discover this new attack surface.

To unveil the beauty of this attack surface and our novel exploitation, we’ll start by analyzing this architecture, followed by 7 vulnerabilities that consist of server-side bugs, client-side bugs, and crypto bugs found via this attack surface. In the end, these vulnerabilities are chained into 3 attack vectors that shine in different attack scenarios: ProxyLogon, ProxyShell, and ProxyOracle. These attack vectors enable any unauthenticated attacker to uncover plaintext passwords and even execute arbitrary code on Microsoft Exchange Servers through port 443, which is exposed to the Internet by ~400K Exchange Servers.

This attack surface has its unparalleled impact for a reason: security researchers tend to find vulnerabilities from a certain perspective, such as digging for memory bugs, injections, or logic flaws, but we took a different approach by looking at Exchange from a high-level architectural view and captured this architecture-level attack surface, which yielded multiple vulnerabilities. We hope this brings a new paradigm to vulnerability research and inspires more security researchers to look into Exchange Server. Last but not least, we’ll provide hardening actions to mitigate such types of 0days in Exchange.

# REFERENCES:

- "Hunting for bugs, catching dragons" by Nicolas Joly in Black Hat USA 2019
- CVE-2020-0688 and CVE-2018-8302 from ZDI blog
- CVE-2020-16875 from @steventseeley

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=5mqid-7zp8k

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20C

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 16:00-16:45 PDT

Title: PunkSPIDER and IOStation: Making a Mess All Over the Internet
When: Saturday, Aug 7, 16:00 - 16:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded
Speakers:_hyp3ri0n aka Alejandro Caceres,Jason Hopper

SpeakerBio:_hyp3ri0n aka Alejandro Caceres
No BIO available

SpeakerBio: Jason Hopper
No BIO available

Description:

We've been getting asked a lot for "that tool that was like Shodan but for web app vulns.” In particular WTF happened to it? Punkspider (formerly known as PunkSPIDER but renamed because none of us could remember where tf the capital letters go) was taken down a couple of years ago due to multiple ToS issues and threats. It was originally funded by DARPA. We weren’t sure in which direction to keep expanding, and it ended up being a nightmare to sustain. We got banned more than a 15 year old with a fake ID trying to get into a bar. It became a pain and hardly sustainable without a lot of investment in time and money. Each time we got banned it meant thousands of dollars and countless hours moving sh** around.

Now we’ve solved our problems and completely re-engineered/expanded the system. It is not only far more efficient with real-time distributed computing and checks for way more vulns, we had to take some creative ways through the woods – this presentation covers both the tool itself and the story of the path we had to take to get where it is, spoiler alert: it involves creating our own ISP and data center in Canada and integrating freely available data that anyone can get but most don’t know is available. Come play with us and see what the wild west of the web looks like and listen to our story, it’s fun and full of angry web developers. We’ll also be releasing at least 10s of thousands of vulnerabilities and will be taking suggestions from the audience on what to search. Fun vulns found get a t-shirt, super fun ones get a hoodie thrown at them.

REFERENCES

https://www.youtube.com/watch?v=AbS_EGzkNgI (Shmoo 2013 talk) https://hadoop.apache.org/ https://aws.amazon.com/kubernetes/ https://www.docker.com/ https://www.python.org/ https://www.apache.org/licenses/LICENSE-2.0 https://kafka.apache.org/ https://owasp.org/www-project-top-ten/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=DlS_sl4hTWg

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20h

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

SOC - Thursday - 16:00-17:59 PDT

Title: QueerCon Party
When: Thursday, Aug 5, 16:00 - 17:59 PDT
Where: Bally's Pool

Description:
Come hang out with the queer hacker community

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 16:00-17:59 PDT

Title: QueerCon Party
When: Friday, Aug 6, 16:00 - 17:59 PDT
Where: Bally's Pool

Description:
Come hang out with the queer hacker community

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 16:00-17:59 PDT

Title: QueerCon Party
When: Saturday, Aug 7, 16:00 - 17:59 PDT
Where: Bally's Pool

Description:
Come hang out with the queer hacker community

Return to Index - Add to Google Calendar - ics Calendar file

PYV - Friday - 11:00-11:59 PDT

Title: Racing cryptoexchanges or how I manipulated the balances
When: Friday, Aug 6, 11:00 - 11:59 PDT
Where: Payment Village (Virtual)

SpeakerBio: Vahagan Vardanyan
No BIO available

Description:

A talk on race condition vulnerabilities detected on large cryptocurrency exchanges and made it possible to manipulate the balance.

Payment Village events will stream to Twitch and YouTube.

--

Twitch: https://www.twitch.tv/paymentvillage

YouTube: https://www.youtube.com/c/PaymentVillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 12:00-12:20 PDT

Title: Racketeer Toolkit. Prototyping Controlled Ransomware Operations
When: Saturday, Aug 7, 12:00 - 12:20 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Dimitry "Op_Nomad" Snezhkov
Dimitry Snezhkov is an Associate Director at Protiviti. In this role he hacks code, tools, networks, apps and sometimes subverts human behavior too. Dimitry has spoken at DEF CON, BlackHat, THOTCON conferences, and presented tools at BlackHat Arsenal.
Twitter: @Op_Nomad

Description:

*** SPECIAL NOTE: Technical difficulties prevented this talk from being shown at the correct time slot on DCTV/Twitch. Please look for another event on the schedule, by the same name; replay is estimated to begin at 19:00 on Track 2 DCTV/Twitch only. You may also watch this talk on-demand, by following the links at the bottom of this message. ***

Offensive testing in organizations has shown a tremendous value for simulating controlled attacks. While cyber extortion may be one of the main high ROI end goals for the attacker, surprisingly few tools exist to simulate ransomware operations.

Racketeer is one such tool. It is an offensive agent coupled with a C2 base, built to help teams to prototype and exercise a tightly controlled ransomware campaign.

We walk through the design considerations and implementation of a ransomware implant which emulates logical steps taken to manage connectivity and asset encryption and decryption capabilities. We showcase flexible and actionable ways to prototype components of fully remote ransomware operation including key and data management, as well as data communication that is used in ransomware campaigns.

Racketeer is equipped with practical safeguards for lights out operations, and can address the goals of keeping strict control of data and key management in its deployment, including target containment policy, safe credential management, and implementing operational security in simulated operations.

Racketeer can help gain better optics into IoCs, and is helpful in providing detailed logs that can be used to study the behavior and execution artifacts of a ransomware agent.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=VJ8aqReB118

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20D

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

DC - Friday - 13:00-13:59 PDT

Title: Ransomeware’s Big Year – from nuisance to “scourge”?
When: Friday, Aug 6, 13:00 - 13:59 PDT
Where: Track 1 Live; DCTV/Twitch #1 Live

SpeakerBio:DEF CON Policy Panel
No BIO available

Description: No Description available

This talk will be given live in Track 1, and will be streamed to DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 16:30-17:59 PDT

Title: Ransomware ATT&CK and Defense with the Elastic Stack
When: Saturday, Aug 7, 16:30 - 17:59 PDT
Where: Blue Team Village - Workshop Track 2 (Virtual)
Speakers: Ben Hughes,Daniel Chen,Fred Mastrippolito

SpeakerBio: Ben Hughes
Ben Hughes (@CyberPraesidium) brings over 15 years of diverse experience in cyber security, IT, and law. He leads Polito's commercial services including Digital Forensics & Incident Response (DFIR), threat hunting, pen testing, and risk assessment. Prior to joining Polito, Ben worked on APT hunt teams at federal and commercial clients. He holds CISSP, GCFA, and GWAPT certifications.
Twitter: @CyberPraesidium

SpeakerBio: Daniel Chen
No BIO available

SpeakerBio: Fred Mastrippolito
Pentester, and incdent response engineer with a passion for technology. Founded @politoinc and focuses on assisting customers operate securely.
Twitter: @politoinc

Description:

This hands-on training will walk attendees through leveraging the open source Elastic (ELK) Stack to proactively identify common ransomware tactics, techniques, and procedures (TTPs) within diverse log data sets. The blue team tools and techniques taught during this workshop can be used to investigate isolated ransomware incidents or implemented at scale for continuous monitoring and threat hunting.

This hands-on training will walk attendees through leveraging the open source Elastic (ELK) Stack to proactively identify common ransomware tactics, techniques, and procedures (TTPs) within diverse log data sets. The blue team tools and techniques taught during this workshop can be used to investigate isolated ransomware incidents or implemented at scale for continuous monitoring and threat hunting. Attendees will be provided with access to a preconfigured Elastic cluster and extensive sample logs containing malicious endpoint and network events waiting to be discovered on a simulated enterprise network. Ransomware attack artifacts will be mapped to the MITRE ATT&CK Framework and tagged accordingly in the provided logs to help demonstrate the value of log enrichment, showcase real-world attacker TTPs, and leverage a methodological approach to incident response and anomaly detection. Emphasis will be placed on live demos and practical training exercises throughout.

Workshop Outline: * Introduction to Ransomware Digital Forensics and Incident Response (DFIR), Threat Hunting, and Threat Intelligence Principles * Introduction to the ATT&CK Framework and Mapping Ransomware TTPs to Relevant Log Data (live demos and labs) * Introduction to the Elastic Stack and Log Data-Driven Analysis (live demos and labs) * Hallmarks of the Ransomware Attack Lifecycle (live demos and labs) * Identifying Ransomware Adversaries and TTPs from Reconnaissance to Exfiltration (live demos and labs)

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Saturday - 12:00-12:59 PDT

Title: RCE via Meow Variant along with an Example 0day
When: Saturday, Aug 7, 12:00 - 12:59 PDT
Where: Packet Hacking Village - Talks (Virtual)

SpeakerBio:Özkan Mustafa AKKUŞ , SENIOR CYBER SECURITY CONSULTANT AND VULNERABILITY RESEARCHER AT TURK TELEKOM
Ozkan (Twitter: @ehakkus) is a vulnerability researcher and senior cyber security consultant in Turkey. Ozkan publishes security vulnerabilities on international platforms that he has discovered. He shares his experiences and works on his personal blog (https://www.pentest.com.tr). He gave training and presentations in many universities and institutions in his country. In addition to these studies, He gave the presentation of "The Vulnerability That Gmail Overlooked and Enabling Threat Hunting" in Packet Hacking Village at DEF CON 28 and "0day Hunting and RCE Exploitation in Web Applications" in AppSec Village at DEF CON 27.
Twitter: @ehakkus

Description:
I will touch Some Alternative Bypass Restriction Techniques. Then I will present a vulnerability of Ericsson Network Location that provides the infrastructure of the research and we are going to touch on the meow variant with details through this vulnerability Towards the end we are going to prepare a Metasploit module and exploit the vulnerability.

All Packet Hacking Village talks will stream on YouTube, Twitch, Facebook, and Periscope.

YouTube: https://youtube.com/wallofsheep

Twitch: https://twitch.tv/wallofsheep

Facebook: https://www.facebook.com/wallofsheep/

Periscope: https://www.periscope.tv/wallofsheep

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Friday - 10:00-10:59 PDT

Title: Ready, fire aim: Hacking State and Federal Law Enforcement Vehicles
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Alissa Knight , Content Creator | Hacker
Alissa Knight is a recovering hacker of 20 years, blending hacking with a unique style of written and visual content creation for challenger brands and market leaders in cybersecurity. Alissa is a cybersecurity influencer, content creator, and community manager as a partner at Knight Ink (http://www.knightinkmedia.com/) that provides vendors go-to market and content strategy for telling brand stories at scale in cybersecurity. Alissa is also the principal analyst in cybersecurity at Alissa Knight & Associates.

Alissa is a published author through her publisher at Wiley, having published the first book on hacking connected cars (https://www.amazon.com/Hacking-Connected-Cars-Techniques-Procedures/dp/1119491800/ref=sr_1_1?crid=X8OQ88MUEP4T&
and recently received two new book contracts to publish her autobiography and a new book on hacking APIs.

As a serial entrepreneur, Alissa has started and sold two cybersecurity companies to public companies in international markets and also sits as the group CEO of Brier & Thorn, a managed security service provider (MSSP).

https://www.alissaknight.com/

https://www.alissaknight.com/

Description:
This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=X0ZNEyzloY8

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Friday - 10:00-10:45 PDT

Title: Recon Village Keynote
When: Friday, Aug 6, 10:00 - 10:45 PDT
Where: Recon Village (Virtual)

SpeakerBio: Ben S
No BIO available
Twitter: @nahamsec

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-17:59 PDT

Title: Red Alert ICS CTF
When: Friday, Aug 6, 10:00 - 17:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236432

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 10:00-17:59 PDT

Title: Red Alert ICS CTF
When: Saturday, Aug 7, 10:00 - 17:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236432

Return to Index - Add to Google Calendar - ics Calendar file

CON - Sunday - 12:00-12:59 PDT

Title: Red Team Village CTF - Closing Ceremony

When: Sunday, Aug 8, 12:00 - 12:59 PDT

Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236421

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 13:00-16:59 PDT

Title: Red Team Village CTF - Finals Part 1
When: Saturday, Aug 7, 13:00 - 16:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236421

Return to Index - Add to Google Calendar - ics Calendar file

CON - Sunday - 10:00-11:59 PDT

Title: Red Team Village CTF - Finals Part 2

When: Sunday, Aug 8, 10:00 - 11:59 PDT

Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236421

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 12:00-12:59 PDT

Title: Red Team Village CTF - Qualifier Prizes and Announcements

When: Saturday, Aug 7, 12:00 - 12:59 PDT

Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236421

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-16:59 PDT

Title: Red Team Village CTF - Qualifiers Part 1
When: Friday, Aug 6, 10:00 - 16:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236421

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 10:00-11:59 PDT

Title: Red Team Village CTF - Qualifiers Part 2
When: Saturday, Aug 7, 10:00 - 11:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236421

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Sunday - 12:00-12:59 PDT

Title: Red vs Blue vs Green : The ultimate battle of opinions (or is it)
When: Sunday, Aug 8, 12:00 - 12:59 PDT
Where: Biohacking Village (Talk - Virtual)
Speakers: Ken Kato,Vee Schmitt

SpeakerBio: Ken Kato , Entrepreneur In Residence @ US Navy, White House Presidential Innovation Fellows
Thought leader. Technology disruptor. Innovator. Experienced in solving problems from bare metal to cloud. Steeped deeply in agile methods and development. Track record of success as a change agent in highly regulated industries.

Ken Kato is an entrepreneur, platform/cloud architect, change agent, and innovator; with a wide range of experience across highly regulated industries from finance, to healthcare, to defense. Most recently as a founding member of Kessel Run, Ken disrupted USAF's technology. Working alongside industry innovators Pivotal to provide a cloud platform and help begin their cloud native journey.

Spending a career working at the bleeding edge; Ken continues to iterate on concepts with a focus lately on IoT sensor data aggregation and predictive analysis, security across software and platform lifecycle, edge computing at the extremes of information availability. Evincing a passion to keep pursuing ideas from when the ideas are theory before technology is available until they are matured as an innovation.

Technology alone can't solve complex problems and with that in mind, Ken thinks of what the future landscape may look like. Between experience and data, Ken predicts how decisions made today will be survivable for years ahead and strives to develop a sustainable strategy for organizational growth.

Twitter: @askKenKato

SpeakerBio: Vee Schmitt , Assistant Professor at Noroff/ Independent Security Researcher at Medtronic/ Partner DFIRLABS
No BIO available

Description:

Often when it comes Medical Devices and Healthcare everyone has an opinion. Ever wonder why there is such a difference of opinion. Deep diving into the context and perspective of the various teams involved in the manufacturing, attacking, and defending of medical devices. We explore and discuss why these opinions are different and how we can better communicate our perspective to one another. This talk explores the complexity and constraints that each team faces and how if the silos are broken down it makes for a more collaborative understanding and coming full circle. Often you will that it is Red versus Blue then versus Green. We work against each other rather than coming full circle logically and openly discussing problems in this space. The main theme of this talk is that differences in opinions are often needed to solve complex problems. Let's face it the secure manufacturing and implementation of these devices is a complex problem. Lifting the veil of problems that each of these team's face.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Friday - 15:00-15:59 PDT

Title: Remote Adversarial Phantom Attacks against Tesla and Mobileye
When: Friday, Aug 6, 15:00 - 15:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Ben Nassi
Ben Nassi (Twitter: @ben_nassi) is a security researcher. He specializes in security of autonomous vehicles and IoT devices.
Twitter: @ben_nassi

Description:

In this talk, we present "split-second phantom attacks," a scientific gap that causes two commercial advanced driver-assistance systems (ADASs), Telsa Model X (HW 2.5 and HW 3) and Mobileye 630, to treat a depthless object that appears for a few milliseconds as a real obstacle/object.

We discuss the challenge that split-second phantom attacks create for ADASs. We demonstrate how attackers can apply split-second phantom attacks remotely by embedding phantom road signs into an advertisement presented on a digital billboard which causes Tesla’s autopilot to suddenly stop the car in the middle of a road and Mobileye 630 to issue false notifications. We also demonstrate how attackers can use a projector in order to cause Tesla’s autopilot to apply the brakes in response to a phantom of a pedestrian that was projected on the road and Mobileye 630 to issue false notifications in response to a projected road sign. This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=6aYPhi16FjA

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Friday - 16:00-17:59 PDT

Title: Remote Ham Radio Exams
When: Friday, Aug 6, 16:00 - 17:59 PDT
Where: Ham Radio Village (Virtual Exams)

Description:

For those participating in DEF CON remotely, the HRV is offering remote ham radio exams as well as in-person exams! Register, as well as study for the exam online though ham.study. Registration can be completed at https://ham.study/sessions/610602949f7bd0fb99cbdf95/1

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Saturday - 17:00-18:59 PDT

Title: Remote Ham Radio Exams

When: Saturday, Aug 7, 17:00 - 18:59 PDT

Where: Ham Radio Village (Virtual Exams)

Description:

For those participating in DEF CON remotely, the HRV is offering remote ham radio exams as well as in-person exams! Register, as well as study for the exam online though ham.study. Registration can be completed at https://ham.study/sessions/6106030b38fc691617d940f8/1

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Friday - 11:00-11:59 PDT

Title: Remotely Rooting Charging Station for fun and maybe profit
When: Friday, Aug 6, 11:00 - 11:59 PDT
Where: Car Hacking Village - Talks (Virtual)
Speakers: Huajiang "Kevin2600" Chen,Wu Ming

SpeakerBio: Huajiang "Kevin2600" Chen
Huajiang "Kevin2600" Chen (Twitter: @kevin2600) is a senior security researcher. He mainly focuses on vulnerability research in wireless and embedded systems. Kevin2600 has spoken at various conferences including KCON; DEFCON and CANSECWEST.
Twitter: @kevin2600

SpeakerBio: Wu Ming
Wu Ming (Twitter: @rapiddns) is a senior security engineer. He specializes in Web Security and a Bug Bounty Hunter.
Twitter: @rapiddns

Description:

In recent years the emergence of a new security threat to the electric vehicle charging ecosystem. How safely and easily charge electric vehicles, is deeply impacting the way people travel. Therefore we conducted an in-depth security analysis for the EV charging stations from Schneider Electric.

In this talk, we'll present 3 vulnerabilities (CVE-2021-22706; CVE-2021-22707, and CVE-2021-22708) which we found in Schneider Electric's EVLink Charging System. We'll start by explaining the architecture; components, and protocols involved in such a system. Then we'll walk through step by step how do we found an RCE Vulnerability from it.

We will be diving into the journey of reverse engineering EVLink Charging station. Start from firmware acquisition, and the various challenges of exploiting EVLink. We'll explain the details of how do we overcome these limits, and show how our payloads manipulate the system in order to get a reverse shell with Root privilege. Finally, we'll present a video demo of exploiting the vulnerability.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=PW60NXN0qZE

Return to Index - Add to Google Calendar - ics Calendar file

Title: reNgine
When: Sunday, Aug 8, 10:00 - 11:50 PDT
Where: DemoLab Video Channel 1

SpeakerBio: Yogesh Ojha
Yogesh Ojha is a Research Software Engineer in TRG Research and Development, Cyprus where his research focuses on building solutions for Crime and Terror.As a Passionate Developer and a Hacker, Yogesh builds and maintains reNgine, an automated reconnaissance framework.He has delivered talks on IoT Security and Car Hacking at several conferences like BlackHat Europe, HITB Cyber Week Abu Dhabi, Open Source Summit, IoT Innovatech LATM, GreHack, NoConName, KazHackStan, FOSS Asia Summit, etc. When not building or breaking technologies, he spends his time with his dog Jasper.

Description:

Short Developer Bio: Yogesh Ojha is a Research Software Engineer in TRG Research and Development, Cyprus where his research focuses on building solutions for Crime and Terror.As a Passionate Developer and a Hacker, Yogesh builds and maintains reNgine, an automated reconnaissance framework.He has delivered talks on IoT Security and Car Hacking at several conferences like BlackHat Europe, HITB Cyber Week Abu Dhabi, Open Source Summit, IoT Innovatech LATM, GreHack, NoConName, KazHackStan, FOSS Asia Summit, etc. When not building or breaking technologies, he spends his time with his dog Jasper.

Tool or Project Name reNgine: An automated reconnaissance engine(framework)

Short Abstract: reNgine is an automated reconnaissance engine(framework) that is capable of performing end-to-end reconnaissance with the help of highly configurable scan engines on web application targets. reNgine makes use of various open-source tools and makes a highly configurable pipeline of reconnaissance to gather the recon result.reNgine also makes it possible for users to choose the tools they desire while following the same reconnaissance pipeline, example - with reNgine you aren't limited to using sublist3r for subdomains discovery, rather reNgine allows you to combine multiple tools like sublist3r, subfinder, assetfinder, and easily integrate them into your reconnaissance pipeline. The reconnaissance results are then displayed in a beautiful and structured UI after performing the co-relation in the results produced by these various tools. The developers behind reNgine understand that recon result most often is overwhelming due to the humongous data, so that's why reNgine also comes with advanced query lookup using natural language operators like and, or and not. Imagine, doing recon on facebook.com and filtering the results like http_status!404&page_title=admin|page_title=dashboard&content_length>0&tech=phporseverity=critical|severity=high&vulnerability_title=xss|vulerability_title=cve-1234-xxxxreNgine's flexibility to easily incorporate any existing open-source tools and with advanced features like configurable scan engines, parallel scans, advanced query lookup on recon results, instant notification about the scan, scheduled scans, etc, separates reNgine from any other recon frameworks. reNgine can be used for both reconnaissance and actively monitoring the targets.URL to any additional information: Official Documentation: https://rengine.wiki reNgine v0.5 Major Update with Vulnerability Scan and Advanced recon Lookup Trailer and Demo: https://www.youtube.com/watch?v=DSOS_dkorBMreNgine release Trailer: https://www.youtube.com/watch?v=u8_Z2-3-o2MreNgine Development Timeline Video Trailer: https://www.facebook.com/10000176436...1638639238246/reNgine featured on Portswigger's The daily Swig: https://portswigger.net/daily-swig/r...or-pen-testers reNgine community review: https://twitter.com/Jhaddix/status/1286547230078275585 https://twitter.com/ITSecurityguard/...58400926543879 https://twitter.com/ojhayogesh11/sta...21166811471872 https://twitter.com/search?q=https%3...rc=typed_query

Detailed Explanation of Tool: reNgine is an advanced reconnaissance framework for web application targets that uses various existing open-source tools to achieve this. The idea for reNgine came when I was bored during the lockdown and had nothing better to do. Back then I was working as a Security Analyst and my day job was to perform penetration testing on web applications. While I enjoyed my job, I hated performing recon on these targets because in almost all the cases the recon steps were pretty similar. Except for certain cases, the recon steps I read, I performed, I saw others doing, were very similar. Same usage of tools, same usage of options/parameters/tuning. But I was bored with this recon methodology because, at times I needed the recon results to be saved in a structured way, come back the next day, and still do the analysis without wasting my yet another day on recon.

Also, since I had a day job, I used to do bug bounty during the night, and obviously, my office would fire me right away if I performed recon on bug bounty targets during my office hours, so also was looking for something that could help me schedule the scans on those targets, something like performing a scan every midnight, or lineup 100 scans on the pipeline and scan these targets one step at a time.

The recon results are very humongous on larger targets, and very difficult to search or find the specific results quickly. This was due to the reason that existing frameworks (open-source) had no ability to store the results on DB, almost all used text as output, and obviously, this wasn't going to be helpful unless you write extremely complex greps. So, I went on to create one for myself and named it reNgine, abbreviated for reconnaissance engine. Why Engine? It is because reNgine has the ability to customize the scan engines. These engines are Yaml based configurations, you can add, remove or customize them.

So what is reNgine and how it solved the problems that no other recon frameworks were providing?

One of the most impressive features of reNgine is that it makes use of something called Scan Engines, these engines are highly configurable and allow you to choose the tools you like, configurations you like, example so you are not limited to using subfinder for subdomain gathering, you can use multiple of them, as many as you want. How difficult is it to choose tools? Very simple, just add the tool name in YAML configuration and you're good to go, reNgine will take care of the rest.This scan engine allows you to fine-tune the tools and perform scans in a much-advanced way. These scan engines have one to many relationships with the targets, meaning, you can define one scan engine, let's say 'Defcon Scan' that does Subdomain Discovery at 100 threads, grab screenshots at 50 threads, and also performs vulnerability scan. Now, once this scan engine is defined, you can use it against n number of targets without the need to modify and fine-tune the parameters every once in a while.

Sample Scan Engine Configuration:

```
subdomain_discovery: uses_tool: [ subfinder, sublist3r, assetfinder, oneforall ] thread: 10 wordlist: default amass_config: config_short_name subfinder_config: config_short_name port_scan: ports: [ top-100 ] exclude_ports: null thread: 10 visual_identification: port: xlarge thread: 2 http_timeout: 3000 screenshot_timeout: 30000 scan_timeout: 100 dir_file_search: extensions: [ php,asp,aspx,txt,conf,db,sql,json ] recursive: false recursive_level: 1 thread: 100 wordlist: default fetch_url: uses_tool: [ gau, hakrawler ] intensity: aggressive vulnerability_scan: concurrent: 10 template: all severity: all excluded_subdomains: - test.rengine.wiki - hello.test.com
```

This configuration and finetuning can be used against n targets. The result of this recon is then stored in DB for co-relation.

Technology Stack:
reNgine uses the following technology stack:Web Framework: DjangoDatabase: PostgresDistributed Message Broker: RedisAsync Tasks and Scheduling Scans: Celery and Celery-beat Redis acts as a message broker between Django and Celery.Containerized everything by Docker reNgine has a dashboard-like UI, which makes it easy to co-relate the recon results.Example:
https://user-images.githubuserconten...087b2b48d3.pnghttps://user-images.githubuserconten...d626127d88.png The purpose of creating the dashboard-like UI was so that one can easily filter the recon results like, "Hey, I quickly want to filter a subdomain that has admin or dashboard in page title, and also has HTTP status as 200". With the existing recon frameworks, this was quite impossible. reNgine's dashboard makes it very easy to filter such use cases. Example:
https://camo.githubusercontent.com/2...795f322e706e67

Key Features of reNgine:

Perform Recon:
Subdomain Discovery
Ports Discovery
Endpoints Discovery
Directory Bruteforce
Visual Reconnaissance (Screenshot the targets) IP Discovery

CNAME discovery
Subdomain Takeover Scan
Highly configurable scan engines, use tools of your choice, open-source or integrate your own tool, use one configuration, fine-tuning against multiple targets Run multiple scans in parallel, running multiple scans is very simple, select n targets, choose the scan engine, and initiate the scan. reNgine and celery will take care of the rest. Run Clocked Scans (Run reconnaissance exactly at X Hours and Y minutes) Run Periodic Scans (Runs reconnaissance every X minutes/hours/days/week) Perform Vulnerability Scan using Nuclei and get notified when a vulnerability is discovered Send scan related notifications to Slack or Discord Perform Advanced Query lookup using natural language alike and, or, not operations Example: Assume that, you are looking for open redirection, you can quickly search for =http and look for HTTP status 30X, this will give high accuracy of open redirection with bare minimum effort.Out-of-Scope options available, if recon need not be performed on specific targets, define them on the scan engine and you're good to go. reNgine won't perform anything on the out-of-scope subdomains.Redefined Dashboard that allows you to quickly find out the most vulnerable target and most commonly occurred vulnerability Example: https://user-images.githubuserconten...7e087c1a26.png

Upcoming Features:
Scan Comparision
Comparision of the scans performed on the target, to find out how many new vulnerabilities have been discovered since the last scan, how many new subdomains have been discovered since the last scan, etc. (Under Development)Interesting Subdomains Discovery

reNgine will discover the interesting subdomains based on the HTTP status, content length, and page title. For example, imagine the time saved by reNgine if reNgine tells you that, Hey admin.facebook.com is an interesting subdomain you might want to look up, now this is depended upon, HTTP status, content length, and many more factors (Under Development)

Source Code: https://github.com/yogeshojha/rengine

Target Audience:
The targeted audience is both Offence and Defence on Web application Security.

The audience on the offense can use reNgine to perform active reconnaissance and gather more information about their next penetration testing target. This information includes but not limited to subdomains, ip address associated with it, endpoints, visual reconnaissance screenshot gathering, ports scan, and vulnerability scan as well.

And, the audience on defense can learn how to use reNgine to perform periodic scans on their (Intra/Extra)net web services, run the periodic open-source-powered vulnerability scanner, and get notified instantly when a vulnerability is identified.The beauty of reNgine is that, with minimal penetration testing and security experience, one can run the entire reconnaissance and gather the result so that it is well suited for both offense and defense.

As the purpose of this demo lab would be to demonstrate the capabilities of reNgine, the demo would be outlined in such a way that it can be well received by the audience of both the offense and defense sides.

reNgine is something I have worked really hard, spent countless nights working on it. Within a very short period of time, reNgine became one of the popular reconnaissance tools. Presenting this to fellow hackers will certainly gather new ideas on making reNgine a more advanced reconnaissance tool, which is one of the major reasons why I wish to present this to Defcon. On the other hand, presenting this to Defcon will foster the open-source and hacker culture as I will explain about the in and out of reNgine and hopefully bring in many developers to contribute to reNgine as well.

Also, I plan to announce a major update in reNgine during Defcon, which I believe will bring innovation and excitement among the attendees as well. And of course, Defcon is the right platform to make everyone aware of the updates, advancements, and new features of reNgine.

This content will be presented on a Discord video channel.

#dl-video1-voice: https://discord.com/channels/708208267699945503/734027693250576505

AIV - Saturday - 12:30-12:59 PDT

Title: Replication as a Security Threat: How to Save Millions By Recreating Someone Else’s Model
When: Saturday, Aug 7, 12:30 - 12:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Stella Biderman
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 10:45-11:30 PDT

Title: Representation Matters
When: Friday, Aug 6, 10:45 - 11:30 PDT
Where: IoT Village (Talk - Virtual)
Speakers: Camille Eddy,Chloe Messdaghi

SpeakerBio: Camille Eddy
No BIO available

SpeakerBio: Chloe Messdaghi
Chloé Messdaghi is a tech changemaker who is innovating tech and information security sectors to meet today’s and future’s demands by accelerating startups and providing solutions that empower. She is an international keynote speaker at major information security and tech conferences and events, and serves as a trusted source to reporters and editors, such as Forbes and Business Insider. Additionally, she is one of the Business Insider’s 50 Power Players. Camille Eddy is a Product Engineer and International Public Speaker. She earned her Bachelor of Science degree in Mechanical Engineering from the University of Idaho. Camille has given her talk “Recognizing Cultural Bias in AI” across the world, including San Francisco, Washington DC and Budapest; Helping Technical and Non-Technical Project Managers, Founders and Engineering Leads build better products. Finally, she coaches women building online platforms, helping them make a profitable business working on their passion.

Description:
We often hear about the importance of Diversity, Equity, and Inclusion (DEI) and how companies are striving to do better. However, there are plenty of examples where DEI that is being promoted is not actually happening behind scenes. Stories of those who are marginalized in tech showcasing we still have a large problem with companies practicing lip service and no actual actions to show for it. One way to see if a company is trying to be better on DEI is reflected on the board and C-suite. Yet, still to this day less than 20% of company boards represent marginalized identities. It's time to increase representation of marginalized identities from less than 20% to 50%+ for all levels in tech. When we shift to incorporating DEI practices by making sure representation is present on the leadership team, board and c-suite, it recognizes the voices of marginalized identities: ethnicities, genders, generations, sexuality, and abilities. Research has repeatedly shown that when we have diverse boards and c-level positions held by marginalized persons, it produces a trickle down effect. Where the company takes actions and voices are finally heard because there’s representation, and it's reflected in the vision, company policies, and hiring practices. This talk discusses why we need representation on the leadership team, and how to get involved to actually bring a change to an industry that has run out of time to become more inclusive.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 18:00-18:45 PDT

Title: Response Smuggling: Pwning HTTP/1.1 Connections
When: Friday, Aug 6, 18:00 - 18:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Martin Doyhenard
Martin is a security researcher at the Onapsis Research Labs. His work includes performing security assessment on SAP and Oracle products and detecting vulnerabilities in ERP systems. His research is focused on Web stack security, reverse engineering and binary analisis, and he is also an active CTF player. Martin has spoken at different conferences including RSA, Troopers, Hack In The Box and EkoParty and presented multiple critical vulnerabilities.
Twitter: @tincho_508

Description:

Over the past few years, we have seen some novel presentations re-introducing the concept of HTTP request smuggling, to reliably exploit complex landscapes and systems. With advanced techniques, researchers were able to bypass restrictions and breach the security of critical web applications.

This presentation will take a new approach, focusing on the response pipeline desynchronization, a rather unexplored attack vector in HTTP Smuggling.

First, I will introduce a Desync variant, using connection-tokens to hide arbitrary headers from the backend. This technique does not abuse discrepancy between HTTP parsers, but instead relies on a vulnerability in the protocol itself!

The issue was found and reported under Google's Vulnerability Reward Program for a nice bounty!

Next, I will show how it is possible to inject multiple messages at the backend server, mixing the pipeline's connection order, and hijack users sessions from login requests.

Finally, using a novel technique known as Response Scripting, I will demonstrate how to create malicious outbound messages using static responses as the building blocks. This will be leveraged to write custom responses and take control of one of the most popular protocols in history!

REFERENCES
RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1 https://tools.ietf.org/html/rfc2616

RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content https://tools.ietf.org/html/rfc7231

CHAIM LINHART, AMIT KLEIN, RONEN HELED, STEVE ORRIN: HTTP Request Smuggling
https://www.cgisecurity.com/lib/HTTP-Request-Smuggling.pdf

James Kettle:
HTTP Desync Attacks: Request Smuggling Reborn
https://portswigger.net/research/http-desync-attacks-request-smuggling-reborn
https://portswigger.net/research/http-desync-attacks-what-happened-next

Emile Fugulin
HTTP Desync Attacks with Python and AWS
https://medium.com/@emilefugulin/http-desync-attacks-with-python-and-aws-1ba07d2c860f

Amit Klein
HTTP Request Smuggling in 2020
https://i.blackhat.com/USA-20/Wednesday/us-20-Klein-HTTP-Request-Smuggling-In-2020-New-Variants-New-Defenses-And-Ne

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=suxDcYViwao

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20M

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 09:00-09:25 PDT

Title: Retired but not forgotten – A look at IFEs
When: Friday, Aug 6, 09:00 - 09:25 PDT
Where: Aerospace Village (Virtual Talk)
Speakers: Alex Lomas,Phil Eveleigh

SpeakerBio: Alex Lomas
Alex is Pen Test Partner’s aerospace specialist. Alex undertakes penetration testing of traditional IT, such as networks, web applications, and APIs, as well as more aviation-specific areas including airport operational technology and avionics embedded systems such as inflight entertainment and e-enabled aircraft.

SpeakerBio: Phil Eveleigh
Phil has undertaken testing of all kinds of embedded systems with Pen Test Partners’ Hardware Team, from consumer routers through to operational technology and household electronic devices. He has now brought his skills to the aviation sector. This is Phil’s first talk at DEFCON!

Description:
Alex Lomas and Phil Eveleigh from Pen Test Partners reminisce about research on two interesting in flight entertainment systems from the past 12 months, including great interactions with vendors, attempts remembering how to pwn NT4, and a reminder that just because an aircraft is going to scrap, it still means that disclosures have to be handled sensitively.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=p0A03vVHXnw

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 14:45-15:30 PDT

Title: Reverse Supply Chain Attack - A Dangerous Pathway To Medical Facilities' Networks
When: Saturday, Aug 7, 14:45 - 15:30 PDT
Where: IoT Village (Talk - Virtual)
Speakers: Barak Hadad,Gal Kaufman

SpeakerBio: Barak Hadad
Barak Hadad is a security researcher at Armis, responsible for hunting zero days and reverse engineering. Formerly an R&D team lead in the Israeli Defense Forces Intelligence, his current focus is unraveling the mysteries of various embedded devices, found in hospitals, factories and anything in-between.

SpeakerBio: Gal Kaufman
No BIO available

Description:

The supply-chain attack vector has gained a lot of attention in the passing year. Our talk, however, will present a different type of a supply-chain attack vector -- the reverse supply-chain attack.

The process of a supply chain attack involves an attacker altering code of software, or the hardware of a device, en route to a potential victim. The reverse supply chain attack starts from the other end of the chain -- when a device is removed from a secure network. While IT departments are aware of the importance of wiping the harddrives of PCs, before they are being thrown away, or sold off, they are not fully aware that certain medical devices also withhold sensitive data, and the process to wipe these devices is also non-trivial.

In this talk, we will demonstrate the type of data that can be recovered from the most popular infusion pump -- the BD Alaris Infusion Pump. The recovered data can allow an attacker to infiltrate internal networks of medical facilities and exfiltrate or alter personal patient data. In the process of analyzing this attack vector, we purchased a handful of these used infusion pumps from eBay, which led us to the credentials of internal networks of large hospital facilities all over the US.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

RFV - Thursday - 12:00-11:59 PDT

Title: RF Propagation and Visualization with DragonOS
When: Thursday, Aug 5, 12:00 - 11:59 PDT
Where: Radio Frequency Village (Virtual)

SpeakerBio:cemaxecuter
No BIO available

Description:

"Today's presentation will start with a brief history of DragonOS, where it started and where it's at today. After a short introduction, I'll dive into the subject of visualizing RF propagation with DragonOS. I'll be showing a fresh OS install and the necessary steps to generate a rough estimate of a transmitter based on SRTM-3 elevation data, as well as a new feature enabling visualization/calculations of the path between transmitter and receiver .

Topics and hands on (pre-recorded) demonstrations will include the following,

- SPLAT! is an RF Signal Propagation, Loss, And Terrain analysis tool for the electromagnetic spectrum between 20 MHz and 20 GHz.
- Signal Server Multi-threaded RF coverage calculator
- Dr. Bill Walker's role
- Signal Server and DragonOS integration
- DF-Aggregator Developer / Modifications for visualization

I'll conclude talking about future improvements to RF propagation and visualization tools."

This talk has been released on YouTube.

YouTube: https://www.youtube.com/watch?v=49RVycafF54

Radio Frequency Village will not be streaming any talks, but they will be making talks available on their YouTube channel.

YouTube: https://youtube.com/c/RFHackersSanctuary

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 13:30-13:59 PDT

Title: Risks of ML Systems in Health Care: The Real Story

When: Saturday, Aug 7, 13:30 - 13:59 PDT

Where: AI Village (Virtual)

SpeakerBio: Barton Rhodes
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 15:00-15:30 PDT

Title: Robo Sumo On site
When: Friday, Aug 6, 15:00 - 15:30 PDT
Where: Hardware Hacking Village (Onsite - Bally's Bronze 4)

SpeakerBio: ShortTie
No BIO available

Description:
Come out for Robo Sumo meetup at the HHV IRL

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 14:00-14:45 PDT

Title: Robots with lasers and cameras (but no security): Liberating your vacuum from the cloud
When: Sunday, Aug 8, 14:00 - 14:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Dennis Giese
Dennis is a PhD student and a cybersecurity researcher at Northeastern University. He was a member of one european ISP's CERT for several years.

While being interested in physical security and lockpicking, he enjoys applied research and reverse engineering malware and all kinds of devices.

His most known projects are the rooting and hacking of various vacuum robots

Twitter: @dgi_DE
https://dontvacuum.me

Description:
Vacuum robots are becoming increasingly popular and affordable as their technology grows ever more advanced, including sensors like lasers and cameras. It is easy to imagine interesting new projects to exploit these capabilities. However, all of them rely on sending data to the cloud. Do you trust the companies promise that no video streams are uploaded to the cloud and that your personal data is safe? Why not collect the dust with open-source software?

I previously showed ways to root robots such as Roborock and Xiaomi, which enabled owners to use their devices safely with open-source home automation. In response, vendors began locking down their devices with technologies like Secure Boot, SELinux, LUKS encrypted partitions and custom crypto that prevents gaining control over our own devices. This talk will update my newest methods for rooting these devices.

The market of vacuum robots expanded in the past 2 years. In particular, the Dreame company has recently released many models with interesting hardware, like ToF cameras and line lasers. This can be a nice alternative for rooting. I will show easy ways to get root access on these devices and bypass all security. I will also discuss backdoors and security issues I discovered from analysis. You will be surprised what the developers left in the firmware.

REFERENCES

> Unleash your smart-home devices: Vacuum Cleaning Robot Hacking (34C3)
> https://dontvacuum.me/talks/34c3-2017/34c3.html

Having fun with IoT: Reverse Engineering and Hacking of Xiaomi IoT Devices
https://dontvacuum.me/talks/DEFCON26/DEFCON26-Having_fun_with_IoT-Xiaomi.html

https://linux-sunxi.org/Main_Page

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=EWqFxQpRbv8

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20D

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Sunday - 11:30-11:59 PDT

Title: Robustness of client-side scanning for illegal content detection on E2EE platforms
When: Sunday, Aug 8, 11:30 - 11:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Shubham Jain
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

Title: Rotten code, aging standards, & pwning IPv4 parsing across nearly every mainstream programming language
When: Friday, Aug 6, 14:00 - 14:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Kelly Kaoudis,Sick Codes

SpeakerBio: Kelly Kaoudis
Kelly Kaoudis is a senior software engineer working in application security in Colorado. Following working with the group to validate and test the node-netmask bypass Viale discovered, Kaoudis wrote many of the proofs-of-concept which demonstrate the critical impact of this cascade of unique vulnerabilities.
Twitter: @kaoudis
https://github.com/kaoudis

SpeakerBio: Sick Codes
Sick Codes maintains popular open source projects, publishes high-profile security vulnerabilities in good faith, and administers his namesake https://sick.codes, a security research and tutorial resource for developers. Sick Codes' work coordinating communication across many companies, foundations, and other open source organisations was invaluable in getting these vulnerabilities patched and responsibly disclosed.

Sick Codes: I am a Hacker, an Independent Security Researcher, an Australian, and an Open Source maintainer. I regularly publish nasty vulnerabilities in everyone's favorite products, from all the best vendors. I've published CVEs in Smart TV's, Browsers, missile design software, and entire programming languages. Freelance automation specialist by day and hacker by trade. I publish weaponized code on GitHub, namely Docker-OSX, which was my first big "thing," which now has 15k stars, and my biggest project, Docker-OSX has over 100,000 downloads on DockerHub.

@sickcodes
https://github.com/sickcodes
https://www.linkedin.com/in/sickcodes/
https://sick.codes

Twitter: @sickcodes
https://sick.codes

Description:
Openness to responsibly disclosed external vulnerability research is crucial for modern software maintainers and security teams. Changes in upstream dependency code may have pulled the safety rug out from underneath widely trusted core libraries, leaving millions of services vulnerable to unsophisticated attacks. The impact of even a single reasonably well-distributed supply-chain security vulnerability will be felt by engineering teams across many applications, companies, and industries.

We'd like to discuss an IP address parsing vulnerability first discovered in private-ip, a small and infrequently maintained yet critically important NodeJS package for determining if an IP address should be considered part of a private range or not. We'll talk about not only the implications of this CVE but taking the main idea and applying it across multiple programming languages in uniquely disturbing ways.

Sometimes, the effects of code rot are even more far-reaching than we could possibly expect, and if you pull on a thread, it just keeps going. Sometimes, you get lucky when you know exactly what you're looking for. Sometimes, it's hard to convince other technically-minded folks that a seemingly trivial implementation flaw is dangerous in capable hands.

This talk is beginner as well as advanced-friendly; we'll show you the basics a hacker or a programmer needs to know about IP address parsing and how to tell your octal from your decimal along the way.

REFERENCES

Researchers involved in this work:
- Victor Viale: https://github.com/koroeskohr, koroeskohr - Sick Codes: https://github.com/sickcodes, sickcodes - Kelly Kaoudis: https://github.com/kaoudis, kaoudis - John Jackson: https://www.johnjhacking - Nick Sahler: https://github.com/nicksahler, tensor_bodega - Cheng Xu: https://github.com/xu-cheng

Selected press coverage (as of May '21) -
https://www.bleepingcomputer.com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/ -
https://www.theregister.com/2021/03/29/netmask_cve/ -
https://www.bleepingcomputer.com/news/security/python-also-impacted-by-critical-ip-address-validation-vulnerability/

Currently released advisories related to this work (as of May '21) - https://sick.codes/sick-2021-011/
- https://vuln.ryotak.me/advisories/6
- https://sick.codes/sick-2021-018/
- https://sick.codes/sick-2020-022/

Additional
-
https://sick.codes/universal-netmask-npm-package-used-by-270000-projects-vulnerable-to-octal-input-data-server-side-request-forg
- https://blog.urth.org/2021/03/29/security-issues-in-perl-ip-address-distros/ - https://blog.dave.tf/post/ip-addr-parsing/ -
https://security-tracker.debian.org/tracker/CVE-2021-29424 - https://security-tracker.debian.org/tracker/CVE-2021-29662 -
https://www.npmjs.com/package/netmask - https://github.com/rs/node-netmask
- https://bugs.python.org/issue36384#msg392423 - https://github.com/rust-lang/rust/pull/83652 -
https://github.com/rust-lang/rust/issues/83648

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=_o1RPJAe4kU

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20K

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 15:00-15:59 PDT

Title: RTV/AIV Red Teaming AI Roundtable
When: Saturday, Aug 7, 15:00 - 15:59 PDT
Where: AI Village (Virtual)
Speakers: Rich Harang,Anita Nikolich

SpeakerBio: Rich Harang
No BIO available

SpeakerBio: Anita Nikolich
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

Title: Ruse
When: Saturday, Aug 7, 10:00 - 11:50 PDT
Where: DemoLab Video Channel 2

SpeakerBio: Mike Kiser
Mike Kiser is insecure. He has been this way since birth, despite holding a panoply of industry positions over the past 20 years—from the Office of the CTO to Security Strategist to Security Analyst to Security Architect—that might imply otherwise. In spite of this, he has designed, directed, and advised on large-scale security deployments for a global clientele. He is currently in a long-term relationship with fine haberdashery, is a chronic chronoptimist (look it up), and delights in needlessly convoluted verbiage. He speaks regularly at events such as the European Identity Conference and the RSA Conference, is a member of several standards groups, and has presented identity-related research at Black Hat and Def Con. He is currently a Senior Identity Strategist for SailPoint Technologies.

Description:

Tool or Project Name: Ruse

Short Abstract:
Facial recognition is eroding privacy and other human rights. Industry and government have ethical responsibilities to prevent this, but what if there were a way to enhance privacy for individuals without waiting for the cavalry? Adversarial technology gives people a way to protect this biometric. Ruse is an open-source mobile app that uses some of the research from the past year to enable “normal” people to protect the photos that they put online from being processed by commercial facial recognition products.

Short Developer Bio:
Mike Kiser is insecure. He has been this way since birth, despite holding a panoply of industry positions over the past 20 years—from the Office of the CTO to Security Strategist to Security Analyst to Security Architect—that might imply otherwise. In spite of this, he has designed, directed, and advised on large-scale security deployments for a global clientele. He is currently in a long-term relationship with fine haberdashery, is a chronic chronoptimist (look it up), and delights in needlessly convoluted verbiage. He speaks regularly at events such as the European Identity Conference and the RSA Conference, is a member of several standards groups, and has presented identity-related research at Black Hat and Def Con. He is currently a Senior Identity Strategist for SailPoint Technologies.

URL to any additional information:
https://github.com/derrumbe/Ruse

Detailed Explanation of Tool:

In an ideal world, this tool would utilize two of the latest techniques (Fawkes (http://sandlab.cs.uchicago.edu/fawkes/) / Lowkey) that have been pioneered at various academic institutions over the past year. However, for an app such as this one to truly work, ease-of-use is essential. This means that it *must* be delivered in a mobile format, which restricts the app to using TensorFlow Lite - which in turn means no on-board learning, and that whatever techniques it uses must be as quick and as easy to use as FaceID on a localized device is. (ironic, no?)

However, decent results can be had with a cheaper, faster combination of techniques — injecting perlin noise into the photos, a la Camera Adversaria: https://github.com/kieranbrowne/camera-adversaria, and modifying the photo by applying an arbitrary style through the relatively well known “arbitrary style transfer” technique. The combination of these two is powerful enough to warrant further development because it impacts two different processes involved in facial recognition: facial detection and facial classification.

This currently comes at a slight cost to the end user in terms of human intelligibility, but the app also allows for in-flow modification of the impact of these changes (and their protection.) There are some onboard facilities to check for the impact of these changes: Google MLKit to check for facial recognition, for example, so that the end user can dial down the modifications to a limit that is effective but not as disruptive.

This is a camera-centric mobile app, so the flow looks like this: photo from camera or roll -> apply perlin noise -> apply style filter -> check for impact against facial recognition -> save to roll or upload to social media

The app is on github here: https://github.com/derrumbe/Ruse and will be released onto the android and apple app stores in its first release (hopefully for DefCon): as noted before, ease-of-use is the goal.

Operating system:
Swift (iOS) / Java (android – lagging behind ios currently, but it will be transposed later this summer, hopefully) Tensorflow Version: TensorFlowLiteSwift , nightly build (with GPU accel on) GoogleMLKit
GPUImage: https://github.com/BradLarson/GPUImage (open source) SimplexNoise :
https://weber.itn.liu.se/~stegu/simp...plexNoise.java (open source)

Supporting Files, Code, etc:
https://github.com/derrumbe/Ruse

Target Audience:
Consumer Mobile Offense?

This content will be presented on a Discord video channel.

#dl-video2-voice: https://discord.com/channels/708208267699945503/734027778646867988

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Sunday - 11:00-11:50 PDT

Title: Safecracking for Everyone!
When: Sunday, Aug 8, 11:00 - 11:50 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio: Jared Dygert
No BIO available

Description:
Safecracking is one of the more obscure type of lock in locksport. However, in most cases they can be manipulated without the need for any tools and opened in 5 minutes. This talk will get you an understanding of how that's done and started on your path to cracking your first safe!

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

CHV - Saturday - 15:00-15:59 PDT

Title: Safety Third: Defeating Chevy StabiliTrak for Track Time Fun
When: Saturday, Aug 7, 15:00 - 15:59 PDT
Where: Car Hacking Village - Talks (Virtual)

SpeakerBio: Eric Gershman
No BIO available

Description:

Electronic Stability Control (ESC) system saves thousands of lives every year by preventing accidents before a driver starts to lose control but it can be a real drag when trying to race a modern electric vehicle. Both the Chevy Spark EV and Bolt electric car communities have been unable to defeat the ESC to get full control of their cars on the track. Join me on my journey as I attempt to defeat Chevy’s Stabilitrak to turn an EV econobox into an autocross speed racer.

This talk will stream on YouTube.

YouTube: https://www.youtube.com/watch?v=OS6rSHZq2N8

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 09:05-09:59 PDT

Title: Scaling AppSec through Education
When: Saturday, Aug 7, 09:05 - 09:59 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Grant Ongers (rewtd)
No BIO available

Description:
Given that:

Security teams are outnumbered by developers 100:1 50 - 80% more bugs are found in code review than in testing More than 70% of CVEs are caused by implementations in code It must follow that AppSec should be the biggest part of your concern as a security person, and that you either need to seriously invest in more AppSec people to keep up with the developer population or you need to get developers looking for AppSec issues during code review.

So, how does one do that?

We'll lay out the problem space in a bit more detail, covering some of the issues described in our BlackHat EU talk (https://www.blackhat.com/eu-20/features/schedule/index.html#are-you-big-friendly-giant---red-unless-blue-finds-green-ru-bfg-22 and then we'll move onto how we solve this.

We'll talk about the OWASP Application Security Curriculum project, it's goals, ambitions, and milestones - as well as talking about the current artefacts.

We'll then talk about how you get developers engaged in the education program and how we leverage other OWASP projects (like Cornucopia and the ASVS) to make it all fit together.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 21:00-20:59 PDT

Title: Scaling Blockchains: A Novel Approach
When: Thursday, Aug 5, 21:00 - 20:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Colin Cantrell
No BIO available

Description:
This talk is now available on YouTube: https://www.youtube.com/watch?v=xJ_I4quSTfI

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 15:00-15:45 PDT

Title: Scaling static analysis for free: add additional codebases with a single line of code and no money
When: Friday, Aug 6, 15:00 - 15:45 PDT
Where: AppSec Village (Virtual)
Speakers: Erin Browning,Tim Faraci

SpeakerBio: Erin Browning
No BIO available

SpeakerBio: Tim Faraci
No BIO available

Description:
Scaling static analysis across languages and multiple codebases is a difficult process at best. Here we walk through our setup, which we've architectured to be easy to maintain, provide few false positives, and trivial to add additional codebases. Plus, the primary tool we use is free, as in beer.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Sunday - 13:15-14:15 PDT

Title: Scaling Up Offensive Pipelines
When: Sunday, Aug 8, 13:15 - 14:15 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Gil Biton , Adversarial Tactics Expert, Sygnia
Gil has over 5 years of experience in the Cyber Security industry, specializing in Red Team operations, phishing campaigns, and network infrastructure assessments. Gil has been involved in numerous security engagements with Fortune 100-500 client where he brought his extensive experience in the development and research domains to implement complex techniques and automate offensive security processes. Gil is a member of the Adversarial Tactics team, the offensive security team within Sygnia's Enterprise Security division.
https://www.linkedin.com/in/gil-biton-a3a385101

Description:
Evolving endpoint protection software with enhanced detection capabilities and greater visibility coverage have been taking red team and purple team operation’s complexity to a higher level. The current situation forces adversaries to take precautions and invest much more time in the weaponization phase to overcome prevention and detection mechanisms. The community has adapted CI/CD pipelines to automate tasks related to offensive tools weaponization. Offensive CI/CD pipelines have been around for a couple of years, with the goal of helping red teams to automate offensive tools creation and evasion techniques implementation. As part of this evolution, we designed and built our own offensive CI/CD pipeline framework that is simple to use, modular, self-managed, automated, collaborative, and fast. Our framework leverages Infrastructure as Code (IaC) to fully automate the deployment of our offensive CI/CD pipeline framework with built in recipes for evading host and network detections. Each recipe is modular and can be customized to fit red team or purple team requirements, such as proprietary techniques or imitation of specific threat actor TTPs.The framework leverages Gitlab CI/CD in conjunction with Kubernetes cluster to automate and manage the process of building and deploying offensive tools at scale.

In this talk, we will discuss the essentials of offensive pipeline and present our innovative approach, while referring to the challenges we solved, and demonstrate how you can leverage our offensive CI/CD framework to empower red team and purple team operations.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Friday - 17:30-17:59 PDT

Title: Scope X: Hunt in the Ocean!
When: Friday, Aug 6, 17:30 - 17:59 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Meisam Eslahi
Meisam is a technical cybersecurity practitioner with solid expertise in providing strategies and technical directions, building new service/business lines, diverse teams, and capabilities. He has over 19 years of experience in information technology, with 15 years dedicated to cybersecurity in leadership and technical roles leading, managing, and delivering a wide range of cybersecurity services to multi-national clients - mainly in the banking, financial, healthcare, and telecom sectors.
Twitter: @drmeisam_

Description:

Almost every cybersecurity services begin with defining a scope to be assessed. There is nothing wrong with scoping unless it is all about what we know. Attackers walk into our network from the entry points that we may not even know about them. This is not an "out of the scope" concept as these entry points are entirely unknown; Let's call it "Scope X." One of the mysterious examples of Scope X is subdomains; this presentation will not talk about techniques to enumerate them as uncle Google provides tons of tutorials. Instead, we discuss threat hunting on discovered subdomains.

This talk defines scope x and its importance in threat hunting by using subdomains as a perfect example. Exploring subdomains may help red teamers look for more sensitive information, forgotten vulnerabilities, and obsolete technologies that could provide additional attack surfaces.

On the other hand, the blue teamers should proactively discover the subdomains, identify the different types of risks and address them. Assume we retrieved a large number of subdomains; what would be the next step?

• Data Validation: When we have a bulk number of subdomains in hands, the first step is to determine which one is really UP to reduce false findings.

• Data classification and reduction: We may face tons of subdomains containing sensitive information, precisely like hunting fishes in an ocean! Before we jump into the analysis phase, we could separate and organize collected data into different groups based on desired parameters or filter out unwanted data to narrow down the hunting scope.

• Say cheese and Take a Picture! Without a doubt navigating the subdomains one by one is not an option! One of the common practices is taking the screenshots in bulk, checking and shortlisting them if we found something interesting. But how do that?

• Keyword Style! Each subdomain page source may contain information that helps us to look for a different type of risk. How fast can we search for specific data in a large volume of subdomains? By the way, what to look for?

• Threats lucky draw: There may be different types of technical and business security risks. How to analyze our data, identify risks, and categorize them?

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Friday - 13:30-13:59 PDT

Title: Scripts and Tools to Help Your ICS InfoSec Journey
When: Friday, Aug 6, 13:30 - 13:59 PDT
Where: ICS Village (Virtual)

SpeakerBio: Don C. Weber , Founder, Cutaway Security
Don C. Weber is a Principal Consultant at and Founder of Cutaway Security, LLC and a Certified SANS Instructor. He specializes in providing information security consulting services to organizations with control environments. In his free time he assists with the ICS Village and provides mentoring and teaching for other information security professionals."
Twitter: @cutaway

Description:
Conducting security assessments and gathering information from control environments are obviously different than doing the same tasks in a corporate environment. But, where do you start? Don will outline some of the tools to conduct research, perform assessments, and gather information. He will review some of the scripts the Cutaway Security team has developed to make this easier for administrators, information security professionals, and operational technology teams teams.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

SEV - Friday - 13:30-14:30 PDT

Title: SE Team vs. Red Team
When: Friday, Aug 6, 13:30 - 14:30 PDT
Where: Social Engineer Village (Virtual)

SpeakerBio: Ryan MacDougall
Ryan MacDougall is presently the Chief Operating Officer and Open Source Intelligence trainer for Social-Engineer, LLC. In addition, he runs operations during penetration tests and exercises with clients, as well as managing client relationships. Additionally, Ryan is also a multiyear Black Hat conference trainer and DEFCON SEVillage speaker, regarding social engineering as well as, open source intelligence gathering.

Description:
What is the difference? Is there a difference? Find out by riding along during a real story of a true SE Team.

Social Engineer Village will stream content to Twitch.

Twitch: https://www.twitch.tv/socialengineerllc

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Saturday - 13:00-13:55 PDT

Title: Sea Pods
When: Saturday, Aug 7, 13:00 - 13:55 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: Grant Romundt
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Sunday - 13:00-13:55 PDT

Title: SeaTF, Pirate Hat, and Salty Sensor Results, Closing Statements
When: Sunday, Aug 8, 13:00 - 13:55 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: Brian Satira
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Saturday - 10:30-10:59 PDT

Title: Secrets of Social Media PsyOps
When: Saturday, Aug 7, 10:30 - 10:59 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: BiaSciLab
BiaSciLab is a 14 year old hacker and maker. She was the youngest speaker at H.O.P.E. and has spoken at DEF CON in the Voting Village, Bio Hacking Village and the r00tz Asylum kids con. She has spoken internationally on election security at DefCamp in Romania. She also received national attention when she hacked the election reporting system at DEF CON 26, this work was recently highlighted at the Congressional Hearing on Election Security. This inspired her to build her own election system, Secure Open Vote.

BiaSciLab is also the Founder and CEO of Girls Who Hack, an organization focused on teaching girls the skills of hacking so that they can change the future. She enjoys inventing things, giving talks and teaching classes on making, programming and hacking. Follow her on twitter @BiaSciLab @GirlsWhoHack @SecureOpenVote or check out her websites www.BiaSciLab.com www.GirlsWhoHack.com www.SecureOpenVote.com

Twitter: @BiaSciLab

Description:
Psychological Warfare through social media is one of the most powerful weapons in today's political battlefield. PsyOps groups have figured out how to sharpen the blade through algorithms and targeted advertising. Nation states are using PsyOps to influence the citizens of their enemies, fighting battles from behind the keyboard. In this talk, BiaSciLab with cover a brief history of PsyOps and how it has been used both on the battlefield and the political stage. Followed by a dive deep into how it works on the mind and how PsyOps groups are using social media to influence the political climate and elections worldwide.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

SEV - Friday - 10:00-11:59 PDT

Title: SECTF4Kids (Pre-Registration Required)
When: Friday, Aug 6, 10:00 - 11:59 PDT
Where: Social Engineer Village (Virtual)
Speakers: Ryan M,Colin H

SpeakerBio: Ryan M
No BIO available

SpeakerBio: Colin H
No BIO available

Description:
For more information, please see https://www.social-engineer.org/events/sevillage-def-con/the-sectf4kids/

Social Engineer Village will stream content to Twitch.

Twitch: https://www.twitch.tv/socialengineerllc

Return to Index - Add to Google Calendar - ics Calendar file

SEV - Saturday - 10:00-11:59 PDT

Title: SECTF4Teens
When: Saturday, Aug 7, 10:00 - 11:59 PDT
Where: Social Engineer Village (Virtual)
Speakers: Chris Silvers,Kris Silvers

SpeakerBio: Chris Silvers
No BIO available

SpeakerBio: Kris Silvers
No BIO available

Description:
For more information, please see https://www.social-engineer.org/events/sevillage-def-con/the-sectf4teens/

Social Engineer Village will stream content to Twitch.

Twitch: https://www.twitch.tv/socialengineerllc

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 10:00-14:59 PDT

Title: Secure Coding Tournament CTF

When: Friday, Aug 6, 10:00 - 14:59 PDT

Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236774

Return to Index - Add to Google Calendar - ics Calendar file

WS - Friday - 15:00-18:59 PDT

Title: Secure messaging over unsecured transports
When: Friday, Aug 6, 15:00 - 18:59 PDT
Where: Workshops - Las Vegas 1+2 (Onsite Only)

SpeakerBio: Ash , Hacker
Ash is just some dude. In the past he's been a network engineer, created a variety of security tools, and is currently working in R&D and protocol development in spaces adjacent to email security. He has spoken at DEFCON, Black Hat, and Bsides San Diego. He has recently developed a weird fascination with hacking vintage electromechanical tech.

Description:

You need to send a message, avoiding traditional channels like email and SMS, to someone who's on a different network, somewhere else in the world. The tools at your disposal are Python, DNS, and an unauthenticated MQTT broker. This message must be end-to-end encrypted, and the recipient must be able to confirm that it was undeniably you who sent it. Now add another constraint: you can't communicate directly with this other party to perform a public key exchange before signing, encrypting, and transmitting the message. This can be a difficult problem to solve, and many specialized secure messaging apps have sprung up to address the challenge of end-to-end secured messaging. We will build our own. While our application won't be as sophisticated as Signal, you'll leave the workshop with an understanding of how DNS can be used to enable end-to-end authenticated and encrypted communication across nearly any public system that can be made to support the publisher/subscriber communication pattern.

Registration Link:
https://www.eventbrite.com/e/secure-messaging-over-unsecured-transports-las-vegas-1-2-tickets-162214713575

Prerequisites

> Students should have a good understanding of DNS, Docker, and the Python programming language. An understanding of how to configure DNSSEC with their DNS server/provider of choice is necessary, and a basic understanding of how PKI works (roots of trust and the use of public keys to secure the conveyance of public keys) will be beneficial.

Materials needed:

- Hardware: Laptop with 4GB of RAM, 20GB hard drive space free after installing software prerequisites
- Software: Please arrive with git, Docker engine, and docker-compose already installed
  Other
- Attendees must have administrative access to a public DNS zone on a server which supports the TLSA record type. Many SaaS DNS services support this, and PowerDNS supports the record type as well. Configure this zone for DNSSEC before class.
- If for some reason you cannot configure DNSSEC for your zone, you must be able to host static content over HTTPS under your domain. For example: if you're bringing mydomain.example to the workshop, you must be able to host static content on a server at https://device.mydomain.example/. If you can't do DNSSEC, bring a web server.

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 13:30-13:59 PDT

Title: Securing the Internet of Biological Things
When: Saturday, Aug 7, 13:30 - 13:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Thom Dixon , National Security & Defence, PhD student at Macquarie University
Thom Dixon is Vice President for the Australian Institute of International Affairs NSW and the Manager, National Security and Defence at Macquarie University, Sydney, Australia.

Description:

The coming age of robust two-way communication between living and non-living systems can simply be described as the Internet of Biological Things (IoBT). Interfacing optoelectronic systems with optogenetic-, bioelectrochemical- and biosensor-based information substrates will challenge key assumptions underpinning information security. A cyberbiosecurity mindset is needed to maximise the benefits and minimise the downsides of the pervasive, persistent and immersive information environment that arises from an IoBT world.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Saturday - 12:00-13:59 PDT

Title: Security Investigations with Splunk
When: Saturday, Aug 7, 12:00 - 13:59 PDT
Where: Packet Hacking Village - Workshops (Virtual)

SpeakerBio: Robert Wagner , SPLUNK AND CO-FOUNDER OF HAK4KIDZ
Robert Wagner (Twitter: @mr_minion) is a security professional with 15+ years of InfoSec experience. He is a co-founder of the “Hak4Kidz” charity, a co-organizer of BurbSec and BurbSecCon in Chicago, and is on the Board of Directors of the ISSA Chicago Chapter.
Twitter: @mr_minion

Description:
Investigating with Splunk is a hands-on workshop designed to familiarize participants with how to investigate incidents using Splunk and open source. This workshop provides users a way to gain experience searching in Splunk to answer specific questions related to an investigation. These questions are similar to what would be asked in their own organizations. The workshop leverages the popular Boss of the SOC (BOTS) dataset in a question-and-answer format. Users will leave with a better understanding of how Splunk can be used to investigate in their enterprise. The class includes access to download the free “Investigating with Splunk” app that can be used to review the exercises after the class.

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Saturday - 09:00-09:59 PDT

Title: Seeing the Forest Through the Trees – Foundations of Event Log Analysis
When: Saturday, Aug 7, 09:00 - 09:59 PDT
Where: Packet Hacking Village - Talks (Virtual)

SpeakerBio: Jake Williams , CTO OF BREACHQUEST
Jake Williams (Twitter: @malwarejake) is an incident responder, red teamer, occasional vCISO, and prolific infosec shitposter. He has traveled the world, but isn't welcome in China or Russia (and avoids most countries they have extradition treaties with). When not speaking at a conference like this one, it's a good bet that Jake is engaged in hand to hand combat with an adversary rooted deep in a network or engineering ways to keep them out. Jake's career in infosec started in the intelligence community, but has taken around the world securing networks of all shapes and sizes, from utilities to hospitals to manufacturing plants.
Twitter: @malwarejake

Description:

During an incident, everyone knows you need to review the logs – but what are they actually telling you? There's a wealth of information to be had in your logs event logs, but most analysts miss the forest because they don't understand the trees. In this talk, Jake will walk you through some of the most impactful event logs to focus on in your analysis. We'll target some old favorites covering login events, service creation, and process execution. We'll also examine task scheduler logs, useful in uncovering lateral movement and privilege escalation. Finally, we'll discuss some of the new event logs available in Windows 10 (if only you enable them first). If you don't want to be barking up the wrong tree during your next insider investigation or getting axed because you failed to identify the lateral movement attempts, make sure to watch this video.

All Packet Hacking Village talks will stream on YouTube, Twitch, Facebook, and Periscope.

YouTube: https://youtube.com/wallofsheep

Twitch: https://twitch.tv/wallofsheep

Facebook: https://www.facebook.com/wallofsheep/

Periscope: https://www.periscope.tv/wallofsheep

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Friday - 12:00-12:59 PDT

Title: Seeing Through The Windows: Centralizing Windows Logs For Greater Visibility
When: Friday, Aug 6, 12:00 - 12:59 PDT
Where: Packet Hacking Village - Talks (Virtual)

SpeakerBio: Matthew Gracie , SENIOR ENGINEER AT SECURITY ONION SOLUTIONS
Matthew Gracie (Twitter: @InfosecGoon) has over a decade of experience in information security, working to defend networks in higher education, manufacturing, and financial services. He is currently a Senior Engineer at Security Onion Solutions and the founder of the Infosec 716 monthly meetup. Matt enjoys good beer, mountain bikes, Debian-based Linux distributions, and college hockey.
Twitter: @InfosecGoon

Description:
This talk is a brief summary of how to collect and centralize Windows Event Logs for analysis and free tools that can be used to do so. There is also a demonstration of how to use Elastic Stack to investigate an incident using these collected logs.

All Packet Hacking Village talks will stream on YouTube, Twitch, Facebook, and Periscope.

YouTube: https://youtube.com/wallofsheep

Twitch: https://twitch.tv/wallofsheep

Facebook: https://www.facebook.com/wallofsheep/

Periscope: https://www.periscope.tv/wallofsheep

Return to Index - Add to Google Calendar - ics Calendar file

CAHV - Saturday - 13:00-13:59 PDT

Title: Selling Yourself as a Security Professional
When: Saturday, Aug 7, 13:00 - 13:59 PDT
Where: Career Hacking Village (Talk)

SpeakerBio: Preston Pierce
No BIO available

Description:

What is the key to advancing your career in cybersecurity? The answer is SALES. No, you don't have to go make cold calls worry about CAN-SPAM laws, but you need to learn how to sell yourself. Many security professionals treat the industry like a chess tournament, expecting the most skilled player to come out on top and relying on skills alone to make the difference. This is not the reality of the world we live in. Most estimates say over half of jobs are filled through networking. Sometimes, who you know will matter as much as what you know in seeking a job. Leave the job boards and online postings and learn from one who has spent a decade in cybersecurity in recruiting (including running a cybersecurity recruiting agency) and sales how best to sell yourself for your next career move. This is going to be a tactical, practical discussion. How do you approach finding a new role from an outbound vs. inbound approach? What are the best places to put yourself out there in the market? What does it really mean to network to find your next job? How can you create a pipeline of job opportunities? Join to learn how to create more demand for YOU in the marketplace, find more job opportunities, and become a sought after person in our industry.

This talk will be available on YouTube: https://www.youtube.com/watch?v=9EA1DtgTrbU

Career Hacking Village content will be available on YouTube.

YouTube: https://youtube.com/careerhackingvillage

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 13:00-13:30 PDT

Title: Shell Language Processing (SLP)
When: Friday, Aug 6, 13:00 - 13:30 PDT
Where: AI Village (Virtual)

SpeakerBio: Dmitrijs Trizna
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Saturday - 12:45-13:30 PDT

Title: Shift Left Using Cloud: Implementing baseline security into your deployment lifecycle
When: Saturday, Aug 7, 12:45 - 13:30 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Avinash Jain
I am an information security researcher working as a Lead Security Engineer managing complete end-to-end information security. I love to break application logic and find vulnerabilities in them, have been - acknowledged by various MNCs like Google, Yahoo, NASA, Vmware, MongoDB, and other top companies. I am also an active blogger, some of my articles and interviews have been published in various newspapers like Forbes, BBC, Techcrunch, Economic times, Huffingtonpost, Hindustan times, ZDNet, Hakin9, Hackerone, etc. I am also a cybersecurity speaker, love to share my views on various infosec threads.
Twitter: @logicbomb_1

Description:

In the agile world, where continuous iteration of development and testing happens throughout the software development lifecycle involving constant collaboration with stakeholders and continuous improvement and iteration at every stage, where engineers release their changes very frequently. All this makes the chances of potential security loopholes become more and more real. A fast-moving lean and agile culture makes it necessary to bring the testing of software support earlier in the development and release process. This brings us to the quote - “Security shouldn’t be treated as an after-thought”, it should be brought as close to engineers and as early in SDLC. When we bring something close to the source, and in this context, if we bring Security closer to the source, we call it Shift Left Security. It not only gives a much better opportunity to see improved security outcomes in products sooner, and include the requirements, suggestions, advice at an earlier stage, but also saves time, effort, and overall cost of product delivery. Shift Left approach takes this a step further, integrating security into CICD. With security requirements represented earlier in the software development process, it also makes enforcement part of the Continuous Delivery pipeline with improved testing, monitoring, and response to support security drift detection. By integrating security in CICD, one can deliver secure and compliant application changes rapidly while running operations consistently with automation. In order to do this well, the most logical place security can be checked are code reviews. But now the series of questions raised - How can it be achieved? How can we make sure every release that goes to production has proper security sign-off? How can we scan and test every piece of code that is changed from not just DAST or SAST point of view but also including wide custom and flexible security test cases? Here we will talk about building such a solution and framework to integrate security in CICD and automating the complete process for continuous scanning of different kinds of potential security issues on every code change in AWS Codepipeline. Some of the improvement it brings - Wide Variety of Security checks — Integration of standard and custom checks Early Checks — Now security checks are performed as soon as any PR is raised or code is modified Highly Flexible —The security checks are very modular. We can add more checks as we want and configure them to perform response-based action Completely Automated — Automation is the key/let the machines do the work Alerting - Integration of SNS alert for check success or failure Reporting - Scan reports are shared across different communication channels Framework as code - Any company having their CICD over AWS can use this framework by just running my in-house built cloud formation template Vulnerability Management - All the vulnerabilities and findings are logged in a single place - AWS Security Hub

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

DL - Saturday - 14:00-15:50 PDT

Title: Shutter
When: Saturday, Aug 7, 14:00 - 15:50 PDT
Where: Palace 1+2

SpeakerBio: Dimitry "Op_Nomad" Snezhkov
Dimitry Snezhkov is an Associate Director at Protiviti. In this role he hacks code, tools, networks, apps and sometimes subverts human behavior too. Dimitry has spoken at DEF CON, BlackHat, THOTCON conferences, and presented tools at BlackHat Arsenal.
Twitter: @Op_Nomad

Description:
Tool or Project Name: Shutter

Short Abstract:
The goal of Shutter is to manage windows network stack communication via Windows Filtering Platform. Management can include blocking or permitting traffic based on IP or an executable that initiates or receives the traffic.

This is useful to blackhole event logging, defensive agent communication, or explicitly permit specific executables to communicate if they have been previously restricted by policy.

Shutter installs rules in a memory running session without touching the windows firewall itself or invocation of `netsh` command, thereby minimizing detection during long haul RT operations.

As a generic mechanism for managing network traffic it can help operators in: punching through firewalls without shutting them down not creating persistent rules
evading reporting on `netsh` invocation blackholing EDRs and activity supervising agents. studying existing security providers, active filters and network endpoints involved in network communication Short Developer Bio:
I support initiatives in offensive testing for my team by writing code where needed.

Interests include network-based command and controls, data exfiltration mechanisms, evasion.

URL to any additional information: https://github.com/dsnezhkov/shutter

Detailed Explanation of Tool: Please see https://github.com/dsnezhkov/shutter...main/README.md

Supporting Files, Code, etc: https://github.com/dsnezhkov/shutter

Target Audience: Offense

Offensive teams can use the tool to better simulate attacks that involve WFP.

Return to Index - Add to Google Calendar - ics Calendar file

Title: Siembol

When: Friday, Aug 6, 12:00 - 13:50 PDT

Where: DemoLab Video Channel 2

SpeakerBio: Marian Novotny

Marian Novotny received his PhD in Computer Science from the Faculty of Sciences at Pavol Jozef Safarik University in Kosice, Slovakia. In his PhD thesis he focused on the design and analysis of security protocols. He is currently working as a software engineer at G-Research, where he is responsible for the design, analysis and implementation of security data processing applications used for security monitoring and intrusion detection. In the past he worked as a specialized software engineer at ESET, where he designed and implemented network intrusion detection systems which were integrated into various ESET products.

Description:

Tool or Project Name: Siembol

Short Abstract:
Siembol is Anti-Malware for the Cloud: an open-source real-time SIEM (Security Information & Event Management) tool based on big data technologies.

Short Developer Bio:
Marian Novotny received his PhD in Computer Science from the Faculty of Sciences at Pavol Jozef Safarik University in Kosice, Slovakia. In his PhD thesis he focused on the design and analysis of security protocols. He is currently working as a software engineer at G-Research, where he is responsible for the design, analysis and implementation of security data processing applications used for security monitoring and intrusion detection. In the past he worked as a specialized software engineer at ESET, where he designed and implemented network intrusion detection systems which were integrated into various ESET products.

URL to any additional information:
https://siembol.io

Detailed Explanation of Tool:
Siembol is an in-house developed security data processing application, forming the core of an internal Security Data Platform. Following the experience of using Splunk, and as early adopters of Apache Metron, the team needed a highly efficient, real-time event processing engine with fewer limitations and more enhanced features. With Metron now retired, Siembol hopes to give the community an evolved alternative. Siembol improvements over Metron:
Components for real-time alert escalation: CSIRT teams can easily create a rule-based alert from a single data source, or they can create advanced correlation rules that combine various data sources. Pending: tool for translating a Sigma rule specification into siembol Ability to integrate with other systems using dedicated components and plugin architecture for easy integration with incident response tools Advanced parsing framework for building fault tolerant parsers Enhanced enrichment component allowing for defining rules and joining enrichment tables Configurations and rules are defined by a modern Angular web application, with a git-based approval process Supports OAUTH2/OIDC for authentication and authorization in the siembol UI Easy installation for use with prepared docker images and helm charts Siembol Use Cases:
SIEM log collection using open-source technologies Detection tool for discovery of leaks and attacks on infrastructure

Supporting Files, Code, etc:
https://github.com/G-Research/siembol

Target Audience:
Defense

Siembol is trying to provide SIEM functionality using open-source technologies, and is enthusiastic about building community around the project. We believe that this approach can help build a better open-source anti-malware cloud product.

This content will be presented on a Discord video channel.

#dl-video2-voice: https://discord.com/channels/708208267699945503/734027778646867988

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 13:00-13:45 PDT

Title: Signed, Sealed, Delivered: Abusing Trust in Software Supply Chain Attacks
When: Friday, Aug 6, 13:00 - 13:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Cheryl Biswas , Threat Intel Specialist, TD
Cheryl Biswas is a Threat Intelligence Specialist with TD Bank in Toronto, Canada, where she produces and delivers annual cyber threat forecasts, and has experience in security audits and assessments, privacy, disaster recovery and change management. She holds an ITIL certification and a specialized honours degree in Political Science. Cheryl is actively engaged in the security community as a conference speaker and volunteer, mentors those entering the field, and champions women and diversity in cyber security as a founding member of "The Diana Initiative".
Twitter: @3ncr1pt3d

Description:

Our technology-driven world increasingly relies on software dependencies: third party code, open source libraries and shared repositories. A history of software supply chain attacks shows how easy it is to create confusion and send malicious code undetected through automated channels to trusting recipients. SolarWinds delivered a hard truth to defenders: everyone is vulnerable when trust can be abused. Are we ready for what will be sent down the pipeline next?

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Signed, Sealed, Delivered: Comparing Chinese APTs behind Software Supply Chain Attacks
When: Sunday, Aug 8, 14:15 - 15:15 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Cheryl Biswas , Threat Intel Specialist, TD
Cheryl Biswas is a Threat Intelligence Specialist with TD Bank in Toronto, Canada, where she produces and delivers annual cyber threat forecasts, and has experience in security audits and assessments, privacy, disaster recovery and change management. She holds an ITIL certification and a specialized honours degree in Political Science. Cheryl is actively engaged in the security community as a conference speaker and volunteer, mentors those entering the field, and champions women and diversity in cyber security as a founding member of "The Diana Initiative".
Twitter: @3ncr1pt3d

Description:

State-sponsored threat actors have engaged in software supply chain attacks for longer than most people realize, as governments seek out access to information and potential control. Of Russia, North Korea and Iran, China has been behind the most attacks, targeting the technology sector for economic espionage and intellectual property theft. In their current drive for innovation and cloud migration, organizations increasingly rely on software development and all its dependencies: third-party code, open - libraries andshared repositories. Recent attacks have shown how easy it is to create confusion and send malicious code undetected through automated channels to waiting recipients.

This talk will walk attendees through the stages of past attacks by Chinese APTs - notably APT10, APT17 and APT41- to show how capabilities have evolved and what lessons could be applied to recent attacks, comparing tactics, techniques and procedures.

TOPICS COVERED:

What constitutes software supply chain attacks. The abuse of trust and compromise at the source. Trust third parties with third parties. How cloud migration and innovation fuel increased code dependency. Understanding CI/CD continuous integration and continuous delivery. The increased use and targeting of online code repositories and automated software distribution. Where mistakes and misconfigurations occur, creating adversarial opportunity A brief history of software supply chain attacks on repositories.

LEARNING FROM THE PAST

A walk through of several major attack including Operation Aurora, CCleaner, NetSarang. Contrast these to a walk through of recent attacks including SolarWinds, Dependency Confusion, Codecov and XCodeSpy.

The value of historical context is that it helps illuminate TTPs that should be monitored for and secured against, especially those which aid in deception and evasion. Recommendations for mitigations and best practices to secure code, dependencies.

TAKEAWAYS

Attendees will learn what software supply chain attacks are and why they are increasing They will understand the opportunity for adversaries because of the vulnerability created by multiple dependencies. A breakdown of key attacks will be mapped to the Lockheed Martin Kill Chain steps and Mitre ATT&CK. Attendees will be familiarized with major Chinese APT group TTPs which they can bring back to their organizations to implement in their monitoring.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Saturday - 13:30-13:59 PDT

Title: Sla(sh*t)ing happens when you stake
When: Saturday, Aug 7, 13:30 - 13:59 PDT
Where: Blockchain Village / Paris Vendome B
Speakers: Nadir Akhtar,Y L

SpeakerBio: Nadir Akhtar , Blockchain Security Engineer, Coinbase
Blockchain security engineer @ Coinbase with deep expertise in digital asset security vulnerabilities https://blog.coinbase.com/securing-an-erc-20-token-for-launch-on-coinbase-68313652768f Former President, Blockchain @ Berkeley edX Blockchain Fundamentals curriculum developer and lecturer

Nadir Akhtar is a Blockchain Security engineer at Coinbase, where he leads security reviews of assets under consideration for Coinbase listing. Previously at Quantstamp, he audited smart contracts and contributed to a book on smart contract security fundamentals. He graduated from UC Berkeley in 2019 with a degree in Computer Science. During his time in Blockchain at Berkeley, he was President and an instructor for the UC Berkeley-endorsed blockchain fundamentals edX course series, reaching over 225,000 enrolled students to date.

SpeakerBio: Y L , System Security Architect, Coinbase
System security Architect @ Coinbase. Leads team that designed, built, and operates Coinbase's current cold storage system. https://www.wired.com/story/coinbase-physical-vault-to-secure-a-virtual-currency/

Description:

Proof of Stake protocols come with their own programmed reward/penalty incentives that impact principal token balance staked as well as staking rewards earning potential. Our talk first reviews our threat model for staking operations and then presents threat countermeasure recommendations to minimize risk of staking losses. This knowledge can be used to help you assess the risk posture of staking service providers and can be used as a best practices guide if you want to build out your own staking infrastructure.

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 13:00-13:45 PDT

Title: Sleight of ARM: Demystifying Intel Houdini
When: Friday, Aug 6, 13:00 - 13:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Brian Hong
Brian Hong is a security consultant at NCC Group, a global information assurance specialist providing organizations with expert security consulting services. He specializes in hardware penetration testing, reverse engineering, and has performed security research related to embedded systems, firmware analysis, web application penetration testing, and Android security and malware analysis. Brian has a B. Eng. in Electrical Engineering and Computer Science from The Cooper Union.

Description:

In the recent years, we have seen some of the major players in the industry switch from x86-based processors to ARM processors. However, you might be surprised to know that Intel has long supported ARM to x86 transition with their binary translator, Houdini, which runs ARM binaries on x86.

In this talk, we will discuss Intel's proprietary Houdini translator, which is primarily used by Android on x86 platforms, such as higher-end Chromebooks and desktop Android emulators. We will start with a high-level discussion of how Houdini works and is loaded into processes. We will then dive into the low-level internals of the Houdini engine and memory model, including several security weaknesses it introduces into processes using it. Lastly, we will discuss methods to escape the Houdini environment, execute arbitrary ARM and x86, and write Houdini-targeted malware that bypasses existing platform analysis.

REFERENCES

> * Ye, Roger. Android System Programming: Porting, Customizing, and Debugging Android HAL. Packt Publishing, 2017. * JNI Functions, Oracle, 12 Nov. 2002, https://docs.oracle.com/javase/7/docs/technotes/guides/jni/spec/functions.html * Chromium OS Docs. Linux System Call Table, https://chromium.googlesource.com/chromiumos/docs/+/master/constants/syscalls.md * The Development Environment : Android Developers. Android Developers, https://developer.android.com/topic/arc/development-environment * Nachoparker. Own Your Bits, 14 June 2018, https://ownyourbits.com/2018/06/13/transparently-running-binaries-from-any-architecture-in-linux-with-qemu-and-binfmt
> * Git at Google. Android container in Chrome OS, archived at https://web.archive.org/web/20200128052853/https://chromium.googlesource.com/chromiumos/platform2/+/master/arc/co
> * Oberheide, J. & Miller, C. 2012, June. Dissecting the Android Bouncer [Presentation] @ SummerCON, Brooklyn, New York

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=9oQ5XjA1aq0

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20E

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Saturday - 15:00-15:30 PDT

Title: Smart Meters: I'm Hacking Infrastructure and So Should You
When: Saturday, Aug 7, 15:00 - 15:30 PDT
Where: ICS Village (Virtual)

SpeakerBio: Hash Salehi
Hash grew up on IRC freely sharing information and benefitting from those more knowledgeable who were willing to reciprocate. He is the founder of RECESSIM, a reverse engineering community where information is freely shared. Over the last few years he has focused on reverse engineering smart meter technology analyzing both the RF communications and hardware design, openly publishing all his findings.
Twitter: @BitBangingBytes

Description:

Why Smart Meters? This is a question Hash is often asked. There's no bitcoin or credit card numbers hiding inside, so he must want to steal power, right? Openly analyzing the technology running our critical infrastructure and publishing the findings is something Hash is passionate about. In the wake of the great Texas freeze of 2021, we can no longer "hope" those in power will make decisions that are in the people's best interest. This talk will present research on the Landis+Gyr GridStream series of smart meters used by Oncor, the largest energy provider in Texas.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

Title: Sneak into buildings with KNXnet/IP
When: Saturday, Aug 7, 14:00 - 14:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Claire Vacherot
Claire Vacherot is a pentester at Orange Cyberdefense. She likes to test systems and devices that interact with the real world and is particularly interested in industrial and embedded device cybersecurity. As a former software developer, she never misses a chance to write scripts and tools.

Description:

Building Management Systems control a myriad of devices such as lighting, shutters and HVAC. KNX (and by extension KNXnet/IP) is a common protocol used to interact with these BMS. However, the public's understanding and awareness is lacking, and effective tooling is scarce all while the BMS device market keeps on growing.

The ability to craft arbitrary KNXnet/IP frames to interact with these often-insecure BMS provides an excellent opportunity in uncovering vulnerabilities in both the implementation of KNX as well as the protocol itself. From unpacking KNX at a lower level, to using a Python-based protocol crafting framework we developed to interact with KNXnet/IP implementations, in this talk we'll go on a journey of discovering how BMS that implement KNXnet/IP work as well as how to interact with and fuzz them.

After this talk you could also claim that "the pool on the roof has a leak"!

REFERENCES

> KNX Standard v2.1 https://my.knx.org/fr/shop/knx-specifications?product_type=knx-specifications Scapy https://github.com/secdev/scapy KNXmap https://github.com/takeshixx/knxmap Papers & talks: in)security in building automation how to create dark buildings with light speed Thomas Brandstetter and Kerstin Reisinger Presented at BlackHat USA 2017 https://www.blackhat.com/docs/us-17/wednesday/us-17-Brandstetter-insecurity-In-Building-Automation-How-To-Create-I Hacking Intelligent Building - Pwning KNX & ZigBee Networks HuiYu Wu and YuXiang Li (Tencent) Presented at HITB Amsterdam 2018 https://conference.hitb.org/hitbsecconf2018ams/materials/D1T2%20-%20YuXiang%20Li,%20HuiYu%20Wu%20&%20Y Security in KNX or how to steal a skyscraper Egor Litvinov Presented at Zero Nights 2015 http://2015.zeronights.org/assets/files/20-Litvinov.pdf HVACking: Understanding the Delta Between Security and Reality Douglas McKee and Mark Bereza Presented at Defcon 27, 2019 https://www.mcafee.com/blogs/other-blogs/mcafee-labs/hvacking-understanding-the-delta-between-security-and-reality/ Anomaly Detection in BACnet/IP managed Building Automation Systems Matthew Peacock – 2019 https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=3180&context=theses

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=QofeTV39kQE

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20C

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Friday - 15:00-15:30 PDT

Title: So What? The CFAA after Van Buren
When: Friday, Aug 6, 15:00 - 15:30 PDT
Where: Crypto & Privacy Village (Virtual)

SpeakerBio: Kendra Albert
Kendra Albert is a public interest technology lawyer with a special interest in computer security law and in protecting marginalized speakers and users. They serve as a clinical instructor at the Cyberlaw Clinic at Harvard Law School, where they teach students to practice law by working with pro bono clients. Kendra is also the founder and director of the Initiative for a Representative First Amendment. Before they joined the Clinic, Kendra worked with Marcia Hofmann at Zeitgeist Law. They serve on the board of the ACLU of Massachusetts and the Tor Project, and provide support as a legal advisor for Hacking // Hustling.

Description:
On June 3, 2021, the Supreme Court of the United States decided Van Buren v. United States, its first case that meaningfully took up the scope of the Computer Fraud and Abuse Act, the federal anti-hacking statute. Originally passed in the aftermath of Wargames (no, really), the CFAA's broad language has been used to criminalize all kinds of activities that might not be traditionally considered hacking, from employees accessing databases for non-job purposes to companies that aimed to aggregate social network data. Post Van Buren, it's clear that the Computer Fraud and Abuse Act is narrower - but what is covered and what isn't is still up in the air. This talk will provide a brief overview of the CFAA, particularly focused on computer security work and research, and then discuss what the consequences of Van Buren might be, including competing theories about the infamous (for lawyers at least) footnote that suggests that non-technical restrictions on access may create CFAA liability.

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Friday - 11:35-12:05 PDT

Title: So You Want to OPSEC, Eh?
When: Friday, Aug 6, 11:35 - 12:05 PDT
Where: Recon Village (Virtual)

SpeakerBio: Ritu Gill
No BIO available
Twitter: @OSINTtechniques

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Saturday - 12:30-12:59 PDT

Title: Social Media Security = Election Security
When: Saturday, Aug 7, 12:30 - 12:59 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Sebastian Bay
Sebastian Bay is a researcher with the Swedish Defense Research Agency specialising in election security and digital harms.

Description:

Digital disinformation is a significant threat to trusted elections and poses a cybersecurity challenge for social media companies. Fake accounts spread content to authentic users, mislead users, and trick users into believing content is more popular. The global market for media manipulation is extensive and growing - many providers openly market their fake engagement services.

Sebastian Bay and his fellow researchers bought fake engagement on Facebook, Instagram, Twitter, Youtube, and Tik Tok to assess the social media companies' ability to combat disinformation. This presentation explores their findings, highlights the differences between social media platforms, and provides recommendations for companies and policy makers.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

Title: Solitude
When: Friday, Aug 6, 12:00 - 13:50 PDT
Where: DemoLab Video Channel 1

SpeakerBio: Dan Hastings
Dan Hastings is a senior security consultant at NCC Group. He spends his time performing mobile and web application penetration tests for fortune 500 companies. Dan has spoken at the Defcon Crypto and Privacy village on his research on discrepancies in iOS Robocall blocking apps privacy policies and their actual data collection practices.

Description:
Tool or Project Name: Solitude: A privacy analysis tool

Short Abstract:
Solitude is an open-source privacy analysis tool that aims to help people inspect where their private data goes once it leaves their favorite mobile or web applications. Whether a curious novice or a more advanced researcher, Solitude makes the process of evaluating an app's privacy accessible for everyone without the need for time-consuming app instrumentation and analysis, which we've abstracted away from the user.

Privacy policies are often difficult to understand when trying to identify how your private data is being shared and with whom it's being shared. My previous research1 has even shown that privacy policies don't always tell the truth of what an app's actual data collection practices actually are. What's more, prior to Solitude, tooling to find this out efficiently didn't exist for security researchers, let alone nontechnical users. Solitude was built to help give users more transparency to understand where their private data goes by the process of proxying HTTP traffic and inspecting HTTP traffic more straightforward, and can be configured to look for arbitrary datatypes captured by a mobile or web application. In its early release, this tool has already been used by journalists to help investigate privacy abuses by mobile app vendors.

Short Developer Bio:
Dan Hastings is a senior security consultant at NCC Group. He spends his time performing mobile and web application penetration tests for fortune 500 companies. Dan has spoken at the Defcon Crypto and Privacy village on his research on discrepancies in iOS Robocall blocking apps privacy policies and their actual data collection practices.

URL to any additional information:
https://github.com/nccgroup/Solitude

Detailed Explanation of Tool:
Solitude can be run in two different ways; either as a stand-alone web application/HTTP intercept proxy, or in a more mobile-friendly docker container that runs an Open VPN server along with the Solitude web application and intercepting HTTP proxy.

Users of Solitude can configure what data they want Solitude to search for in the Solitude web application. Solitude automatically searches through all websockets and HTTP requests using yara rules based upon what users have configured to search for. Solitude recursively decodes base64 and URL encoded data, searches for sha1,sha256 and md5 hashes of all configured data and supports protobuf and gzip. Several built-in searches are pre-configured to search for GPS coordinates and internal IP addresses. Once a configured piece of data is found the data and domain that the data is being sent to is displayed in the Solitude web application.

Supporting Files, Code, etc:
https://github.com/nccgroup/Solitude

Target Audience:
Mobile, Offense, Privacy enthusiasts.

Solitude makes the process of gaining transparency into where your private data goes when you use your favorite apps easier than reading and trusting a privacy policy. App users deserve more insight the data collection practices of the apps they use. Solitude is unique in that it aims to make an otherwise technical process easy and empower people to make informed decisions about the applications they choose to use.

This content will be presented on a Discord video channel.

#dl-video1-voice: https://discord.com/channels/708208267699945503/734027693250576505

Return to Index - Add to Google Calendar - ics Calendar file

Title: SPARROW: A Novel Covert Communication Scheme Exploiting Broadcast Signals in LTE, 5G & Beyond
When: Saturday, Aug 7, 14:00 - 14:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded
Speakers: Chuck McAuley,Reza Soosahabi

SpeakerBio: Chuck McAuley
Chuck McAuley is a principal security researcher with the Application & Threat Intelligence Research Center (ATIRC) at Keysight Technologies. Chuck has a variety of interests that include 5G and LTE packet core vulnerabilities, reverse engineering botnets, finding novel forms of denial of service, and researching weird esoteric protocols for weaknesses and vulnerabilities
Twitter: @nobletrout

SpeakerBio: Reza Soosahabi
Reza Soosahabi is a lead R&D engineer with Application & Threat Intelligence Research Center (ATIRC) at Keysight Technologies. His current field of research includes RAN security, data exfiltration and ML / statistical algorithms. He has been a 5G system engineer prior to joining Keysight in 2018. He contributes in IEEE proceedings related to signal processing and information security. As a math-enthusiast, Reza often tries unconventional analytical approaches to discover and solve technically diverse problems. He also enjoys cutting boxes with Occam's Razor and encourages the others around him to do so.
Twitter: @darthsohos
https://scholar.google.com/citations?user=SNFxK60AAAAJ&hl=en

Description:

When researching methods for covert communications in the wireless space, we noticed most hackers are barely looking below the IP layer, and even the wireless guys are focused on creating their own radio (PHY layer) solutions rather than looking at what's already available to them. We discovered a sweet spot that takes advantage of MAC layer protocols in LTE and 5G, enabling long range communication using other people's networks, GSMA CVD-2021-0045. We can use SPARROW devices almost everywhere in a variety of scenarios, such as data exfiltration and command and control. Despite limited data rates, the new scheme can defeat known covert communication schemes with dedicated PHY in the following ways:

- Maximum Anonymity: SPARROW devices do not authenticate with the host network while operating. This eliminates their exposure to network security and lawful intercept systems as well as spectrum scanners. Utilizing limited resources, they cause very minimal impact on the host network services.
- More Miles per Watt: SPARROW devices can be several miles apart exploiting broadcast power of base stations or non-terrestrial technologies. The range can be further extended by deploying several of them in a geographically sparse mesh network.
- Low Power & Low Complexity: SPARROW devices can utilize existing protocol implementation libraries installed on commodity SDRs. They can operate on batteries or harvest energy from the environment for long durations, just like real sparrows!
  REFERENCES

  > There are no direct references of prior study that I (Reza) have (aside from general knowledge of 5G standard and RF), however the following talks and items led me towards this discovery:
- DEF CON Safe Mode - James Pavur - Whispers Among the Stars - https://www.youtube.com/watch?v=ku0Q_Wey4K0
- DNS Data Exfiltration techniques
- My boss buying me a 5G base station emulator and saying "find something wrong with this!"

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=oaLIo9HwW-g

Media

(Main Talk)
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%2

(Demo)
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20R

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

HRV - Friday - 12:30-13:30 PDT

Title: Spectrum Coordination for Amateur Radio
When: Friday, Aug 6, 12:30 - 13:30 PDT
Where: Ham Radio Village (Virtual Talks)

SpeakerBio: Bryan Fields
Bryan Fields, W9CR, is one of the founding members of the Florida Amateur Spectrum Management Association ("FASMA") and operates a number of wide coverage repeaters in the Tampa Bay region. Bryan holds several FCC licenses, he was first licensed in 1995 at age 10, and holds a GROL+RADAR license as well. He's served as a technical committee member to ARDC, the holder of 44/8 ("AMPRNET"), and is a founding member of AllStarLink. Professionally Bryan has worked in the carrier networking space, focusing on IP/MPLS networks and wireless communications. Currently he is a senior consulting engineer with a major router vendor.

Description:

In this presentation we'll cover the basis for coordination of repeater and other other stations in the amateur radio service. The theory will focus on the practices used in Florida, but generally are applicable to other coordination bodies.

All Ham Radio Village talks will be streamed to Twitch, with discussion in Discord.

For more information, see https://hamvillage.org/dc29.html

Twitch: https://www.twitch.tv/hamradiovillage

#hrv-presentation-text: https://discord.com/channels/708208267699945503/736674835413073991

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Friday - 16:00-16:30 PDT

Title: State of Cryptocurrency Ransomware AMA
When: Friday, Aug 6, 16:00 - 16:30 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Guillermo Christensen
No BIO available

Description:
Guillermo will give an overview of the state of cryptocurrencies and ransomware, focusing on what he hears in the national security/law Enforcment sector plus incident response and then work on what options are there for addressing the proliferation of ransomware tied to cryptocurrencies but avoiding some of the global solutions like banning.

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Saturday - 14:00-14:59 PDT

Title: Staying Fresh While the Feds Watch: Changes in Government Surveillance and Why it Matters
When: Saturday, Aug 7, 14:00 - 14:59 PDT
Where: Crypto & Privacy Village (Virtual)

SpeakerBio: Anthony Hendricks
Anthony Hendricks is an attorney who advises clients as the chair of Crowe & Dunlevy’s Cybersecurity & Data Privacy Practice Group. In that role, he frequently analyzes and litigates legal issues related to IoT devices. Prior to beginning his practice, he studied as Howard University's first Marshall Scholar and later graduated from Harvard Law School. He now teaches cybersecurity law as an adjunct professor at Oklahoma City University School of Law.

Description:

Technology is constantly changing and evolving. While our laws are slow to keep up, this hasn’t stopped the government from adapting. Whether it’s using IoT devices as informants, paying for access to databases of information that the government could not collect without a warrant, or the increased use of facial recognition software, government surveillance is changing. This presentation will explore the current trends in government surveillance and investigations, the gaps in the law, the impact on all of us, and what we should be asking the law to do.

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 11:30-11:55 PDT

Title: Steal This Drone: High-Assurance Cyber Military Systems
When: Friday, Aug 6, 11:30 - 11:55 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Darren Cofer
Darren Cofer is a Fellow at Collins Aerospace. He earned his PhD in Electrical and Computer Engineering from The University of Texas at Austin. He has worked in the aerospace industry for 26 years, applying formal methods for verification and certification of high-integrity systems.

Description:

As part of DARPA's High Assurance Cyber Military Systems program, Collins Aerospace led a team of researchers developing new tools for building aircraft software that is provably secure against many classes of cyber attack. We developed system architecture models, software components, and operating system software which have been mathematically analyzed to ensure key security properties. This talk describes the research results and demonstration in-flight on a military helicopter.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=gjYNu-2IEnc

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 12:00-12:30 PDT

Title: Strategic Trust and Deception in the Internet of Things
When: Saturday, Aug 7, 12:00 - 12:30 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Juneau Jones
Raised in the woods of Alaska, Juneau attributes her love of hacking to a childhood spentbuilding and breaking things outside. After studying computer science and economics, she moved to Dallas, Texas, where she found a home in the local hacker community. Juneau began research on applying behavioral economics to adversarial tactics. After her successful first talk at Dallas Hacker's Association on the prisoner's dilemma, she began presenting her research at cons across the country. Currently, she works as an adversarial analyst doing consultant red teaming. She is also continuing her research and education as a cybersecurity fellow at NYU. When she is not hacking or asking strangers to act out the prisoner's dilemma, Juneau breathes fire, plays the bass, and runs DC214; Dallas's DefCon group.

Description:

Game Theory is the study of choices and strategies made by rational actors, called ""players,"" during times of conflict or competition. It has been used throughout history to map human conflict. Statisticians use game theory to model war, biology, and even football. In this talk, we will model interactions between IoT devices based on strategic trust; how agents decide to trust each other. The talk will provide an overview of game-theoretic modeling and its application to the IoT landscape. The landscape facilitates deception; players must decide whether or not to trust other agents in the network, and agents may have misaligned incentives. There is a trade-off between information gained and short-term security. This talk will build a framework for predictive and strategic trust where players make decisions based on the incentives of their ""opponents."" This talk will not look at network topology or protocols but will instead look at information exchange and strategy.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Structured Analytical Techniques for Improving Information Security Analyses
When: Saturday, Aug 7, 17:00 - 17:30 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Rabbit
Rabbit is an information security engineer and lagomorph enthusiast with a background in medical device security and biometric access system assessment who now manages the secure development and testing of IoT smart home and smart lock devices.
Twitter: @ra6bit

Description:

Based on tradecraft documents openly published by the CIA, this talk takes structured analytical techniques intended for intelligence analysis and refactors them for use in improving typical Information Security investigations and analyses as well as OSINT investigations.

In 2009, the Central Intelligence Agency published a document titled "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis " which lays out a number of techniques for improving the accuracy and reliability of intelligence analyses. I found the document fascinating and set out to reapply the techniques for use in my day to day Information Security work. The techniques are a fantastic tool set for improving the quality of analysis products by bringing alternative narratives and solutions to light, highlighting contradictory evidence, and developing confidence in analysis conclusions. Additionally there are techniques for imaginatively creating and evaluating new scenarios which may fit a given set of evidence.

The techniques can be divided into three categories. "Diagnostic Techniques", which are intended to assess and improve the quality of source material used in an analysis. "Contrarian Techniques", which are intended to surface potential alternate hypotheses that fit the information available, and "Imaginative Thinking" techniques which are used to generate new starting points for hypotheses that can then be developed further by applying the previous techniques.

An example of a Diagnostic technique is a "Key assumptions check". This exercise is simply to list all of the assumptions that have been made within an analysis, which can then be analyzed to identify unsupported assumptions or assumptions with excessive uncertainty. In an information security context, such as during incident response, this type of analysis can illuminate where assumptions have been made that can't be verified, such as confusing correlation with causation, or when errors have been made due to trusting timing information sources without verifying other reference events are properly synchronized in the source material. In an OSINT investigation, this technique can help weed out correlations that have been made based on dubious evidence.

An example of a Contrarian technique most people are probably familiar with already is the "Devils advocate" technique, where narratives are created which intentionally directly refute the hypothesis of the analysis to be improved. These opposite narratives are then evaluated to determine if they could be valid primary hypotheses. A lesser known technique, however, would be a "High Impact/Low probability" analysis, where an incident is analyzed in reverse. If the event is assumed to be a foregone conclusion, analyzing what conditions would necessarily have to have occurred for that condition to be possible can lead to the identification of additional places where supporting evidence may be available, or it may lead to a hypothesis being rejected as not fitting the available evidence.

An example of an Imaginative analysis is the "Red Team analysis". While a lot of people in Information Security will be familiar with what a red team is, particularly in the BTV, in this technique, the focus is on analyzing the red team itself, rather than applying red team techniques. What this means is to analyze the driving motivations of the adversary and factors which may influence their behavior as attackers. It's more like "red teaming the red team" to develop an idea of how and why they may act in a certain way in a given situation. In the information security realm, an example of applying this sort of technique is to develop a potential model of a threat based on their TTPs, then use that to determine if there are other investigations that should occur. For instance, if a breach was caused by a hacktivist, the ultimate goal of their attack may be completely different than that of a corporate rival, or a nation state, and identifying those motivations can help you further understand the motives and meanings behind the actions they take and their ultimate goals within your systems.

The final portion of this talk would be to apply some of the techniques to sample sets of evidence to illustrate how each technique can be applied, and how each can improve, support, or refute the initial hypothesis.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 21:00-20:59 PDT

Title: Subtle and Not So Subtle Ways to Lose Your Cryptocurrency
When: Thursday, Aug 5, 21:00 - 20:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Josh McIntyre , Software Engineer, Founder of Chaintuts
Josh McIntyre is a software engineer and tech educator with a passion for learning and teaching others. His project chaintuts hopes to educate people on the fascinating world of cryptocurrency and security with free and open-license content.

Description:

As the cryptocurrency ecosystem grows, thieves and scammers are evolving their tactics to get their piece of someone else's crypto pie. This talk will examine common ways that users lose cryptocurrency, and how to prevent these types of attacks. We will cover attack vectors such as malware, social engineering, user error, and more.

This talk is now available on YouTube: https://www.youtube.com/watch?v=npvSnOiqh10

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 10:00-10:45 PDT

Title: Summer of Fuzz: MacOS
When: Friday, Aug 6, 10:00 - 10:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Jeremy Brown
Jeremy is a security professional largely focused on offensive and application security along with vulnerability research and automation. He has gained extensive software security experience working at software and service companies, large and small, for over a decade as well as publishing research in the security community. He has taken the opportunity to gain expertise in many different areas including bug hunting, app/prod/infra security, fuzzing, as well as breaking cloud and web services and enjoys all things interesting in the realm of computer security.

Description:

Thinking of fuzzing applications on OS X can quickly lead to a passing conversation of "ooh exotic Mac stuff", "lets fuzz the kernel" or it can otherwise not be thought of as an exciting target, at least for looking for crashes in stuff other than Safari or the iPhone. While there are some intricacies and nuance involved, workaround for security protections to enable debugging and finding tools that work and work well, this research will detail how it can be done in a reliable way and make the topic more tangible and easier to digest, kind of like how people think about using AFL on Linux: it "just works". We'll explore some of the overlooked attack surfaces of file parsers and some network services on Mac, how to fuzz userland binaries and introduce a new fuzzer that makes setup and crash triage straightforward while poking at some Apple core apps and clients. Have you ever thought "This thing has got to have some bugs" but think twice because it's only available on Mac and not worth the effort? If so, you may now find yourself both more motivated and better equipped to do some bug hunting on the sleek and eventually accommodating Mac OS.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Friday - 16:00-16:30 PDT

Title: Surviving 51% Attacks on Blockchains
When: Friday, Aug 6, 16:00 - 16:30 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Yaz Khoury , Developer Realtions Engineer at Celo
Yaz Khoury is currently a developer relations engineer at Celo, mobile-first smart contract blockchain. Previously he was the Director of Developer Relations at Ethereum Classic. He has worked on many new toolings to help the blockchain ecosystem in infrastructure and security, including building Ethercluster, an open-source alternative to Infura with infra-as-code design specifications for cloud blockchain deployments. He has also built ForkWatch, a simple anomaly detection tool for NiceHash rentable-mining market to track if it's being used for 51% attacks. He has done lots of volunteer work in the blockchain space as a judge and mentor at hackathons like ETHDenver and ETHBerlin and Celo Camp, a speaker at Consensus and TABConf and EDCON. He also has done Ethereum webinars and education for Hyperledger Foundation and was the co-chair of the Testnet Working Group of the Enterprise Ethereum Alliance. His favorite industry topics are on-chain attacks and Miner-Extractable Value (MEV).

Description:
The talk highlights the speakers experience managing four 51% attacks on the Ethereum Classic network and how the attacks were each different and unfolded. Yaz goes over each event and how it impacted the network, how to minimize such events, and he goes over ways to monitor and respond to such attacks using existing and new tools in the space.

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Sunday - 10:15-11:30 PDT

Title: Surviving DeFi: How to Prevent Economic Attacks
When: Sunday, Aug 8, 10:15 - 11:30 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Jan Gorzny , Senior Blockchain Researcher at QuantStamp
No BIO available

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Thursday - 07:00-06:59 PDT

Title: Table Top Exercise - Deus Ex Machina (Pre-registration Required)
When: Thursday, Aug 5, 07:00 - 06:59 PDT
Where: Biohacking Village (TTX)

Description:
https://www.villageb.io/ttx

Return to Index - Add to Google Calendar - ics Calendar file

Title: Taking Apart and Taking Over ICS & SCADA Ecosystems: A Case Study of Mitsubishi Electric
When: Sunday, Aug 8, 10:00 - 10:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Mars Cheng,Selmon Yang

SpeakerBio: Mars Cheng
Mars Cheng (@marscheng_) is a threat researcher for TXOne Networks, blending a background and experience in both ICS/SCADA and enterprise cybersecurity systems. Mars has directly contributed to more than 10 CVE-IDs, and has had work published in three Science Citation Index (SCI) applied cryptography journals. Before joining TXOne, Mars was a security engineer at the Taiwan National Center for Cyber Security Technology (NCCST). Mars is a frequent speaker and trainer at several international cyber security conferences such as Black Hat Europe, SecTor, FIRST, HITB, ICS Cyber Security Conference Asia and USA, HITCON, SINCON, CYBERSEC, CLOUDSEC and InfoSec Taiwan as well as other conferences and seminars related to the topics of ICS and IoT security. Mars is general coordinator of HITCON (Hacks in Taiwan Conference) 2021 and was vice general coordinator of HITCON 2020.
Twitter: @marscheng_

SpeakerBio: Selmon Yang
Selmon Yang is a Staff Engineer at TXOne Networks. He is responsible for parsing IT/OT Protocol, linux kernel programming, and honeypot development and adjustment. Selmon also spoke at ICS Cyber Security Conference Asia, HITCON, SecTor and HITB.

Description:
Diversified Industrial Control System (ICS) providers create a variety of ecosystems, which have come to operate silently in the background of our lives. Among these organizations, Mitsubishi Electric ranks among the most prolific. Because the operation of this ecosystem is so widely used in key manufacturing, natural gas supply, oil, water, aviation, railways, chemicals, food and beverages, and construction, it is closely-related to people's lives. For this reason, the security of this ecosystem is extraordinarily important.

This research will enter the Mitsubishi ecosystem's communication protocol, using it as a lens with which to deeply explore the differences between itself and other ecosystems. We will show how we successfully uncovered flaws in its identity authentication function, including how to take it over and show that such an attack can cause physical damage in different critical sectors. We'll explain how we accomplished this by applying reverse engineering and communication analysis. This flaw allows attackers to take over any asset within the entire series of Mitsubishi PLCs, allowing command of the ecosystem and full control of the relevant sensors. A further complication is that making a fix to the various communication protocols in the ICS/SCADA is extremely difficult. We will also share the various problems we encountered while researching these findings and provide the most workable detection and mitigation strategies for those protocols.

REFERENCES
[1] https://ladderlogicworld.com/plc-manufacturers/ [2] https://www.mitsubishielectric.com/fa/products/cnt/plc/pmerit/case.html [3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5594 [4] https://www.mitsubishielectric.com/fa/products/cnt/plc/pmerit/index.html

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=L0w_aE4jRFw

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20M

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

Title: TEMPEST radio station
When: Saturday, Aug 7, 13:00 - 13:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Paz Hameiri
Paz started his professional life 30 years ago, hacking games and developing tools in his teen years. Since then, he has worked in several companies, developing both hardware and software.

Paz has six years of experience with telecommunication systems design and circuits. He explored GPU hardware and software design in his Master's thesis. For 12 years, Paz led multidisciplinary systems development as a systems engineer in an international homeland security company.

At home, Paz explores ideas he finds interesting. In 2019 he published his work on a body-tracking device that records keystrokes on a safe's keypad.

https://il.linkedin.com/in/paz-hameiri-251b11143

Description:

TEMPEST is a cyber security term that refers to the use of electromagnetic energy emissions generated by electronic devices to leak data out of a target device. The attacks may be passive (where the attacker receives the emissions and recovers the data) or active (where the attacker uses dedicated malware to target and emit specific data).

In this talk I present a new side channel attack that uses GPU memory transfers to emit electromagnetic waves which are then received and processed by the attacker. Software developed for this work encodes audio on one computer and transmits it to the reception equipment positioned fifty feet away. The signals are received and processed and the audio is decoded and played. The maximum bit rate achieved was 33kbit/s and more than 99% of the packets were received.

Frequency selection not only enables maximization of signal quality over distance, but also enables the attacker to receive signals from a specific computer when several computers in the area are active. The software developed demonstrates audio packets transfers, but other types of digital data may be transmitted using the same technique.

REFERENCES

> Eck W. “Electromagnetic radiation from video display units: an eavesdropping risk?” Computers and Security, 4, no. 4: 269-286, 1985. Kuhn, M. G., and Anderson, R. J. Soft. “Tempest: Hidden Data Transmission Using Electromagnetic Emanations.” In Information Hiding (1998), ed. D. Aucsmith, vol. 1525 of Lecture Notes in Computer Science, (Springer): 124–142. Thiele, E., “Tempest for Eliza.” 2001. http://www.erikyyy.de/tempest/. Kania B., “VGASIG: FM radio transmitter using VGA graphics card.” 2009. http://bk.gnarf.org/creativity/vgasig/vgasig.pdf. Guri M., Kedma G., Kachlon A., Elovici Y. “AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies.” In Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on IEEE, 2014: 58-67. 2pkaqwtuqm2q7djg,"OVERCLOCKING TOOLS FOR NVIDIA GPUS SUCK, I MADE MY OWN". 2015. https://1vwjbxf1wko0yhnr.wordpress.com/2015/08/10/overclocking-tools-for-nvidia-gpus-suck-i-made-my-own/ nvapioc project: https://github.com/Demion/nvapioc SDRplay API Specification v3, https://www.sdrplay.com/docs/SDRplay_API_Specification_v3.pdf Simon Rockliff's Reed-Solomon encoding-decoding code at http://www.eccpage.com/rs.c

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=m9WkEwshNKc

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20P

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

BICV - Friday - 12:30-12:30 PDT

Title: The Action Plan for Cyber Diversity!
When: Friday, Aug 6, 12:30 - 12:30 PDT
Where: Blacks in Cyber

SpeakerBio: Keith Chapman
Keith Chapman is an information security professional, cyber education chair and conference presenter. His background includes incident response, threat intelligence and governance, risk and compliance. He also invests in the information security community by attending and speaking at and conferences. Keith serves as the Cincinnati, OH ambassador for Blacks in Cyber. He is committed to increasing diversity, equity, and inclusion in our field and mentors students in the Ohio Public School System, specifically the Cyber Academy.
Twitter: @S1lv3rL10n

Description:
What does it take to increase diversity, equity, and inclusion in information security? An inside perspective with actionable steps. These actions will build a stronger defense and future for us all.

Blacks in Cyber talks will be streamed on YouTube.

YouTube: https://www.youtube.com/c/BlacksInCybersecurity

Return to Index - Add to Google Calendar - ics Calendar file

Title: The Agricultural Data Arms Race: Exploiting a Tractor Load of Vulnerabilities In The Global Food Supply Chain
When: Sunday, Aug 8, 14:30 - 14:50 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Sick Codes
Sick Codes maintains popular open source projects, publishes high-profile security vulnerabilities in good faith, and administers his namesake https://sick.codes, a security research and tutorial resource for developers. Sick Codes' work coordinating communication across many companies, foundations, and other open source organisations was invaluable in getting these vulnerabilities patched and responsibly disclosed.

Sick Codes: I am a Hacker, an Independent Security Researcher, an Australian, and an Open Source maintainer. I regularly publish nasty vulnerabilities in everyone's favorite products, from all the best vendors. I've published CVEs in Smart TV's, Browsers, missile design software, and entire programming languages. Freelance automation specialist by day and hacker by trade. I publish weaponized code on GitHub, namely Docker-OSX, which was my first big "thing," which now has 15k stars, and my biggest project, Docker-OSX has over 100,000 downloads on DockerHub.

@sickcodes
https://github.com/sickcodes
https://www.linkedin.com/in/sickcodes/
https://sick.codes

Twitter: @sickcodes
https://sick.codes

Description:
How I hacked the entire American Food Supply Chain over the course of 3 months, assembled a team of hacker strangers, and how we used a "full house" of exploits on almost every aspect of the agriculture industry. See the process in which it happened, the private exploits we used, the vectors we attacked from, and how it could happen again, or be happening right now.

How the ongoing analytics arms race affects everyone, and how Tractor companies have metastasized into Tech companies, with little to no cyber defenses in place. Learn how farms are not like they used to be; telemetry, crop & yield analytics, and more telemetry.

REFERENCES

https://github.com/sickcodes/Docker-OSX https://github.com/sickcodes/osx-serial-generator
https://www.vice.com/en/article/akdmb8/open-source-app-lets-anyone-create-a-virtual-army-of-hackintoshes
https://www.bleepingcomputer.com/news/security/python-also-impacted-by-critical-ip-address-validation-vulnerability/
https://sick.codes/sick-2021-012/ https://sick.codes/sick-2021-031/
https://sick.codes/leaky-john-deere-apis-serious-food-supply-chain-vulnerabilities-discovered-by-sick-codes-kevin-kenney-
https://www.vice.com/en/article/4avy8j/bugs-allowed-hackers-to-dox-all-john-deere-owners
https://www.youtube.com/watch?v=rB_SleNKBus wabaf3t https://twitter.com/wabafet1 D0rkerDevil
https://twitter.com/D0rkerDevil ChiefCoolArrow https://twitter.com/ChiefCoolArrow johnjhacking
https://twitter.com/johnjhacking rej_ex https://twitter.com/rej_ex w0rmer https://twitter.com/0x686967
https://climate.com/press-releases/transform-data-into-value-with-climate-fieldview/14
https://www.agriculture.com/news/business/john-deere-to-acquire-precision-plting_5-ar50937
https://www.reuters.com/article/us-monsanto-m-a-deere-idUSKBN17X2FZ
https://twitter.com/sickcodes/status/1385218039734423565?s=20

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=zpouLO-GXLo

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20S

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 09:30-10:20 PDT

Title: The Antenny Board Design and Fabrication Saga: Sweat and Tears Along the Supply Chain
When: Friday, Aug 6, 09:30 - 10:20 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Ang Cui
Dr. Ang Cui is the Founder and Chief Scientist of Red Balloon Security. Dr. Cui received his PhD from Columbia University in 2015. Ang has focused on developing technologies to defend embedded systems. He has also uncovered vulnerabilities within embedded devices like Cisco routers and HP printers.

Description:
Over the past few months, Red Balloon Security has been developing and manufacturing the Antenny v5 board, and like anyone else who is putting together hardware, we ran headlong into the famous chip shortage. Listen to our story of how we overcame the shortage, found the most treasured of surprises in the most unlikely of places, and distilled all the drama into the little purple boards over in the Aerospace Village area.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=5trlb5hEXAw

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

RFV - Saturday - 08:00-07:59 PDT

Title: The Basics of Breaking BLE - Part 2: Doing More With Less

When: Saturday, Aug 7, 08:00 - 07:59 PDT

Where: Radio Frequency Village (Virtual)

SpeakerBio:freqy

Freqy is a security consultant and researcher with a particular interest in wireless technologies like BLE, ZigBee, Wi-Fi, etc. She has spent the past two year working with companies to help improve the wireless security of devices found in millions of homes and businesses.
Twitter: @freqyXin

Description:

Part 2 of this series continues our discussion on BLE security with an introduction to some additional testing methods using affordable devices and open-source software. From there, we'll talk about scripting simple BLE attacks, dealing with BlueZ, and exploring BLE devices in the wild. Attendees will also have the opportunity to field questions about BLE security during a live Q/A session following the video.

Radio Frequency Village will not be streaming any talks, but they will be making talks available on their YouTube channel.

YouTube: https://youtube.com/c/RFHackersSanctuary

Return to Index - Add to Google Calendar - ics Calendar file

BICV - Friday - 14:30-14:30 PDT

Title: The Big Cleanup: Tackling The Remnants of Systematic Discrimination in the Tech Industry
When: Friday, Aug 6, 14:30 - 14:30 PDT
Where: Blacks in Cyber

SpeakerBio: Maurice Turner
Maurice Turner is the Cybersecurity Fellow at the Alliance for Securing Democracy at the German Marshall Fund of the United States. He is a recognized public interest technologist and cybersecurity expert focused on developing strategies to secure critical infrastructure and deter cyber operation escalation. He has also provided testimony before the United States Congress, shared his insights with the European Union, and spoken at numerous security conferences. He most recently served as Senior Advisor to the Executive Director at the United States Election Assistance Commission, where he provided subject matter expertise in support of local, state, and federal partners to administer elections fairly and securely. Prior to that he was Deputy Director of the Internet Architecture project at the Center for Democracy & Technology, where he led the Election Security and Privacy Project, identifying and updating election cybersecurity practices and infrastructure through multi-sector partnerships. He also served as a TechCongress Congressional Innovation Fellow assigned to the U.S. Senate Homeland Security and Governmental Affairs Committee, where he shaped policy and oversaw the preparation of memos, briefings, and hearings on federal Information Technology systems, cybersecurity threats, and cybersecurity regulations. He holds an MA in Public Administration from the University of Southern California, an BA in Political Science from California State University Fullerton, and a Certificate in Cybersecurity Strategy from Georgetown University.
Twitter: @TypeMRT

Description:
It’s easy to just accept the status quo even when it’s harmful because that’s just how it’s always been done. Discrimination in the tech industry is no different. The reuse and amplification of discriminatory language can have damaging effects on those within the industry, as well as in other physical spaces. It adds to the barriers that prevent folks from even trying to participate because they think that they don’t belong. ã
Using technology to challenge how concepts are labeled can help break down those barriers and drive inclusivity. Changing how practitioners label concepts like Whitelist/Blacklist and Master/Slave makes the tech industry more inclusive internally. We can also use technology to uncover remnants of discrimination in the analog world. Thousands of geographic places across the country have official names that are racist like Negro Run and Squaw Creek. They are now easy to find using services like Google Maps. When those names are changed, everyone can see the update immediately. ã
Old baggage has a way of sticking around when new systems are built using legacy data. Regardless of my role in organizations, I look for ways to turn that around and cleanup some of those remnants of systematic discrimination. I will highlight two of those experiences where I have been able to make small changes with big impact by ensuring inclusive language in voting securing standards and changing the racist name of a river using a mapping service. I hope you see that you too can make small changes that make a difference at scale.

Blacks in Cyber talks will be streamed on YouTube.

YouTube: https://www.youtube.com/c/BlacksInCybersecurity

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 12:00-12:30 PDT

Title: The Black Box and the Brain Box: When Electronics and Deception Collide
When: Friday, Aug 6, 12:00 - 12:30 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Gigs
Gigs is the founder of ##electronics on Freenode (may it rest in peace), and a long time electronics enthusiast and DEF CON HHV volunteer. He, working with see_ess, did the PCB and hardware design for this year's TorBadge, a mini-polygraph device.
Twitter: @gigstaggart
gigsatdc.org

Description:
Electricity has, from the earliest history of man, been seen as an almost mystical force. From Thor's lightning onward, various individuals and groups have used electricity and electrical devices to baffle, mystify, mislead, and control people. In the modern day, this practice continues in the form of polygraph, questionable uses of fMRI and EEG, and other high-tech props intended to dazzle the victim or lend a technological veneer of credibility to the user. This talk will focus on the history and current applications of deception by and with electrical and electronic devices.

#hhv-talk-qa-blackbox-brainbox-text https://discord.com/channels/708208267699945503/709254868329693214

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 10:30-10:59 PDT

Title: The Black Box and the Brain Box: When Electronics and Deception Collide
When: Saturday, Aug 7, 10:30 - 10:59 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Gigs
Gigs is the founder of ##electronics on Freenode (may it rest in peace), and a long time electronics enthusiast and DEF CON HHV volunteer. He, working with see_ess, did the PCB and hardware design for this year's TorBadge, a mini-polygraph device.
Twitter: @gigstaggart
gigsatdc.org

Description:

Electricity has, from the earliest history of man, been seen as an almost mystical force. From Thor's lightning onward, various individuals and groups have used electricity and electrical devices to baffle, mystify, mislead, and control people. In the modern day, this practice continues in the form of polygraph, questionable uses of fMRI and EEG, and other high-tech props intended to dazzle the victim or lend a technological veneer of credibility to the user. This talk will focus on the history and current applications of deception by and with electrical and electronic devices.

#hhv-talk-qa-blackbox-brainbox-text https://discord.com/channels/708208267699945503/709254868329693214

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Sunday - 15:00-15:30 PDT

Title: The Black Box and the Brain Box: When Electronics and Deception Collide
When: Sunday, Aug 8, 15:00 - 15:30 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio: Gigs
Gigs is the founder of ##electronics on Freenode (may it rest in peace), and a long time electronics enthusiast and DEF CON HHV volunteer. He, working with see_ess, did the PCB and hardware design for this year’s TorBadge, a mini-polygraph device.
Twitter: @gigstaggart
gigsatdc.org

Description:
Electricity has, from the earliest history of man, been seen as an almost mystical force. From Thor’s lightning onward, various individuals and groups have used electricity and electrical devices to baffle, mystify, mislead, and control people. In the modern day, this practice continues in the form of polygraph, questionable uses of fMRI and EEG, and other high-tech props intended to dazzle the victim or lend a technological veneer of credibility to the user. This talk will focus on the history and current applications of deception by and with electrical and electronic devices.

#hhv-talk-qa-blackbox-brainbox-text https://discord.com/channels/708208267699945503/709254868329693214

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Saturday - 10:40-11:10 PDT

Title: The Bug Hunter’s Recon Methodology
When: Saturday, Aug 7, 10:40 - 11:10 PDT
Where: Recon Village (Virtual)

SpeakerBio: Tushar Verma
No BIO available
Twitter: @e11i0t_4lders0n

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

LPV - Saturday - 15:00-15:30 PDT

Title: The Coat Hanger Talk: A Noob's Look Into the Thieves World
When: Saturday, Aug 7, 15:00 - 15:30 PDT
Where: Lock Pick Village (Virtual)

SpeakerBio: De
No BIO available

Description:
The talk starts with me describing a typical work environment, and explaining how creativity is a fundamental for the LPV. I, As a noob, steps into the shoes of a broad audience and explains how creativity is a huge issue when it comes to basic security, both physical, with locks, and a bit with software.

Lock Pick Village will be streaming their activities to Twitch and YouTube.

Twitch: https://www.twitch.tv/toool_us?

YouTube: https://youtube.com/c/TOOOL-US

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 11:00-11:59 PDT

Title: The Coming AI Hackers
When: Friday, Aug 6, 11:00 - 11:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Bruce Schneier
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 11:00-11:59 PDT

Title: The Coming AI Hackers
When: Saturday, Aug 7, 11:00 - 11:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Bruce Schneier
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 11:00-11:45 PDT

Title: The Curious case of knowing the unknown
When: Saturday, Aug 7, 11:00 - 11:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Vandana Verma Sehgal
No BIO available

Description: No Description available

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Friday - 11:00-11:45 PDT

Title: The Digital Physiome - How wearables can (and are) transforming healthcare
When: Friday, Aug 6, 11:00 - 11:45 PDT
Where: Biohacking Village (Talk - Virtual)
Speakers: Jennifer Goldsack,Jessilyn Dunn

SpeakerBio: Jennifer Goldsack , CEO at the Digital Medicine Society (DiMe)
No BIO available

SpeakerBio: Jessilyn Dunn , ãAssistant Professor of Biomedical Engineering, Duke University
No BIO available

Description:
Only in the recent past have accurate and scalable methods for biometric monitoring and edge computing become possible, providing a unique opportunity to collect and analyze continuous physiologic measurements and enabling a new mechanistic understanding of acute and chronic diseases. We are focused on using digital health tools such as wearables and smart phones to uncover physiologic signatures of disease, which we refer to as digital biomarkers and that can serve as sentinels of disease onset. Overall, we aim to develop tools and infrastructure using digital health data for disease detection, monitoring, and intervention.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 11:00-11:45 PDT

Title: The Fault in Our Stars - Attack vectors for APIs using AWS API Gateway Lambda Authorizers
When: Friday, Aug 6, 11:00 - 11:45 PDT
Where: Cloud Village (Virtual)
Speakers: Alexandre Sieira,Leonardo Viveiros

SpeakerBio: Alexandre Sieira
Alexandre Sieira is a successful information security entrepreneur with a global footprint since 2003. He began his security career as a Co-Founder and CTO of CIPHER, an international security consulting and MSSP from Brazil acquired in 2018 by Prosegur. In 2015, became Co-Founder and CTO of Niddel, a bootstrapped security analytics SaaS startup running entirely on the cloud, which won a Gartner Cool Vendor award in 2016. After the acquisition of Niddel by Verizon in January 2018, he became the Senior manager and global leader of the Managed Security Services - analytics products management team in the Detect & Respond portfolio tower at Verizon. In late 2019 founded Tenchi Security, a company that focuses on cloud security solutions and services. Experienced speaker featured at Black Hat, DEF CON Cloud Village, BSides San Francisco, FIRST Conference and others.
Twitter: @AlexandreSieira

SpeakerBio: Leonardo Viveiros
A Software Engineer at heart, Leonardo has been working in tech in different roles, from interacting with clients to building robust, scalable solutions. Experienced in building Cloud Native solutions as well as Front-end applications. Led the product roadmap of a smart mobility startup from Rio de Janeiro. Current DevSecOps Specialist at Tenchi Security enabling our clients to achieve a safer software development life cycle.
Twitter: @LeonardoViveiro

Description:
Serverless applications are a really interesting new trend that promises benefits such as increased scalability and reduced cost. Frameworks like Serverless Application Model (SAM) and Serverless Framework are increasingly used to build them. APIs are a natural part of serverless applications, and in AWS that typically is implemented using the AWS API Gateway backed by Lambdas that implement the actual API endpoint logic. Our research focused on API Gateway Lambda Authorizers. This is a feature that allows developers to use a custom authentication and authorization scheme that uses a bearer token authentication strategy (like JWTs, OAuth or SAML), or that uses request parameters to determine the caller's identity and enforce which API endpoints they are allowed to access. We will present (AFAIK novel) techniques to attack the authentication and authorization of APIs that use Lambda Authorizers. We show how IAM policy injection is possible in theory but highly unlikely in practice due to some good decisions by AWS. We also show a class of problems based on incorrect security assumptions baked into AWS' own documentation and Lambda Authorizer open source code templates. Sample source code will be provided to demonstrate all techniques.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 22:30-23:30 PDT

Title: The Hangar – Cocktail Making Event

When: Saturday, Aug 7, 22:30 - 23:30 PDT

Where: Aerospace Village (Workshop - Paris Rivoli B)

Description:

There's nothing like a nice cocktail after a long day of travel and/or hacking! Come join us Saturday afternoon for a cocktail building session. We'll be making and tasting the most appropriate cocktail, the Aviation, which evokes beautiful clouds and sunsets. It's sophisticated and full of gin (just like our UK friends). We're working on a virtual version where we will publish a CBOM – Cocktail Bill of Materials, so you know what to collect/purchase to build your own while we share one with you, no matter your location.

Return to Index - Add to Google Calendar - ics Calendar file

SEV - Saturday - 13:30-14:30 PDT

Title: The Innocent Lives Foundation: A Beacon of Light in a Dark World
When: Saturday, Aug 7, 13:30 - 14:30 PDT
Where: Social Engineer Village (Virtual)

SpeakerBio: John McCombs
John McCombs serves as the Executive Assistant to the ILF, where he assists in administrative duties, fundraising, project management and public speaking. At age 12, John began his first job in the industry as a web developer, and shortly thereafter, as a help-desk operator at an international health supplement company.

In addition to having over a decade of experience in the technology industry, John also holds a bachelor's degree in Teaching English to Speakers of Other Languages (TESOL) and has had extensive training in public speaking.

Description:

The Innocent Lives Foundation: A Beacon of Light in a Dark World, is a talk to bring awareness to the ILF and the mission of identifying and bringing child predators to justice. Topics will include an introduction to the ILF, our mission, our vision, why we are needed now more than ever, our stance on vigilantism, and neutrality. We wish to introduce the ILF to a broad audience and encourage involvement through financial support and ambassadorship.

Social Engineer Village will stream content to Twitch.

Twitch: https://www.twitch.tv/socialengineerllc

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 17:15-17:59 PDT

Title: The Journey of Establishing IoT Trustworthiness and IoT Security Foundation
When: Saturday, Aug 7, 17:15 - 17:59 PDT
Where: IoT Village (Talk - Virtual)
Speakers: Amit Elazari,Anahit Tarkhanyan,Ria Cheruvu

SpeakerBio: Amit Elazari
Dr. Amit Elazari is Director, Global Cybersecurity Policy, Government Affairs at Intel Corp. and a Lecturer at UC Berkeley School of Information Master in Cybersecurity program. She graduated her Doctor of Science of the Law (J.S.D.) from UC Berkeley School of Law. Her work on security and technology law has been published in leading academic journals and popular press, including The New York Times, The Washington Post and Wall Street Journal and presented in top conferences including RSA, BlackHat, USENIX Enigma, USENIX Security and more. Elazari holds three prior degrees, summa cum laude (LL.B., LL.M. in the Law and a B.A. in Business) from IDC, Israel. Her work was awarded among others a USENIX Security Distinguished Paper Award, Annual Privacy Papers for Policymakers (PPPM) Award Academic Paper Honorable Mention, Casper Bowden PET award for Outstanding Research in Privacy Enhancing Technologies, University of California, Berkeley School of Information Distinguished Faculty Award. She is currently one of the co-editors of ISO/IEC 27402 at JTC1, SC27 (in draft, IoT Security Baseline Requirements).

SpeakerBio: Anahit Tarkhanyan , Principal Engineer, Intel Corp., Network and Edge Group, IoT CTO Office
Anahit leads the security architecture of Intel edge portfolio. Her area of expertise covers security of Edge to Cloud systems and AI/ML, security standards and regulation. Anahit is IEEE Senior Member and has PhD in Distributed Computer Systems and Networks. She holds several patents, and has publications in diverse security technology. "Dr. Amit Elazari, Intel Corp., Director, Global Cybersecurity Policy, Government Affairs

SpeakerBio: Ria Cheruvu
Ria Cheruvu is an AI Ethics Lead Architect at the Intel Network and Edge engineering group working on developing trustworthy AI products. She is 17 years old, and graduated with her bachelor's degree in computer science at Harvard University at 11 and her master's degree in data science from her alma mater at 16. Her pathfinding domains include solutions for security and privacy for machine learning, fairness, explainable and responsible AI systems, uncertain AI, reinforcement learning, and computational models of intelligence. She enjoys composing piano music, ocean-gazing with her family, and contributing to open-source communities in her free time.

Description:
The Internet of Things (IoT) ecosystem holds tremendous promise to promote innovation and productivity, and societal benefits. Yet, with increased connectivity, concerns remain with the growing attack surface. While the DFECON community often focuses on the security aspects of these issues, the multidimensional nature of IoT devices and the combination of AI/ML solutions, sparked standardization activities focusing more generally on the concept of "IoT trustworthiness". This talk will introduce the audience to the latest developments in the IoT Security Policy landscape, proposals for confidence/certifications mechanisms emerging globally, and key IoT Security baseline standards developments, while exploring the connection to the IoT trustworthiness concept across the IoT Supply Chain. We will describe a case study of IoT robustness and trustworthiness applied in context of AI and smart analytics, including the importance of characterizing the behavior of data.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

WS - Friday - 10:00-13:59 PDT

Title: The Joy of Reverse Engineering: Learning With Ghidra and WinDbg
When: Friday, Aug 6, 10:00 - 13:59 PDT
Where: Workshops - Jubilee 2 (Onsite Only)

SpeakerBio: Wesley McGrew , Senior Cybersecurity Fellow
Dr. Wesley McGrew directs research, development, and offensive cyber operations as Senior Cybersecurity Fellow for MartinFederal. He has presented on topics of penetration testing and and malware analysis at DEF CON and Black Hat USA and taught a self-designed course on reverse engineering to students at Mississippi State University, using real-world, high-profile malware samples. Wesley has a Ph.D. in Computer Science from Mississippi State University for his research in vulnerability analysis of SCADA HMI systems.

Description:

While it can be intimidating to "get into" software reverse engineering (RE), it can be very rewarding. Reverse engineering skills will serve you well in malicious software analysis, vulnerability discovery, exploit development, bypassing host-based protection, and in approaching many other interesting and useful problems in hacking. Being able to study how software works, without source code or documentation, will give you the confidence that there is nothing about a computer system you can't understand, if you simply apply enough time and effort. Beyond all of this: it's fun. Every malicious program becomes a new and interesting puzzle to "solve".

The purpose of this workshop is to introduce software reverse engineering to the attendees, using static and dynamic techniques with the Ghidra disassembler and WinDbg debugger. No prior experience in reverse engineering is necessary. There will be few slides--concepts and techniques will be illustrated within the Ghidra and WinDbg environments, and attendees can follow along with their own laptops and virtual environments. We will cover the following topics:

Software Reverse Engineering concepts and terminology Setting up WinDbg and Ghidra (and building the latter from source) The execution environment (CPU, Virtual Memory, Linking and Loading) C constructs, as seen in disassembled code Combining static and dynamic analysis to understand and document compiled binary code Methodology and approaches for reverse engineering large programs Hands-on malware analysis
How to approach a "new-to-you" architecture

Registration Link:
https://www.eventbrite.com/e/the-joy-of-reverse-engineering-learning-with-ghidra-and-windbg-jubilee-2-tickets-162215935229

Prerequisites

> No previous reverse engineering experience required. Basic familiarity with programming in a high-level language is necessary (C preferred).

Materials needed:

- A laptop with a fresh Windows 10 Virtual Machine.
- Being able to dedicate 8GB RAM to the VM (meaning, you probably have 16GB in your laptop) will make the experience smoother, but you can get by with 4GB
- 10 GB storage free in the VM (after installing Windows)
- Administrative privileges
- Ability to copy exercise files from USB

We will be working with live malware samples. Depending on your comfort level with this, bring a "burner" laptop, use a clean drive, or plan on doing a clean install before and after the workshop.

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 17:00-17:30 PDT

Title: The Little Things
When: Saturday, Aug 7, 17:00 - 17:30 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Mixæl Laufer , Director of the Institute for Autonomous Medicine. Four Thieves Vinegar Collective.
No BIO available

Description:

Was 2020 not the best year for you? Has 2021 not been a huge improvement? Are you sick of being dependent on infrastructure which fails? Do you wish there was something to look forward to? The Four Thieves Vinegar Collective has been quiet, because we've been busy this last year. We have a lot of things to share.

But that's not what this talk is about. Instead of the new tools to eradicate diseases, tools to make medicines, ways to administer them, and DIY medical machinery, we're talking about just making it through the day.

There are tools which are not well known, but are easily accessible and can help you sleep better, not be hungover, clear brain fog, and take the edge off depression. These tools are not as well known as they should be, so we're talking about them.

Because as fun as the big things are, daily life is about the little things.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 12:30-12:50 PDT

Title: The Mechanics of Compromising Low Entropy RSA Keys
When: Friday, Aug 6, 12:30 - 12:50 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Austin Allshouse
Austin Allshouse is a Research Scientist at BitSight where he applies information security, statistical modeling, and distributed computing concepts to develop quantitative methods of assessing security risk. He has a decade of experience researching the technologies and methodologies underpinning digital network surveillance systems.
Twitter: @AustinAllshouse

Description:

Over the past decade, there have been a number of research efforts (and DEFCON talks!) investigating the phenomenon of RSA keys on the Internet that share prime factors with other keys. This can occur when devices have poorly initialized sources of “randomness” when generating keys; making it trivial to factor the RSA modulus and recover the private key because, unlike large integer factorization, calculating the greatest common divisor (GCD) of two moduli can be fast and efficient. When describing their research, past hackers and researchers have attested that they “built a custom distributed implementation of Batch-GCD;” which seems like one hell of a detail to gloss over, right? This talk will detail a hacker's journey from understanding and implementing distributed batch GCD to analyzing findings from compromising RSA keys from network devices en masse.

REFERENCES

Amiet, Nils and Romailler, Yolan. “Reaping and breaking keys at scale: when crypto meets big data.” DEF CON 26, 2018.

Heninger, Nadia, et al. "Mining your Ps and Qs: Detection of widespread weak keys in network devices." 21st {USENIX} Security Symposium ({USENIX} Security 12). 2012.

Hastings, Marcella, Joshua Fried, and Nadia Heninger. "Weak keys remain widespread in network devices." Proceedings of the 2016 Internet Measurement Conference. 2016.

Kilgallin, JD. “Securing RSA Keys & Certificates for IoT Devices.”
https://info.keyfactor.com/factoring-rsa-keys-in-the-iot-era. 2019

Daniel J. Bernstein. Fast multiplication and its applications, 2008.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=BRsXsUEIU70

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20A

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

RGV - Friday - 14:00-14:30 PDT

Title: The Neuroscience of Magic (Registration required)
When: Friday, Aug 6, 14:00 - 14:30 PDT
Where: Rogues Village (Virtual)

SpeakerBio: Daniel Roy
Born and raised in San Francisco, Daniel was firmly bitten by the magic bug at the age of 10. Since then, he has appeared at the world-famous Hollywood Magic Castle and the prestigious Chicago Magic Lounge. His audiences have included Fortune 500 Companies, Hollywood actors, and members of the U.S. Congress. In 2019, he became one of the youngest magicians ever to receive the Milbourne Christopher award for Close-Up Magician of the Year.

Description:
Presented via Zoom. Space is limited so please register here:

https://docs.google.com/forms/d/e/1FAIpQLSf06PkmQ1s_pAJ_L971Vm2nPXFtPUr1nut09GFZl3IuWxsfXQ/viewform

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Friday - 12:00-12:59 PDT

Title: The Next Critical Infrastructure: Understanding the Bioeconomy
When: Friday, Aug 6, 12:00 - 12:59 PDT
Where: Biohacking Village (Talk - Virtual)
Speakers: Charles Fracchia,Nathan Case

SpeakerBio: Charles Fracchia , Biomedical researcher for the digital age
No BIO available

SpeakerBio: Nathan Case
No BIO available

Description:
We will use a fictional -but highly realistic- biomanufacturing scenario and company to share with the audience how cybersecurity has become a critical component of biosecurity and public health. We will review the importance of biomanufacturing to the world's public health posture, in particular in light of the COVID19 pandemic and share how vulnerable digital technologies have become exploited vectors for global geopolitical moves.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

BICV - Saturday - 12:30-12:30 PDT

Title: The OPSEC of Protesting
When: Saturday, Aug 7, 12:30 - 12:30 PDT
Where: Blacks in Cyber

SpeakerBio: Ochaun Marshall
Ochaun (pronounced O-shawn) Marshall is an application security consultant. In his roles at Secure Ideas, he works on ongoing development projects utilizing Amazon Web Services and breaks other people's web applications. When he is not swallowing gallons of the DevOps Kool-Aid, he can be found blasting J Cole while hacking, blogging, and coding. He covers everything he does with the signature phrase: I code; I teach; I hack.
Twitter: @OchaunM

Description:

Technology both facilitates and complicates the human condition in many ways, especially in the tradition of protesting. Activists and those supporting social movements need to be aware of the risks of social demonstrations. In this talk, we dive into communication strategies for activists, as well as the basics of OPSEC. We'll do threat modeling against both nation-state & opposition movements and discuss the utility of basic security hygiene in this context. We will also examine these principles against case studies of the Civil rights movement, BLM, Hong Kong Separation movement, Election protests, and recent "hacktivist" attacks against Parler and Gab.

Blacks in Cyber talks will be streamed on YouTube.

YouTube: https://www.youtube.com/c/BlacksInCybersecurity

Return to Index - Add to Google Calendar - ics Calendar file

Title: The PACS-man Comes For Us All: We May Be Vaccinated, but Physical Access Control Still Sucks
When: Sunday, Aug 8, 11:00 - 11:45 PDT
Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded
Speakers: Anze Jensterle,Babak Javadi,Eric Betts,Nick Draffen

SpeakerBio: Anze Jensterle
Anze Jensterle is a Computer Science student by day, professional door opener by night that comes from Slovenia (not Slovakia). Having been involved with InfoSec since he was 17, when he made his first bug bounty, he has continuously been developing his skills in different areas including Web, RFID and Embedded System Security.
Twitter: @applejacksec

SpeakerBio: Babak Javadi
Babak Javadi is the Founder of The CORE Group and Co-Founder of the Red Team Alliance. In 2006 he co-founded of The Open Organisation of Lockpickers, serving as Director for 13 years. As a professional red teamer with over a decade of field experience, Babak's expertise includes disciplines from high-security mechanical cylinders to alarms and physical access controls.
Twitter: @babakjavadi

SpeakerBio: Eric Betts
Eric Betts is an exuberant, passionate, pragmatic software engineer. He is an avid open-source contributor. He likes to buy all the latest gadgets, and then take them apart. His claim to fame is making $10k from Snapchat (without taking his clothes off) for an RCE bug bounty. He responds to "Bettse" both online and in-person.
Twitter: @aguynamedbettse

SpeakerBio: Nick Draffen
Nick Draffen sometimes gives off a mad scientist vibe, an engineer who dives deep into technology, namely in the area where the physical and digital world meet. By day a security engineer/architect working to secure lab instruments and everything around them, and by night building/breaking things in his lab.
Twitter: @tcprst

Description:
It's 2021. You're still here! You're vaccinated! You should be happy and carefree! And yet…the PACS-man still haunts us all. Why should this be? Don't we have newer, better tech with more bits of encryption and fewer wires? Haven't the professional sentinels we've entrusted with our physical security software-defined ALL THE THINGS and made them better?

Nay, these are but fruits of the poisonous physical security tree! Come, fellow hackers and weary travelers, visit with the ghosts of access control and learn of the lies they've laid before us!

Come see how false guardians have used BLE slight-of-hand to increase complexity and cost while reducing security and ask that they be paid a tithing for the privilege! Witness young software-defined gladiators do battle in an arena they did not prepare for and falter!

Behold as our friendly ghosts of access control forge never-before seen tools to help slay false security prophets!

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=NARJrwX_KFY

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20E

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 14:00-14:59 PDT

Title: The Real History of Adversarial Machine Learning
When: Saturday, Aug 7, 14:00 - 14:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Eugene Neelou
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Saturday - 14:00-14:59 PDT

Title: The Real Story on Patching Medical Devices
When: Saturday, Aug 7, 14:00 - 14:59 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Michael Murray , Founder / CEO · Chief Security Officer, Scope Security
Mike Murray is the CEO of Scope Security where he builds on his nearly two decades of experience to solve critical security problems in healthcare. Prior to Scope, Murray served as the CSO at Lookout, lead pre-market security at GE Healthcare and co-founded The Hacker Academy & MAD Security.
Twitter: @mmurray

Description:
One of the constant debates in the medical device sector is around patching of medical devices. While the FDA issues clear guidance that devices can and should be patched, some device manufacturers often claim that the FDA is the reason that they can't issue patches, and the hospitals and healthcare organizations using the devices are left confused and accepting risk that they can't manage. With this panel, we will have the conversation out in front of the Defcon audience. Panelists will include representation from the FDA, a product security leader from a device manufacturer and a healthcare CISO with the goal being for the entire Defcon Biohacking Village audience to come away understanding what the truth really is about whether they can patch their devices, and how the sector can continue to move this conversation forward.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

BHV - Sunday - 13:00-13:30 PDT

Title: The Security of Your Digital DNA, from Inception to Death
When: Sunday, Aug 8, 13:00 - 13:30 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Garrett Schumacher , Cybersecurity Engineer at Velentium | Co-Founder & CTO at GeneInfoSec
Garrett Schumacher both hacks biology and defends it. He began his career in genetics and biotech, but he now focuses on infosec within these fields. He is a medical device cybersecurity engineer at Velentium, the co-founder and CTO of GeneInfoSec, and an instructor at the University of Colorado.
Twitter: @GJSchumacher

Description:

Genetic data is some of your most sensitive and personal info, and it is being used to advance society. However, it is also identifiable, immutable and weaponizable. For these and other reasons, our genetic data deserves the highest security. But how secure is its point of origin? This talk will cover the current genetic threat landscape and the potential risks from the misuse of genetic data. A focus will be applied to DNA sequencers and their operational environments, where both digital genetic data and insecurity are introduced into the system.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Sunday - 09:00-09:30 PDT

Title: The State of AI Ethics
When: Sunday, Aug 8, 09:00 - 09:30 PDT
Where: AI Village (Virtual)

SpeakerBio: Abishek Gupta
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

Title: The threat hiding in daylight: Police Monitoring legislation and individual privacy in chat
When: Saturday, Aug 7, 16:30 - 17:30 PDT
Where: Crypto & Privacy Village (Virtual)
Speakers: Vic Huang,Joy Ho

SpeakerBio: Vic Huang , Member, UCCU Hacker
Vic Huang is member of UCCU Hacker, a hacker community in Taiwan. He is interested in Web/Mobile/Blockchain Security and penetration testing. He has been focusing on Blockchain for over 4 years. Vic shared his research on CYBERSEC 2021, CODE BLUE 2020, HITB+cyberweek 2019, HITCON Pacific 2018, AIS3, ISIP (Information Security Incubation Program), and so on.

SpeakerBio: Joy Ho , Ph. D. Candidate, Soochow University
Joy Ho is a privacy counsel now working in a technical company in handling personal data infringement events and in legal compliance of Personal Information Protection Act. Joy is certified Internal Management Specialist, Internal Auditor & Certified Verification Professional – Lead Auditor of Taiwan Personal Information Protection & Administration System (TPIPAS), also Lead Auditor of ISO 27001.

Description:

Since all the messenger services emphasize the trust relationship between the service provider and users, technology companies have been actively strengthening user data protection and providing better encryption measures in recent years. However, focusing on criminal investigation, national security and Anti-terrorism, law enforcement agencies in many countries have begun to formulate rules requiring technology companies to cooperate with the government to provide user data decryption to protect national security. This presentation try to introduce relevant issues about the police monitoring legislation and individual privacy in chat from technical and legal perspectives and the special case study from Taiwan.

First , we would share some police investigation in TW. The methods and targets have been changed due to the evolution of times. Then we would dive into a new critical target - messengers apps. Discuss about the technical part of messengers apps and Police Monitoring possibility. There are some messengers which is popular in different regions. In these apps, not only personal information are stored in the data collector side - service provider, but also our private chat messages with our family and friends. The messenger app companies say they use point-to-point encryption (end-to-end encryption, E2EE) to technically protect user privacy, but actually each what is E2EE? What is the difference between messenger apps E2EE? And how’s it possible that there are some monitor(spying) apps clarify that they could reach to the data under E2EE scope? It makes the Police monitoring possible because many spying apps are existed. In this part we will also discuss about the technical part of privacy protection and spying. The discussion would then point out “what and how the police could really get in real world” from the technical perspective.

Secondly, we would start from Technology Investigation Act draft in Taiwan. On September 8, 2020, the Taiwan Ministry of Justice announced the draft Technology Investigation Act, which introduced different high-tech investigation approaches, including the “source telecommunications surveillance.” We will introduce the draft Technology Investigation Act and the source telecommunications surveillance ruled. The issues related to the access of individual communication content would be raised: (1) If public interest is the reason to get individual communication, what is the line between privacy protection and public interest?What is the legal basis to get individual communication? (2) Could Government request or compel technology companies to provide my communication content? (3) How about the encrypted one? Through the discussion of 3 questions above, this presentation would provide an example to see the accessible information of messengers by criminal investigation, hoping to find the balance between privacy protection and police investigation. The last but not the least, we would share a case study about the police in Taiwan use the personal information collected for COVID-19 measurements to investigate the case.

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: The Unbelievable Insecurity of the Big Data Stack: An Offensive Approach to Analyzing Huge and Complex Big Data Infrastructures
When: Friday, Aug 6, 16:00 - 16:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Sheila A. Berta
Sheila A. Berta is an offensive security specialist who started at 12 years-old by learning on her own. At the age of 15, she wrote her first book about Web Hacking, published in several countries. Over the years, Sheila has discovered vulnerabilities in popular web applications and software, as well as given courses at universities and private institutes in Argentina. She specializes in offensive techniques, reverse engineering, and exploit writing and is also a developer in ASM (MCU and MPU x86/x64), C/C++, Python and Go. The last years she focused on Cloud Native and Big Data security. As an international speaker, she has spoken at important security conferences such as Black Hat Briefings, DEF CON, HITB, Ekoparty, IEEE ArgenCon and others. Sheila currently works as Head of Research at Dreamlab Technologies.
Twitter: @UnaPibaGeek

Description:

Honoring the term, the variety of technologies in the Big Data stack is hugely BIG. Many complex components in charge of transport, storing, and processing millions of records make up Big Data infrastructures. The speed at which data needs to be processed and how quickly the implemented technologies need to communicate with each other make security lag behind. Once again, complexity is the worst enemy of security.

Today, when conducting a security assessment on Big Data infrastructures, there is currently no methodology for it and there are hardly any technical resources to analyze the attack vectors. On top of that, many things that are considered vulnerabilities in conventional infrastructures, or even in the Cloud, are not vulnerabilities in this stack. What is a security problem and what is not a security problem in Big Data infrastructures? That is one of the many questions that this research answers. Security professionals need to count on a methodology and acquire the necessary skills to competently analyze the security of such infrastructures.

This talk presents a methodology, and new and impactful attack vectors in the four layers of the Big Data stack: Data Ingestion, Data Storage, Data Processing and Data Access. Some of the techniques that will be exposed are the remote attack of the centralized cluster configuration managed by ZooKeeper; packet crafting for remote communication with the Hadoop RPC/IPC to compromise the HDFS; development of a malicious YARN application to achieve RCE; interfering data ingestion channels as well as abusing the drivers of HDFS-based storage technologies like Hive/HBase, and platforms to query multiple data lakes as Presto. In addition, security recommendations will be provided to prevent the attacks explained.

REFERENCES

> I plan to release a white paper at the conference, in the white paper there will be all the references. Anyway, as the attacks are novel, the references are related to infrastructure stuff mostly, not so much about security.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=vl9hk4fQdos

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20S

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Friday - 09:00-09:59 PDT

Title: The War for Control of DNS Encryption
When: Friday, Aug 6, 09:00 - 09:59 PDT
Where: Packet Hacking Village - Talks (Virtual)

SpeakerBio: Paul Vixie , CHAIRMAN AND CEO AND COFOUNDER OF FARSIGHT SECURITY, INC
Dr. Paul Vixie (Twitter: @PaulVixie) is an Internet pioneer. Currently, he is the Chairman, Chief Executive Officer and Cofounder of Farsight Security, Inc. He was inducted into the Internet Hall of Fame in 2014 for work related to DNS and DNSSEC. Dr. Vixie is a prolific author of open-source Internet software including BIND, and of many Internet standards documents concerning DNS and DNSSEC. In addition, he founded the first anti-spam company (MAPS, 1996), the first non-profit Internet infrastructure software company (ISC, 1994), and the first neutral and commercial Internet exchange (PAIX, 1991). He earned his Ph.D. from Keio University.
Twitter: @PaulVixie

Description:

Pervasive monitoring of the Internet by both government, corporate, and criminal actors has triggered an encryption wavefront as wide as the Internet itself. DNS, as the map of the Internet's territory, is seen as especially sensitive and there are now several competing encryption standards waiting to be deployed. In this short talk, Dr. Vixie will explain the original problem, describe the protocol-level solutions, and then show how vendors like Google, Mozilla Corporation, Microsoft, and Apple are deploying these technologies across their product lines. Opinions may also be offered.

All Packet Hacking Village talks will stream on YouTube, Twitch, Facebook, and Periscope.

YouTube: https://youtube.com/wallofsheep

Twitch: https://twitch.tv/wallofsheep

Facebook: https://www.facebook.com/wallofsheep/

Periscope: https://www.periscope.tv/wallofsheep

Return to Index - Add to Google Calendar - ics Calendar file

AVV - Saturday - 10:00-10:59 PDT

Title: The Way of The Adversary
When: Saturday, Aug 7, 10:00 - 10:59 PDT
Where: Adversary Village (Virtual)

SpeakerBio: Phillip Wylie , Offensive Cybersecurity Practitioner & Educator, The PWN School Project
Phillip has over two decades of information technology and cybersecurity experience. His specialties include penetration testing, red teaming, and application security. When Phillip is not hacking, he is educating others. Phillip is the founder of The Pwn School Project, an education-focused cybersecurity organization. He co-authored the book, “The Pentester Blueprint: Starting a Career as an Ethical Hacker” based on his popular talk presented at numerous conferences. He is an Innocent Lives Foundation Ambassador and a ‘Hacking is NOT a Crime’ Advocate.
Twitter: @PhillipWylie
https://www.linkedin.com/in/phillipwylie

Description:
The adversary philosophy and mindset are important when trying to emulate a threat actor during a red team operation or offensive cybersecurity assessment or trying to understand them as a defender. In this talk we will take a look at the philosophy and mindset of an adversary as well as what motivates them.

Adversary Village talks and workshops will be streamed on YouTube and Twitch.

Q&A sessions will happen in DEF CON Official Discord server after each talk.

YouTube: https://www.youtube.com/channel/UCOhn9WALnpb5YAbW18R1Hzg

Twitch: https://twitch.tv/adversaryvillage

Discord: https://discord.gg/defcon

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Saturday - 16:00-16:30 PDT

Title: The Wild West of DeFi Exploits
When: Saturday, Aug 7, 16:00 - 16:30 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Anna Szeto , Intern Blockchain Security Coinbase
Anna Szeto is a Software Engineering Intern on the Blockchain Security team at Coinbase. She is a rising third-year student at Columbia University, with a major in computer science and interests in blockchain, decentralized finance, and artificial intelligence.

Description:

Decentralized finance (DeFi) has become increasingly popular, and DeFi-related hacks and scams have become more frequent as the market expands. This talk reviews how and why these hacks and scams occur, both from a technical, code-oriented perspective and a psychological perspective. Recent examples of DeFi scams, as well as tips for avoiding them, are also covered. DeFi can seem like a lawless land, but investors can navigate safely if they know what to look out for.

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Friday - 12:00-12:30 PDT

Title: This is what we thought would happen in 2021
When: Friday, Aug 6, 12:00 - 12:30 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Gert-Jan Bruggink
Gert-Jan (GJ) Bruggink is a cyber threat intelligence leader, specialized in understanding adversary tradecraft and thereby helping leaders make more informed decisions. GJ has extensive experience at the crossing of offense, defence & strategic risk management and spend the last 10+ years specializing on providing leaders actionable threat intelligence products and building secure organizations. GJ previously co-founded and delivered defensive services at FalconForce, led the Dutch cyber threat intelligence team at a Big Four accounting firm and delived security services at a security integrator.
Twitter: @gertjanbruggink

Description:

At the beginning of each year, companies share lessons learned and forecasts on what (cyber) threats are expected in the next 12 months. The reality is that a lot of teams and companies publish about this and you probably did not read all these articles or reports.

This talk explores the results of a meta-analysis on threat forecasting, based on open-source reports and articles. As a defender you constantly balance between pushing Jira tickets and looking ahead. By giving you a TLDR, defenders have context into what needs to be prioritised next to the daily operations.

This talk explores the concept of forecasting to help your cyber security program. Following concepts introduced in the book ‘Superforecasting: the art and science of prediction’ (Tetlock, Gardner), the average of multiple forecasts is usually the most accurate.

In preparation to this talk, all publicly available research released in Jan-April 2021 from companies on their expectations for 2021’ threat landscape has been analysed. This exercise resulted into a prioritised list of topics expected for 2021. This list is also actively tracked, to monitor if events already occurred and topics are more/less relevant. By giving you the TLDR, defenders have more context into what needs to be prioritised - next to the daily operations.

As a defender, there is always the constant balance where to focus your precious time. There is great value in looking ahead, yet this is hard when constantly pivoting between Jira tickets. Forecasting is just one way to look ahead and prepare yourself and your teams.

The objective of this talk is to provide defenders access to a larger narrative around cyber threats to support both business and senior stakeholder’s decision making. Providing more situational awareness. As a defender you constantly balance between pushing Jira tickets and looking ahead. This session supports keeping that balance.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

CAHV - Friday - 15:00-15:59 PDT

Title: This Job Ad Sucks
When: Friday, Aug 6, 15:00 - 15:59 PDT
Where: Career Hacking Village (Talk)

SpeakerBio: Kirsten Renner
No BIO available

Description:

I'm mostly kidding, but not really. I have taught managers for years how to write better descriptions and candidates how to write better resumes, and I will continue to do that. I even spoke at multiple conferences over the last few years for that purpose. But the key is to have a way of getting around and through bad descriptions (and other road blocks), because I don't think we can ever really fix that problem completely. In other words, even though those obstacles exist and likely always will, there are ways to get through it, and that is what I will be presenting. In the same way that a poorly written resume is not a fair depiction of the potential a candidate has to offer, it just take a bit of coaching and, well, hacking, to get around road blocks in the system to make good matches between the opportunities and talent. This presentation isn’t going to offer a solution to making employers do a better job advertising for and determining the best fits for their openings - there's plenty of content out there for them to do that. It will however tell [the candidates] how to make it through bad descriptions, as well as less than effective interviewers and maybe it will even help them see the light! Looking for a job is an engineering problem. Gather the requirements, do some QA, launch (get out there) and keep updating!

This talk will be available on YouTube: https://www.youtube.com/watch?v=6GvuhfzvQGE

Career Hacking Village content will be available on YouTube.

YouTube: https://youtube.com/careerhackingvillage

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 12:00-12:25 PDT

Title: Threat Modeling for Space Hitchhikers
When: Friday, Aug 6, 12:00 - 12:25 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: James Pavur
James Pavur is a Rhodes Scholar and DPhil Student at Oxford University where he researches satellite cyber-security in the Department of Computer Science’s System Security Lab.

Description:

When you strap someone else’s satellite to your rocket, how much should you trust them? In this talk, we’ll explore threats relating to launch integration and the role of secondary payloads, such as CubeSats, in modern missions. The briefing combines strategic and policy perspectives with dynamic simulations exploring space-to-space radio attacks from compromise or malicious payloads. While it includes technical components, it assumes no prior experience with radio communications or aerospace.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=W91uGzCWHXI

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 12:00-12:20 PDT

Title: Time Turner - Hacking RF Attendance Systems (To Be in Two Places at Once)
When: Saturday, Aug 7, 12:00 - 12:20 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Vivek Nair
Vivek Nair is a Ph.D. student studying applied cryptography in the EECS department at UC Berkeley. He was the youngest-ever recipient of Bachelor's and Master's degrees in Computer Science at the University of Illinois at the ages of 18 and 19 respectively. He is also a National Science Foundation CyberCorps Scholar and a National Physical Science Consortium Fellow.
https://github.com/VCNinc/Time-Turner

Description:

It's a tale as old as time: a graduating senior needs two more courses to graduate, but the lectures happen to be scheduled at the same time and the school's new high-tech wireless attendance tracking system makes it impossible to attend both courses... in theory. By reverse-engineering the attendance devices and emulating them using a hidden Arduino, the system can be tricked into giving attendance credit for both courses without being physically present. It's a real-life "time turner," allowing him to be in two places at once.

REFERENCES
https://github.com/wizard97/iSkipper/releases/download/v1.0.0/iskipper.pdf
https://courses.ece.ubc.ca/cpen442/termproject/reports/2010/iclicker.pdf
https://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/f2015/cs886_kdv8/cs886_kdv8/cs886_kdv8/index.html
https://github.com/wizard97/iSkipper https://github.com/charlescao460/iSkipper-Software

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=wEslemikn48

Media Server (Main Talk):
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20V

Media Server (Demo 1):
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20V

Media Server (Demo 2):
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20V

Media Server (Demo 3):
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20V

Media Server (Demo 4):
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20V

Media Server (Demo 5):
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20V

Media Server (Demo 6):
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20V

Media Server (Demo 7):
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20V

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 13:00-13:59 PDT

Title: Timeless Timing Attacks
When: Sunday, Aug 8, 13:00 - 13:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Mathy Vanhoef,Tom Van Goethem

SpeakerBio: Mathy Vanhoef
Mathy Vanhoef is a postdoctoral researcher at New York University Abu Dhabi. His research interest lies in computer security with a focus on network and wireless security (e.g. Wi-Fi), software security, and applied cryptography. In these areas Mathy tries to bridge the gap between real-world code and (protocol) standards. He previously discovered the KRACK attack against WPA2, the RC4 NOMORE attack against RC4, and the Dragonblood attack against WPA3.
Twitter: @vanhoefm

SpeakerBio: Tom Van Goethem
Tom Van Goethem is a researcher with the DistriNet group at KU Leuven in Belgium, mainly focusing on practical side-channel attacks against web applications and browsers. By exposing flaws that result from the unintended interplay of different components or network layers, Tom aims to bring us closer to a more secure web that we all deserve. He has spoken at various venues such as Black Hat USA and Asia, OWASP Global, and USENIX Security. In his spare time, Tom provides animal sculptures with pink tutus.
Twitter: @tomvangoethem

Description:
25 years ago, the first timing attacks against well-known cryptosystems such as RSA and Diffie-Hellman were introduced. By carefully measuring the execution time of crypto operations, an attacker could infer the bits of the secret. Ever since, timing attacks have frequently resurfaced, leading to many vulnerabilities in various applications and cryptosystems that do not have constant-time execution. As networks became more stable and low-latency, it soon became possible to perform these timing attacks over an Internet connection, potentially putting millions of devices at risk. However, attackers still face the challenge of overcoming the jitter that is incurred on the network path, as it obfuscates the real timing values. Up until now, an adversary would have to collect thousands or millions of measurements to infer a single bit of information.

In this presentation, we introduce a conceptually novel way of performing timing attacks that is completely resilient to network jitter. This means that remote timing attacks can now be executed with a performance and accuracy that is similar as if the attack was performed on the local system. With this technique, which leverages coalescing of network packets and request multiplexing, it is possible to detect timing differences as small as 100ns over any Internet connection. We will elaborate on how this technique can be launched against HTTP/2 webservers, Tor onion services, and EAP-pwd, a popular Wi-Fi authentication method.

REFERENCES
See page 15 to 17 in our paper for a list of references: https://www.usenix.org/system/files/sec20-van_goethem.pdf

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=s5w4RG7-Y6g

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20T

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

CON - Thursday - 10:00-16:59 PDT

Title: Tin Foil Hat Contest
When: Thursday, Aug 5, 10:00 - 16:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/236423

Return to Index - Add to Google Calendar - ics Calendar file

RGV - Friday - 10:00-10:59 PDT

Title: Top 10 BOGUS Biometrics!
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: Rogues Village (Virtual)

SpeakerBio: Vic Harkness
Vic is a Security Consultant at F-Secure Consulting who can commonly be found talking about something weird. She has previously spoken at conferences about defeating facial recognition systems, ATM malware, and future attacks on connected/autonomous vehicles. She holds a Bachelor's degree in Robotics & Artificial Intelligence and a Master's degree in Cyber Security, which she believes qualifies her to talk about a range of completely unrelated topics.
Twitter: @VicHarkness
https://vicharkness.co.uk/

Description:

Every now and then, you come across an article. Top 10 WILDEST biometrics! Number 5 will SHOCK YOU. I’ve seen them too. But, these articles never go beyond the surface. They’ll tell you that buttholes are a viable biometric modality, but rarely provide a source to these claims. This talk describes the results of me delving into the dark hole of weird biometrics. Come learn about how legit clickbait modalities actually are, or where the disinformation may have come from. Or maybe you'll learn about the hot new biometrics that you'll be seeing in the future- You'll have to watch to find out!

This talk will go live on Twitch: https://www.twitch.tv/roguesvillage

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Sunday - 11:00-11:59 PDT

Title: Top 20 Secure PLC Coding Practices
When: Sunday, Aug 8, 11:00 - 11:59 PDT
Where: ICS Village (Virtual)
Speakers: Sarah Fluchs,Vivek Ponnada

SpeakerBio: Sarah Fluchs , CTO, admeritia
Sarah Fluchs is the CTO of admeritia, which specializes in security consulting for the process industry, manufacturing, and critical infrastructures. A process and automation engineer herself, Sarah is convinced that creating solid engineering methods that speak the language of automation engineers is key for OT Security. Her main research interests include security and systems engineering, security for safety, and security engineering information models. Sarah is an active contributor to ISA/IEC standards and a board member at the ISA Standards & Practices board and the German water industry organization KDW. She writes a monthly ""security briefing for hard hats"" (admeritia.de/hardhats) and a blog (fluchsfriction.medium.com). She's one of the founders and leaders of the Top 20 Secure PLC Coding Project (plc-security.com).
Twitter: @SarahFluchs

SpeakerBio: Vivek Ponnada , GE
Vivek Ponnada works for GE as a Service Manager and is responsible for GE's Gas Power transactional customers (Utilities and Co-generation) across Canada. Prior to this role, he was in Sales & Business development (Control system upgrades and Cybersecurity solutions), and started his career as a Field Engineer, commissioning turbine controls systems in Europe, Africa, Middle-East and South East Asia. Vivek is passionate about industrial controls cybersecurity and enjoys learning & contributing to the security community.
Twitter: @ControlsCyber

Description:

This presentation is the outcome of a community driven project called "Top 20 Secure PLC Coding Practices", with document version 1.0 to be released on plc-security.com on June 15th, 2021, for downloading free or charge, and will have no restrictions on distribution and use.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Saturday - 13:00-13:30 PDT

Title: Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure
When: Saturday, Aug 7, 13:00 - 13:30 PDT
Where: ICS Village (Virtual)

SpeakerBio: Lauren Zabierek , Harvard Kennedy School's Belfer Center for Science and International Affairs
Lauren Zabierek is the Executive Director of the Cyber Project at Harvard Kennedy School’s Belfer Center. She comes to this role as a 2019 graduate of the Kennedy School's mid-career MPA program.

Lauren served as an intelligence officer in the United States Air Force at the beginning of her career. Later, as a civilian intelligence analyst with the National Geospatial Intelligence Agency (NGA) assigned to the Office of Counterterrorism, she completed three war zone deployments. Throughout her six years at NGA, she became a subject matter expert on Activity Based Intelligence (ABI) and served as an adjunct professor in ABI at the NGA college.

After leaving NGA, she joined the cybersecurity threat intelligence startup Recorded Future, and was instrumental in building its Public Sector business practice. In her role as a Senior Intelligence Analyst, she fused intelligence methodologies with cybersecurity and machine learning technologies to help public and private sector customers improve their cyber posture. She also managed a team of analysts and worked alongside the Product Management and Training teams to improve her customers' experience with the software.

A Gold Star Sister, Lauren is committed to supporting families of the fallen and has volunteered several times as a mentor with the Tragedy Assistance Program for Survivors (TAPS). She also co-founded the Recorded Future Women's Mentorship Initiative, helped to start a women's initiative at NGA, is a member of the NatSecGirlSquad, and is the co-founder of the online social media movement called #ShareTheMicInCyber, which aims to dismantle racism and sexism in cybersecurity and privacy.

Twitter: @lzxdc

Description:

The recent ransomware and cyber espionage campaigns prove that a fundamental redesign of our domestic cyber defensive posture is both necessary and urgent to protect against future cyber threats. As such, we believe the time is now to develop an integrated, networked approach to collaborative defense and intelligence analysis and sharing between the federal government, state and local governments, and the private sector. My team of student researchers and I conducted several interviews with stakeholders in both the state and federal governments and the private sector and poured over existing literature. We've created a roadmap toward this vision, answering how a 21st century threat can be tackled by the tools available in its own time. We don't purport to have all the answers, but we would be interested in feedback from the community on the feasiblity and desirability of these ideas.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 21:00-20:59 PDT

Title: Towards Understanding the Unlimited Approval in Ethereum
When: Thursday, Aug 5, 21:00 - 20:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Dabao Wang , Research Assistant at Zhejiang University
DABAO WANG is currently a research assistant at Zhejiang University, Hangzhou, China. His current research interests include Blockchain and DeFi security. Wang received a bachelor degree with honours in computer science from Monash University. Contact him at dabao.wang@monash.edu

Description:

With the prosperous development of the DeFi ecosystem, trading tokens in decentralized applications (DApps) has become more and more frequent. ERC20 tokens, as one of the most popular token types, vastly circulate in the crypto market and obtain great value. Ideally, to trade ERC20 tokens in DApps, users first invoke the method approve() to permit DApps or other users to transfer the expected amount of tokens based on the ERC20 standard. In reality, many DApps request unlimited approvals from users to improve user experience. Unfortunately, this design caused a considerable loss on both users or even DApps themself. For example, the design flaw of smart contracts might cause the permission leak of approved tokens (Bancor). Moreover, some malicious platforms even trick users into approving tokens so that they can easily steal users' approved asserts (Unicat). In this paper, we carefully elaborate on the unlimited approval problem with five real-world incidents. We then conduct two types of measurements. As a result, 21 platforms require unlimited approval in their service. However, only 3 (out of 15) wallets and no (out of 27) platforms reveal sufficient information and provide the modification feature for users. Moreover, we discover that over half of the approval transactions belong to unlimited approval.

This talk is now available on YouTube: https://www.youtube.com/watch?v=ijgYfdOADVI

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Thursday - 16:00-21:59 PDT

Title: Toxic BBQ
When: Thursday, Aug 5, 16:00 - 21:59 PDT
Where: See Description

Description:
Off-site at Sunset Park, Pavilion F, (36.0636, -115.1178)

Communal Supply Run leaves at 1300 from Paris Info Booth near Reg

OR

Drop by the park and see how you can help. Here are things we always need:

1. More meat!
2. Ice
3. Chips and Sides
4. Drinks (soft and hard, no glass)
5. Grill volunteers
6. Clean-up volunteers

See #ToxicBBQ on Twitter

For more information, see https://forum.defcon.org/node/236426

Forums: https://forum.defcon.org/node/236426

History: https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20events/ToxicBBQ-History-Continuous.pdf

Return to Index - Add to Google Calendar - ics Calendar file

CON - Saturday - 17:00-17:59 PDT

Title: Trace Labs OSINT Search Party CTF - Award Ceremony
When: Saturday, Aug 7, 17:00 - 17:59 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/236424

Return to Index - Add to Google Calendar - ics Calendar file

Title: Trace Labs OSINT Search Party CTF - Briefing
When: Saturday, Aug 7, 09:00 - 09:59 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/236424

Return to Index - Add to Google Calendar - ics Calendar file

Title: Trace Labs OSINT Search Party CTF
When: Saturday, Aug 7, 10:00 - 15:59 PDT
Where: See Description

Description:
For more information, see https://forum.defcon.org/node/236424

Return to Index - Add to Google Calendar - ics Calendar file

Title: Tracee
When: Saturday, Aug 7, 12:00 - 13:50 PDT
Where: DemoLab Video Channel 1

SpeakerBio: Yaniv Agman
Yaniv Agman is a Security Researcher at Aqua Security. He specializes in low-level Linux instrumentation technologies to perform dynamic analysis on Linux containers and systems. He is currently completing his Master's thesis in cyber security at BGU on detecting Android malware with eBPF technology. While not in front of a computer screen, he likes watching Sci-Fi movies and playing with his kids.

Description:
Tool or Project Name: Tracee

Short Abstract:
Linux Runtime Security and Forensics using eBPF

Short Developer Bio:
Yaniv Agman is a Security Researcher at Aqua Security. He specializes in low-level Linux instrumentation technologies to perform dynamic analysis on Linux containers and systems. He is currently completing his Master's thesis in cyber security at BGU on detecting Android malware with eBPF technology. While not in front of a computer screen, he likes watching Sci-Fi movies and playing with his kids.

Roi is a Security Researcher at Aqua Security. His work focuses on researching threats in the cloud native world. When not at work, Roi is a B.A. student in Computer Science at the Open University. He also enjoys going out into nature and spending time with family and friends.

URL to any additional information:
https://aquasecurity.github.io/tracee/dev

Detailed Explanation of Tool:
Tracee is a Runtime Security and forensics tool for Linux. It is using Linux eBPF technology to trace your system and applications at runtime, analyze collected events to detect suspicious behavioral patterns, and capture forensics artifacts. It is delivered as a Docker image that monitors the OS and detects suspicious behavior based on a predefined set of behavioral patterns.

Here is a more detailed information about the tool: Tracee is a runtime security and forensics tool for Linux. It is composed of tracee-ebpf, which collects OS events based on some given filters, and tracee-rules, which is the runtime security detection engine.

Tracee-ebpf is capable of tracing all processes in the system or a group of processes according to some given filters (these are: newly created processes, processes in a container, uid, command name, pid, tid, mount namespace id, process namespace id, uts name).

The user can select the set of events to trace, and also filter by their arguments.

The events which can be traced include the following: System calls and their arguments
LSM hooks (e.g. security_file_open, security_bprm_check, cap_capable) Internal kernel functions: (e.g. vfs_write and commit_creds) Special events and alerts (magic_write and mem_prot_alert) Other than tracing, Tracee-ebpf is also capable of capturing files written to disk or memory (e.g. "fileless" malwares), and extracting binaries that are dynamically loaded to an application's memory (e.g. when a malware uses a packer). Using these capabilities, it is possible to automatically collect forensic artifacts for later investigation. For more detailed information about these capabilities, see:

https://blog.aquasec.com/ebpf-contai...ware-detection

Tracee-Rules, is a rule engine that helps you detect suspicious behavioral patterns in streams of events. It is primarily made to leverage events collected with Tracee-eBPF into a Runtime Security solution. Tracee supports authoring rules in Golang or in Rego.

Following are some of the currently available rules: Code injection - Possible code injection into another process Dynamic Code Loading - Writing to executable allocated memory region Fileless Execution - Executing a process from memory, without a file in the disk Supporting Files, Code, etc:
https://github.com/aquasecurity/tracee

Target Audience: Defense
We believe Tracee is a valuable tool for anyone who want to perform runtime protection on Linux systems. In the demo we will introduce the tool, and see how it helped us to find real threats and other possible uses.

This content will be presented on a Discord video channel.

#dl-video1-voice: https://discord.com/channels/708208267699945503/734027693250576505

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 13:30-14:30 PDT

Title: Trailblazing the AI for Cybersecurity Discipline: Overview of the Field and Promising Future Directions
When: Friday, Aug 6, 13:30 - 14:30 PDT
Where: AI Village (Virtual)

SpeakerBio: Sagar Samtani
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 11:00-12:30 PDT

Title: Tricks for the Triage of Adversarial Software
When: Saturday, Aug 7, 11:00 - 12:30 PDT
Where: Blue Team Village - Workshop Track 1 (Virtual)
Speakers: Dylan Barker,Quinten Bowen

SpeakerBio: Dylan Barker
Dylan Barker is a technology professional with 10 years' experience in the information security space, in industries ranging from K12 and telecom to financial services. He has held many distinct roles, from security infrastructure engineering to vulnerability management. In the past, he has spoken at BSides events and has written articles for CrowdStrike, where he is currently employed as a senior analyst.
Twitter: @HBRH_314

SpeakerBio: Quinten Bowen
Quinten Bowen is an Information Security Professional who works as a Senior Analyst at CrowdStrike. Additionally, Quinten has expertise in malware analysis, penetration testing, threat hunting, and incident response in enterprise environments, holding relevant certifications such as GREM, OSCP, eCPPT, and eCMAP. Quinten spends his off-time volunteering for the Collegiate Cyber Defense Competition (CCDC), mentoring, and can be found around a table playing D&D.

Description:
A malware analysis and triage workshop covering quick static and dynamic analysis techniques along with common adversarial obfuscation techniques. Followed by a short malware analysis tournament challenge with gift-card prizes.

The workshop will cover techniques outlined in Malware Analysis Techniques (Published by Packt), written and delivered by myself, Dylan Barker, and the Technical Reviewer Quinten Bowen.

We'll examine ways to de-obfuscate common malicious scripts and droppers utilized in real-world attacks by threat actors such as those responsible for DarkSide ransomware and Emotet Banking Trojan threats.

Also covered will be ascertaining the capabilities and instruction flow of malware within NSA's Ghidra framework, crafting IOCs based on PE characteristics, and advanced dynamic analysis techniques including utilizing tools such as Inetsim, ProcDot, and manually unpacking malicious samples using debuggers to closely examine them without obfuscation.

The second half of the workshop will revolve around utilizing these techniques to answer questions, which will be scored on time and accuracy utilizing a CTF framework.

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Saturday - 15:00-15:15 PDT

Title: Triptych
When: Saturday, Aug 7, 15:00 - 15:15 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Sarang Noether, Ph.D.
Sarang Noether is a researcher who focuses on privacy-preserving cryptographic constructions and protocols.

Description:

Triptych is a zero-knowledge proving system that can be used as part of a privacy-preserving transaction model. In this talk, we'll walk through the research and development process that led to an ongoing implementation of Triptych compatible with the Monero protocol, and provide insight into some of the tradeoffs and complexities that come with protocol updates. No particular background is required to understand this talk!

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

Title: True Story: Hackers in the Aerospace Sector

When: Saturday, Aug 7, 14:30 - 14:55 PDT

Where: Aerospace Village (Virtual Talk)

Speakers: Declyn S.,Ginny Spicer,Olivia Stella,Steve Luczynski,Thomas Bristow

SpeakerBio: Declyn S.

Declyn is a cybersecurity specialist for the Aviation ISAC. He taught himself basic security principles and after finding aviation related vulnerabilities and reported them to the A-ISAC. He now works in the intel team at the A-ISAC specialising in threat intelligence and vulnerability disclosure management.

SpeakerBio: Ginny Spicer

Ginny Spicer is a master's student studying information security at Royal Holloway University of London. She is a packet nerd and likes to focus on network analysis, Wireshark, new protocols, and interplanetary communications. Ginny is a member of the technical documentation working group in the Interplanetary Networking SIG and an advisor for the California Cyber Innovation Challenge. Her particular areas of interest are DTN and encrypted DNS. This is her second year helping out with the DEF CON Aerospace Village.

SpeakerBio: Olivia Stella

Olivia Stella is a cybersecurity engineer for Los Alamos National Laboratory. In her current role, she focuses on agile space cybersecurity. With over twelve years of experience, she's worked for multiple companies in the aerospace industry including an in-flight entertainment company, major US airline, and government contractors. Olivia has supported incident response, vulnerability management, pen testing, bug bounty & coordinated disclosure, risk & compliance activities. Her academic background includes degrees in computer science and software engineering, along with an alphabet soup of security certifications. When she's not wearing her security hat, she loves to curl and is an avid toastmaster. (That's right, ice curling.)

SpeakerBio: Steve Luczynski

No BIO available

SpeakerBio: Thomas Bristow

Thomas Bristow is a Cyber Security Certification Specialist for the UK Civil Aviation Authority where he works on a whole range of things, from cyber threat modeling to running the CyberFirst summer placement scheme. He's a recent graduate from Royal Holloway with a degree in computer science and two back to back wins of society of the year. While his role is in cyber security he always tries to help others: whether this is educating colleagues on the LGBTQIA+ flags (and their meanings), performing careers talks at schools or just helping to make their team wiki easy to use.

Description:

What's it like to be a hacker working in government, for an airline, or pursuing a degree? When you read that question did you think, ew, why would I ever do that?! Or did you think, wow, that sounds great tell me more!

This isn't your typical workforce talk!

Join a diverse panel of folks working in the aerospace sector who are just like you! Learn how they got into their roles, why they chose to work there, what motivates them, and how they gained their skills and experience.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=ngoYRudoJqA

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

BHV - Friday - 15:00-15:30 PDT

Title: Truth, Trust, and Biodefense
When: Friday, Aug 6, 15:00 - 15:30 PDT
Where: Biohacking Village (Talk - Virtual)

SpeakerBio: Eric Perakslis , Chief Science and Digital Officer, Duke Clinical Research Institute
Eric Perakslis, PhD is the Chief Science and Digital Officer at the Duke Clinical Research Institute. He leads the strategic vision of digital research initiatives and technology affairs of the DCRI, provides oversight for the DCRI's Technology and Data Solutions, and serves as faculty lead for the DCRI's Health Services Research group. Dr. Perakslis transitioned to the DCRI from his role as a Rubenstein Fellow at Duke University, where his work focused on collaborative efforts in data science that spanned medicine, policy, engineering, computer science, information technology, and security. Immediately prior to his arrival at Duke, Dr. Perakslis served as Chief Scientific Advisor at Datavant, Lecturer in the Department of Biomedical Informatics at Harvard Medical School, and Strategic Innovation Advisor to Médecins Sans Fronti©res. Previously, Dr. Perakslis had senior leadership roles, including Senior Vice President and Head of the Takeda R&D Data Science Institute, Chief Information Officer and Chief Scientist (Informatics) at the U.S. Food and Drug Administration, and Senior Vice President of Research & Development Information Technology at Johnson & Johnson Pharmaceuticals. Throughout these roles, Dr. Perakslis created and led major transformations, bringing data, science, and technology together to advance the strategies of each of these organizations.

Description:

We all hope for a truly "post-COVID" world sooner rather than later, but that can only happen if we learn from the past and apply those lessons to our future. Our institutions and our people were unprepared for the harsh realities of the medical, scientific, economic and social demands that an emergency such as the COVID pandemic entails. Our national biodefense program had been steadily diminished while at the same time its focus was increasingly dedicated to human/terrorist threats over two decades. Our decentralized "public health" infrastructure was quickly shown to be simultaneously redundant and ineffective, and our national response was critically hampered by political agendas and rampant propaganda at the greatest scale ever witnessed in US history. Despite the tragic loss of more than 600,000 lives in the United States and millions worldwide, infectious disease experts know that it could have been much worse—and would have been, if the pathogen had been even slightly more deadly than the SARS-CoV-2 virus proved to be. Can we imagine the outcome if the COVID mortality rate was far greater than the 1.8% seen in the United States? What if coronavirus infections carried the same mortality rate as infectious encephalitis (100%), Ebola Zaire (25%-90%), or even smallpox in unvaccinated populations (>65%)? In this talk, we will discuss the history and future of biodefense with a specific focus on data, technology, communications, and the rapidly deteriorating concept of "truth." Radicalization, misinformation, technology, the surveillance economy, information security, and personal privacy will all be discussed with an eye toward building back better, smarter, and more engaged institutions that are driven by better-prepared humans.

All Biohacking Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/channel/UCm1Kas76P64rs2s1LUA6s2Q

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Saturday - 11:30-11:59 PDT

Title: Tryptich Talk
When: Saturday, Aug 7, 11:30 - 11:59 PDT
Where: Blockchain Village / Paris Vendome B

SpeakerBio: Sarang Noether, Ph.D.
Sarang Noether is a researcher who focuses on privacy-preserving cryptographic constructions and protocols.

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Sunday - 12:00-12:59 PDT

Title: Twitter Ethics Bug Bounty: Winners and Wrap-up
When: Sunday, Aug 8, 12:00 - 12:59 PDT
Where: AI Village (Virtual)

SpeakerBio: Rumman Chowdhury
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

RGV - Saturday - 12:00-12:59 PDT

Title: Twitter Q&A regarding Top 10 BOGUS Biometrics!
When: Saturday, Aug 7, 12:00 - 12:59 PDT
Where: Rogues Village (Virtual)

SpeakerBio: Vic Harkness
Vic is a Security Consultant at F-Secure Consulting who can commonly be found talking about something weird. She has previously spoken at conferences about defeating facial recognition systems, ATM malware, and future attacks on connected/autonomous vehicles. She holds a Bachelor's degree in Robotics & Artificial Intelligence and a Master's degree in Cyber Security, which she believes qualifies her to talk about a range of completely unrelated topics.
Twitter: @VicHarkness
https://vicharkness.co.uk/

Description:

The talk can be found on our our Twitch channel (https://www.twitch.tv/roguesvillage) after 10am, Friday August 6. Post questions you have for her about her talk on Twitter with the hashtag #BogusBio and tag her (@VicHarkness) or us (@RoguesVillage). Starting at 12pm PDT she will post replies and answers to your questions, as well as additional fun facts and details that didn’t make it into the talk.

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 10:00-18:30 PDT

Title: UART to UBOOT to ROOT
When: Friday, Aug 6, 10:00 - 18:30 PDT
Where: IoT Village (Onsite)

Description:
For more information, see https://www.iotvillage.org/defcon.html

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 10:00-18:30 PDT

Title: UART to UBOOT to ROOT
When: Saturday, Aug 7, 10:00 - 18:30 PDT
Where: IoT Village (Onsite)

Description:
For more information, see https://www.iotvillage.org/defcon.html

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 15:00-15:59 PDT

Title: UFOs: Misinformation, Disinformation, and the Basic Truth
When: Friday, Aug 6, 15:00 - 15:59 PDT
Where: Track 1 CLOSED; DCTV/Twitch #1 Pre-Recorded

SpeakerBio: Richard Thieme AKA neuralcowboy
Richard Thieme, https://thiemeworks.com has addressed security and intelligence issues for 28 years. He has keynoted security conferences in 15 countries and given presentations for the NSA, FBI, Secret Service, Pentagon Security Forum, U.S. Department of the Treasury, and Los Alamos National Laboratory. He has been speaking at Def Con since Def Con 4. His sixth book, a novel, Mobius: A Memoir, about an intelligence professional looking back on his career and how it led down unexpected paths, is receiving rave reviews. He has explored UFO phenomena seriously for 43 years.
Twitter: @neuralcowboy

Description:

The talk, "UFOs and Government: A Historical Inquiry" given at Def Con 21 has been viewed thousands of times. It was a serious well-documented exploration of the UFO subject based on Thieme's participation in research into the subject with colleagues. The book of that name is the gold standard for historical research into the subject and is in 100+ university libraries.

This update was necessitated by recent UFO incidents and the diverse conversations triggered by them. Contextual understanding is needed to evaluate current reports from pilots and naval personnel, statements from senators and Pentagon personnel, and indeed, all the input from journalists who are often unfamiliar with the field and the real history of documented UFOs over the past 70 years.

Thieme was privileged to participate with scholars and lifelong researchers into the massive trove of reports. We estimate that 95% can be explained by mundane phenomena but the remainder suggest prolonged interaction with our planetary society over a long period. Thieme also knows that when you know you don't know something, don't suggest that you do. Stay with the facts, stay with the data. Sensible conclusions, when we do that, are astonishing enough.

Reality, as Philip K. Dick said, will not go away just because we refuse to believe in it.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=mExktWB0qz4

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20R

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will only be broadcast to DCTV1, in local hotels and on Twitch. This talk is not being presented in Track 1.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 13:00-13:50 PDT

Title: Unboxing the Spacecraft Software BlackBox – Hunting for Vulnerabilities

When: Friday, Aug 6, 13:00 - 13:50 PDT

Where: Aerospace Village (Virtual Talk)

SpeakerBio: Brandon Bailey

Brandon Bailey has more than 15 years of experience supporting intelligence and civil space customers. Brandon’s specialties include vulnerability assessments and penetration testing for space systems. Brandon was awarded NASA’s Exceptional Service Medal for his landmark cybersecurity work in 2019.

Description:

As the commercialization of space increases or access to source code is not feasible, it is getting more common that spacecraft/embedded binaries are a black box. There needs to be a way automate code inspection in a cost effective, fast, repeatable manner which can be constantly enhanced to have the latest capability to build secure spacecraft SW. Synthetic vulnerabilities were created and analyzed with varying results.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=WvKtdXSRvhM

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 15:45-16:45 PDT

Title: Uncomfortable Networking
When: Saturday, Aug 7, 15:45 - 16:45 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Charles Rumford
Charles is currently a network engineer with Deft. He has a background in network engineering, programming, information security, usability, and linux systems administration. He likes to ensure things are secure, usable, and users are informed.
Twitter: @TallWireless

Description:
There is so much networking architecture we do in the name of security which ultimately just gets in the way of so many thing. Learn about things to simplify your network design and reduce your management overhead while maintaining or increasing your security posture.

When it comes to security, networking can be your first line of defense, but it shouldn't be your only, and it shouldn't add complexity and management overhead to your system. There are ways to keep the network design simple while also keeping resources secure.

Come and hear from a security and usability focused network engineer about the things we do to our network architectures and design in the name of security but ultimately create large amounts of complexity, management overhead, and the need to redesign constantly.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Uncovering covert network behaviors within critical infrastructure environments
When: Friday, Aug 6, 15:30 - 16:30 PDT
Where: Blue Team Village - Main Track (Virtual)
Speakers: Michael Raggo,Chester Hosmer

SpeakerBio: Michael Raggo
Michael Raggo has over 20 years of security research experience. His current research focuses on Cloud security. His research has been highlighted on television's CNN Tech, and numerous media publications including TIME, Forbes, Bloomberg, Dark Reading, TechCrunch, TechTarget, The Register, and countless others. Michael is the author of "Mobile Data Loss: Threats & Countermeasures" and "Data Hiding" for Syngress Books, and is a contributing author for "Information Security the Complete Reference 2nd Edition". His Data Hiding book is also included at the NSA's National Cryptologic Museum at Ft. Meade. A former security trainer, Michael has briefed international defense agencies including the FBI and Pentagon; and is a former participating member of the PCI Council. He is also a frequent presenter at security conferences, including Black Hat, DEF CON, RSA, OWASP, HackCon, and SANS. He was also awarded the Pentagon's Certificate of Appreciation.
Twitter: @datahiding

SpeakerBio: Chester Hosmer
No BIO available

Description:
We'll explore vulnerabilities we've discovered in our IoT, IIoT, and ICS research to reveal the systemic problems that exist as a result of the fragmented supply chain, inconsistent configurations, and overall poor security standards found across the critical networks and devices. We'll then show how we have applied discoveries of these aberrant behaviors to ML algorithms to uncover the risky and potentially very damaging covert channels communicating with the outside world and the types of data being harvested along with the new attack surfaces that they offer.

Through the evolution of IoT, IIoT, and ICS networks we've been uncovering new risks and vulnerabilities. Most of these risks and vulnerabilities are so unpredictable when considering the fragmented supply chain of hardware, operating systems, and software; making signature-based and operating system-centric security solutions inadequate.

Leveraging the Active Cyber Defense framework and combining that with our homegrown ML, we've created our own approach to detecting aberrant network behavior through passive network monitoring to discover covert communications, rogue devices, emerging threats, and more. The analysis of protocols, device behavior, and network activity within these environments is critical and can aid investigators when responding to incidents that have national impacts. (For example, the recent Colonial Pipeline Ransomware Attack, and the Oldsmar Florida water poisoning attempt).

We'll explore many vulnerabilities we've discovered in our IoT, IIoT, and ICS research to reveal the systemic problems that exist as a result of the fragmented supply chain, inconsistent configurations, and overall poor security standards found across the critical networks and devices. We will build upon our previous real-world examples and current threat research within this presentation and show how we have applied the discoveries of these aberrant behaviors to machine learning algorithms to uncover the risky and potentially very damaging covert channels communicating with the outside world and the types of data that is being harvested along with the new attack surfaces that they offer.

The combined lecture and demonstration will take a deep dive into the early identification of network activities that map to each stage of the cyber kill chain. We'll also demo our open source and free Modbus TCP pcap analysis tool to identify malicious behaviors within ICS environments.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Sunday - 11:15-11:59 PDT

Title: Understanding common Google Cloud misconfiguration using GCP Goat
When: Sunday, Aug 8, 11:15 - 11:59 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Joshua Jebaraj
Joshua Jebaraj is Security Researcher at we45. He is an active member of many open-source communities like Null, Ansible and Hashicorp. He frequently speaks at null Chennai chapter and OWASP Vit Chennai. He has previously spoken at conferences like Owasp-Seasides,Bsides-Delhi and Open-Security-Summit.
Twitter: @joshva_jebaraj

Description:
As organisations workflows move into the cloud we see a wider adoption of cloud based platforms like Google Cloud (GCP). While cloud based platforms offer a higher level of scalability critical aspects into security can fall to the sidelines. With cybersecurity attacks on the rise in the cloud space (Gitlab-blog, Rhino-security-blog) we have to make sure all our applications hosted on cloud infrastructure like GCP are kept safe. The talk starts with the common service misconfiguration like open buckets and moves to advanced and GCP specific services like, gcloud container registry. This talk not only covers the offensive side but also covers the defensive side where the audience will see demonstration of how those vulnerabilities can be mitigated. GCP Goat is an intentionally vulnerable project which consists of common misconfiguration in the Google Cloud that is open source for the audience to test their newly learned information after the talk. By the end of the talk the audience will have a better understanding of the common threat surface on GCP and How they can mitigate it. The talk starts with Introduction about the GCP goat and how we can deploy it(5 mins) -

- Attacking Compute Engine (5 mins)
- Attacking the App engine (5 mins)
- Attacking SQL Instance (5 mins)
- Attacking GCP buckets (5 mins)
- Attacking GCP GKE clusters (5 mins)
- Privilege Escalation (5 mins)
- Conclusion and QA (5 mins)

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Friday - 13:00-15:59 PDT

Title: Understanding Space in the Cyber Domain
When: Friday, Aug 6, 13:00 - 15:59 PDT
Where: Aerospace Village (Virtual Workshop)

Description:

This half-day course examines the practical issues of developing and sustaining a secure cyber environment through all phases of the space mission lifecycle. The course is organized around the SPAce Domain Cybersecurity (SpaDoCs) Framework. The SpaDoCs Framework provides a comprehensive and systematic model for understanding and tackling all critical issues of cybersecurity in the space domain. An examination of the Key objectives— confidentiality, integrity, availability—provides the foundation for the course. From there, the space domain is examined layer by layer starting from the enterprise layer, then drilling down through mission, system and DevSecOps layers. Threats and vulnerabilities at each layer are highlighted. Finally, first principles of cybersecurity are discussed (domain separation, process isolation, etc.) as well as key enablers (vision, strategy, etc.) to help frame plans for action to address the cybersecurity issues exposed by this course. Course exercises center around practical application of the material to real-world space mission scenarios.

Return to Index - Add to Google Calendar - ics Calendar file

ASV - Saturday - 10:00-12:59 PDT

Title: Understanding Space in the Cyber Domain
When: Saturday, Aug 7, 10:00 - 12:59 PDT
Where: Aerospace Village (Virtual Workshop)

Description:

This half-day course examines the practical issues of developing and sustaining a secure cyber environment through all phases of the space mission lifecycle. The course is organized around the SPAce Domain Cybersecurity (SpaDoCs) Framework. The SpaDoCs Framework provides a comprehensive and systematic model for understanding and tackling all critical issues of cybersecurity in the space domain. An examination of the Key objectives— confidentiality, integrity, availability—provides the foundation for the course. From there, the space domain is examined layer by layer starting from the enterprise layer, then drilling down through mission, system and DevSecOps layers. Threats and vulnerabilities at each layer are highlighted. Finally, first principles of cybersecurity are discussed (domain separation, process isolation, etc.) as well as key enablers (vision, strategy, etc.) to help frame plans for action to address the cybersecurity issues exposed by this course. Course exercises center around practical application of the material to real-world space mission scenarios.

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 11:00-11:45 PDT

Title: UPnProxyPot: fake the funk, become a blackhat proxy, MITM their TLS, and scrape the wire
When: Saturday, Aug 7, 11:00 - 11:45 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Chad Seaman
Chad is the SIRT team lead @ Akamai Technologies. He spends his time being an internet dumpster diver and emerging threats researcher focusing on DDoS, malware, botnets, and digital hooliganism in general.
https://www.linkedin.com/in/that-chad-seaman/

Description:

UPnP sucks, everybody knows it, especially blackhat proxy operators. UPnProxyPot was developed to MITM these operators to see what they're doing with their IoT proxy networks and campaigns. We'll cover SSDP, UPnP, UPnProxy research/campaigns as well as cover a new Golang based honeypot, so we can all snoop on them together!

REFERENCES

> http://www.upnp-hacks.org (OG disclosure) https://www.youtube.com/watch?v=FU6qX0-GHRU (DEF CON 19 talk I attended) https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-pa (my initial UPnProxy research) https://blogs.akamai.com/sitr/2018/11/upnproxy-eternalsilence.html (additional UPnProxy campaign researcher, also mine)

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=mHCGNUsrTf0

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20C

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

HTSV - Saturday - 15:00-15:55 PDT

Title: US Coast Guard 2021 Cyber Strategic Outlook
When: Saturday, Aug 7, 15:00 - 15:55 PDT
Where: Hack the Sea (Virtual)

SpeakerBio: Michael Chien , CDR, USCG Cyber
No BIO available

Description: No Description available

Hack the Sea Village will stream their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/h4ckthesea

YouTube: https://www.youtube.com/channel/UC5htD_rPiP8N7v8VQKyJkOQ

Return to Index - Add to Google Calendar - ics Calendar file

Title: USBSamurai
When: Saturday, Aug 7, 12:00 - 13:50 PDT
Where: DemoLab Video Channel 2

SpeakerBio: Luca Bongiorni
Luca Bongiorni is working as Head of Offensive Security. He is also actively involved in InfoSec where his main fields of research are: Radio Networks, Reverse Engineering, Hardware Hacking, Internet of Things, and Physical Security. He also loves to share his knowledge and present some cool projects at security conferences around the globe.

Description:
Tool or Project Name: USBsamurai

Short Abstract:
During this talk, after a bit of history of hardware implants, will be presented a new hacking device: USBsamurai. A remotely-controlled USB HID injecting cable that costs less than 10 EUR to produce from off-the-shelf components (a cable and a USB radio transceiver) that can be used to compromise targets remotely (i.e. over a 2.4GHz undetectable protocol) in the stealthiest way ever seen & also bypass Air-Gapped Environments like a boss!

Extended Version:
During the last years, hardware implants have become a popular attack vector in air-gapped environments such as industrial networks: Stuxnet (2010), Operation Copperfield (2017), and the recent ransomware attack that has led to a shutdown in a US natural gas facility are only some notable cases. In parallel, in an effort to raise the bar of red-teaming operations, security researchers have been designing and releasing powerful open-source devices with the intent to make Red-Teaming operations even more interesting and disruptive. Smoothing the path to new TTPs and improving old ones. As a result, hardware implants should always be included in the threat modeling of an industrial facility. During this talk, after a bit of history of hardware implants, will be presented a new hacking device: USBsamurai. A remotely-controlled USB HID injecting cable that costs less than 10 EUR to produce from off-the-shelf components (a cable and a USB radio transceiver) that can be used to compromise targets remotely (i.e. over a 2.4GHz undetectable protocol) in the stealthiest way ever seen & also bypass Air-Gapped Environments like a boss!

This presentation will be quite technical, tailored for an ICS security audience. Come to this talk to start preparing for the next wave of attacks that can pass undetected by most of the existing security solutions available on the market.

Finally, I'll conclude the talk with practical, actionable countermeasures to prevent and detect HID attacks, and conclude by explaining how to approach a forensics analysis in presence of USB implants.

Short Developer Bio:
Luca Bongiorni is working as Head of Offensive Security. He is also actively involved in InfoSec where his main fields of research are: Radio Networks, Reverse Engineering, Hardware Hacking, Internet of Things, and Physical Security. He also loves to share his knowledge and present some cool projects at security conferences around the globe.

URL to any additional information:
https://medium.com/@LucaBongiorni/us...0-ebf4b81e1d0b

Detailed Explanation of Tool:
USBsamurai is a DIY hardware implant disguised as USB cable that allows to remotely inject over an undetectable RF channel an agent in memory that allows a remote threat actor to get a realtime shell over a target that can also be air-gapped. In practice a nightmare for any BlueTeam out there. Have you ever seen an USB cable that can bypass an air-gapped system and return a live remote-shell over an undetectable RF channel? https://www.youtube.com/watch?v=2BAzD27k_Gk (Please keep it confidential because the link is unlisted)

Supporting Files, Code, etc:
https://medium.com/@LucaBongiorni/us...s-4bd47abf8f87

Target Audience:
Offense, Hardware, ICS

Create awareness on Hardware Implants. The real ones. Not the grain of rice from Bloomberg's article. ;]

During the years I have tested multiple DLP solutions out there claiming to sanitize and protect assets from USB-related threats. Surprisingly, most of the time vendors kinda lie (or... saying in a more polite way... they forget about HID class of devices).

Security Officers MUST understand that hardware implants exist and they don't cost anymore like 10,000 $USD like NSA's TAO FIREWALK implant!

Finally, in pure DEF CON style, sharing how to create an offensive hardware implant out of a 10$ USB dongle from a commercial mouse, it is always a good way to spread knowledge among fellow hackers. :)

This content will be presented on a Discord video channel.

#dl-video2-voice: https://discord.com/channels/708208267699945503/734027778646867988

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 11:00-11:59 PDT

Title: Use a PortaProg to flash, dump, and test ISP and UPDI chips
When: Friday, Aug 6, 11:00 - 11:59 PDT
Where: Hardware Hacking Village (Virtual Talk)
Speakers: Bradán Lane,Sara Cladlow

SpeakerBio: Bradán Lane
Bradán Lane is a UX Design and User Researcher who had his own ""Alice's Adventures in Wonderland"" experience when he discovered badge making. While he has made a number of fun blinky beepy ornaments and badges, his found his passion with the 2020 eChallengeCoin - an interactive and text story challenge puzzle. To help with his development, he created the PortableISP. The 2021 eChallengeCoin required a new chip which precipitated the creation of the PortaProg which serves as both his development tool an his production and test device.

Website: https://aosc.cc
https://gitlab.com/bradanlane
https://aosc.cc/blinks

Twitter: @bradanlane

SpeakerBio: Sara Cladlow
No BIO available

Description:
What is a PortaProg and why would I use it? You can use the PortaProg for flashing firmware to a wide range of Atmel chips using the ISP or UPDI interfaces. It can also read/write FUSES, and access EEPROM. It can flash a chip interactively during development or from its on-board SPIFFS storage at the bench or in the field. The talk will demonstrate it being used for rapid programming of ATTiny badges, performing an update to an ATMega device in the field, and dumping the firmware from an Ardiuno based device without a computer. You will also see how the PortProg has spawned a 3D printed plug-and-play test jig design …. or just attend to see if the demos crash and burn.

#hhv-talk-qa-use-a-portaprog-text https://discord.com/channels/708208267699945503/739571364821729310

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 09:30-10:30 PDT

Title: Use a PortaProg to flash, dump, and test ISP and UPDI chips

When: Saturday, Aug 7, 09:30 - 10:30 PDT

Where: Hardware Hacking Village (Virtual Talk)

Speakers: Bradán Lane,Sara Cladlow

SpeakerBio: Bradán Lane
Bradán Lane is a UX Design and User Researcher who had his own ""Alice's Adventures in Wonderland"" experience when he discovered badge making. While he has made a number of fun blinky beepy ornaments and badges, his found his passion with the 2020 eChallengeCoin - an interactive and text story challenge puzzle. To help with his development, he created the PortableISP. The 2021 eChallengeCoin required a new chip which precipitated the creation of the PortaProg which serves as both his development tool an his production and test device.

Website: https://aosc.cc
https://gitlab.com/bradanlane
https://aosc.cc/blinks

Twitter: @bradanlane

SpeakerBio: Sara Cladlow
No BIO available

Description:
What is a PortaProg and why would I use it? You can use the PortaProg for flashing firmware to a wide range of Atmel chips using the ISP or UPDI interfaces. It can also read/write FUSES, and access EEPROM. It can flash a chip interactively during development or from its on-board SPIFFS storage at the bench or in the field. The talk will demonstrate it being used for rapid programming of ATTiny badges, performing an update to an ATMega device in the field, and dumping the firmware from an Ardiuno based device without a computer. You will also see how the PortProg has spawned a 3D printed plug-and-play test jig design …. or just attend to see if the demos crash and burn.

#hhv-talk-qa-use-a-portaprog-text https://discord.com/channels/708208267699945503/739571364821729310

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Sunday - 11:30-12:30 PDT

Title: Use a PortaProg to flash, dump, and test ISP and UPDI chips
When: Sunday, Aug 8, 11:30 - 12:30 PDT
Where: Hardware Hacking Village (Virtual Talk)
Speakers: Bradán Lane,Sara Cladlow

SpeakerBio: Bradán Lane
Bradán Lane is a UX Design and User Researcher who had his own ““Alice’s Adventures in Wonderland”” experience when he discovered badge making. While he has made a number of fun blinky beepy ornaments and badges, his found his passion with the 2020 eChallengeCoin - an interactive and text story challenge puzzle. To help with his development, he created the PortableISP. The 2021 eChallengeCoin required a new chip which precipitated the creation of the PortaProg which serves as both his development tool an his production and test device.

Website: https://aosc.cc
https://gitlab.com/bradanlane
https://aosc.cc/blinks

Twitter: @bradanlane

SpeakerBio: Sara Cladlow
No BIO available

Description:

What is a PortaProg and why would I use it? You can use the PortaProg for flashing firmware to a wide range of Atmel chips using the ISP or UPDI interfaces. It can also read/write FUSES, and access EEPROM. It can flash a chip interactively during development or from its on-board SPIFFS storage at the bench or in the field. The talk will demonstrate it being used for rapid programming of ATTiny badges, performing an update to an ATMega device in the field, and dumping the firmware from an Ardiuno based device without a computer. You will also see how the PortProg has spawned a 3D printed plug-and-play test jig design …. or just attend to see if the demos crash and burn.

#hhv-talk-qa-use-a-portaprog-text https://discord.com/channels/708208267699945503/739571364821729310

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 10:15-11:15 PDT

Title: Use DNS to detect your domains are abused for phishing
When: Saturday, Aug 7, 10:15 - 11:15 PDT
Where: Blue Team Village - Main Track (Virtual)
Speakers: Karl Lovink a.k.a. Cyb0rg42,Arnold Holzel

SpeakerBio: Karl Lovink a.k.a. Cyb0rg42
Jarl is the Technical Lead of the Security Operations Center of the Dutch Tax and Customs Administration. He must ensure that the security analysts of the SOC can do their job well in the technical field. Besides, he is responsible, among other things, for strengthening the network of governments and companies, so that the right information is quickly available in the event of threats and incidents. Karl obtained the title Master of Security in Information Technology (MSIT) at Eindhoven University of Technology. He loves biohacking technology and has seven RFID / NFC chips implanted in his body, including a credit card.
Twitter: @cyb0rg42

SpeakerBio: Arnold Holzel
No BIO available

Description:

As a high-profile public-sector organization, the Dutch Tax and Customs Administration deals with criminals claiming to be representatives of the organization and contacting the public with phishing e-mails every day. By using Splunk and RFC's like, RFC7208 – Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, we have developed a technique to identify phishing attacks that are carried out under the disguise of the Dutch Tax and Customs Administration.

We start with a short introduction to protocols available to secure e-mail. Securing e-mail means making it more difficult to intercept e-mails in transport and perform phishing attacks. After that, we present some real-life phishing examples pointing to how finding the phishers would have been much easier. The same applies to the Notice and Take Downs for the phishing sites. We continue by introducing the secure e-mail standards like STARTTLS, Sender Policy Framework (SPF), Domain Identified Keys (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC), SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE), SMTP Mail Transfer Agent Strict Transport Security (MTA-STS) on which the technique detecting phishing attacks is based on. Here we present how all secure e-mail protocols work together to be able to monitor e-mail traffic for potential phishing attacks. You can get information about the senders' e-mail address, sender's MTA and the recipient's MTA. Both the receiving and the sending MTAs are not located within your infrastructure. Passive DNS intelligence and Shodan are used for the enrichment of the IP addresses. We have implemented these techniques in Splunk, including various dashboards, searches, and lookups. But the implementation can be done in either which log management system, for instance, ElasticSearch. Also, a wizard has been created to facilitate the generation of the TXT records for your DNS zone file. The implementation we have created in Splunk is downloadable from GitHub for free. The Splunk App contains all necessary dashboards, searches, lookups to get a quick start. Also, a wizard is included to create the DNS TXT records, which can be complicated. In principle, an e-mail track-and-trace system has been built using Splunk and DNS logs.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Saturday - 12:15-12:45 PDT

Title: Using Barq to perform AWS Post-Exploitation Actions

When: Saturday, Aug 7, 12:15 - 12:45 PDT

Where: Cloud Village (Virtual)

SpeakerBio: Mohammed Aldoub

Mohammed Aldoub is an independent security consultant and Blackhat Trainer from Kuwait, who, in his 11 years of experience, worked on creating Kuwait's national infrastructure for PKI, cryptography, smartcards and authentication. Mohammed delivers security trainings, workshops and talks in the Netherlands, USA, Sweden, London, Czech Republic, Singapore, Dubai, Lebanon, Riyadh, Kuwait, in events like Blackhat (USA,EU) Infosec in the City, OPCDE, SEC-T and others. Mohammed is focusing now on APIs, secure devops, modern appsec, cloud-native security, applied cryptography, security architecture and microservices. He is the author of "barq", the AWS post exploitation attack framework, which you can find at: https://github.com/Voulnet/barq and he's also the author of Desharialize, which you can find at: https://github.com/Voulnet/desharialize Mohammed is deeply interested in malware, especially those used by state actors in the Middle East zone, where he volunteered as OWASP Kuwait's chapter leader.
Twitter: @Voulnet
https://github.com/voulnet

Description:

barq is a post-exploitation framework that allows you to easily perform attacks on a running AWS infrastructure. It allows you to attack running EC2 instances without having the original instance SSH keypairs. It also allows you to perform enumeration and extraction of stored Secrets and Parameters in AWS.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Friday - 14:40-15:10 PDT

Title: Using OSINT to Aid in Human Trafficking and Smuggling Cases
When: Friday, Aug 6, 14:40 - 15:10 PDT
Where: Recon Village (Virtual)

SpeakerBio: Rae
No BIO available
Twitter: @wondersmith_rae

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Friday - 10:55-11:25 PDT

Title: Using Passive DNS for gathering Business Intelligence
When: Friday, Aug 6, 10:55 - 11:25 PDT
Where: Recon Village (Virtual)

SpeakerBio: Andy Dennis
No BIO available

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

SEV - Saturday - 12:30-13:30 PDT

Title: Using SE to create insider threats and win all the things
When: Saturday, Aug 7, 12:30 - 13:30 PDT
Where: Social Engineer Village (Virtual)

SpeakerBio: Lisa Forte
Lisa Forte is a European social engineering and insider threat expert. She runs cyber crisis simulations for large companies to help them prepare for attacks of all types. She actually started her security career stopping pirates off the coast of Somalia.

Lisa a passionate about two things: tech for good and that pineapple on pizza should be banned by the United Nations.

She is a proud Italian/ Brit and has won numerous awards for her contributions in tech. Little known fact she actually once auditioned for Cirque Du Soleil.

When she is not working you can usually find her exploring abandoned mines or hanging off the side of a cliff somewhere.

Description:

We talk a lot about that "quick and dirty" social engineering but there is a much scarier, longer term attack that yields far more damage. Instead of that persuasive email or that one hugely urgent phone call these attacks are aimed at turning your key staff from loyal employees into insider threats- Without your knowledge and even without theirs.

How can loyal, hard working staff be convinced to acquire and exfiltrate sensitive commercial data? It all starts with a friend request.

Social Engineer Village will stream content to Twitch.

Twitch: https://www.twitch.tv/socialengineerllc

Return to Index - Add to Google Calendar - ics Calendar file

RFV - Thursday - 12:00-11:59 PDT

Title: Using UAV in Military Zone Areas by GPS Spoofing with RF Devices
When: Thursday, Aug 5, 12:00 - 11:59 PDT
Where: Radio Frequency Village (Virtual)

SpeakerBio: Mehmet Onder Key
No BIO available

Description:
This talk has been released on YouTube.

YouTube: https://www.youtube.com/watch?v=yQ2lrUJ5a04

Radio Frequency Village will not be streaming any talks, but they will be making talks available on their YouTube channel.

YouTube: https://youtube.com/c/RFHackersSanctuary

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 20:00-01:59 PDT

Title: Vampire the Masquerade (Party)
When: Friday, Aug 6, 20:00 - 01:59 PDT
Where: Bally's Skyview 2

Description:

Its... Vampire the masquerade for the Las vegas setting, in las vegas... Because I heard people like Vegas and it might be fun to do.

Return to Index - Add to Google Calendar - ics Calendar file

Title: VDP in aviation: Experiences and lessons learnt as a researcher
When: Saturday, Aug 7, 09:30 - 10:50 PDT
Where: Aerospace Village (Virtual Talk)

SpeakerBio: Matt Gaffney
Following his career in the British Army, Matt has been working with clients in various industries. However, his best years were spent working in aviation, specifically systems found in the Aircraft Information Systems Domain. More recently he has turned his attention to security in UAS.

Description:

Following a Vulnerability Disclosure to an aircraft manufacturer in 2019 little did Gaffers know that he was about to start on a journey in to a world where vulnerabilities are considered features and unless you can argue a safety impact you are not taken seriously. Without divulging the details, this talk will discuss the steps taken, what worked, what failed and some advice for anyone else who finds themselves in a similar situation.

This talk will be streamed on YouTube: https://www.youtube.com/watch?v=q5E_y8jLTv8

Aerospace Village talks will be streamed to YouTube.

YouTube: https://www.youtube.com/c/AerospaceVillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Velociraptor - Dig Deeper
When: Friday, Aug 6, 10:45 - 11:45 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Mike Cohen
Dr. Mike Cohen has over 20 years of experience in applying and developing novel incident response and digital forensics tools and techniques. He has previously worked in the Australian Department of Defence as an information security specialist, at the Australian Federal Police specialising in digital forensics, network and memory forensics, and spent 8 years in Google developing tools such as GRR and Rekall. In 2018, Mike founded the Velociraptor project, an advanced open source DFIR framework. Mike has recently joined Rapid7 to promote and further develop Velociraptor into a fully featured enterprise DFIR toolkit.
Twitter: @velocidex

Description:

The recent increase in network compromises and sophistication of attackers has underscored the need to rapidly identify and remediate attacks at a large scale across the enterprise. Having the ability to rapidly collect, detect and remediate across a network is a game changer for any Digital Forensics and Incident Response (DFIR) team. It provides unprecedented visibility into the state of the endpoint and the ability to tailor responses as the investigation evolves. Having this capability in an open-source tool that allows for truly surgical collection – at speed, at scale and free – is a triple bonus.

Velociraptor is fast becoming the standard DFIR tool for hunting at scale. Featuring a powerful query language called VQL, allowing for rapidly adapting to fluid DFIR introsions, Velociraptor places unprecedented reach, flexibility and power in the hands of responders.

Unlike more traditional remote forensic tools which collect large amounts of raw data for offline processing, VQL allows defenders to perform analysis directly on the endpoint. This new approach allows defenders to collect only high value, tactical information to affect their response, and leverage current state of the art digital forensic analysis techniques into detection.

This talk will provide some examples of Velociraptor's use in typical DFIR scenarios, such as compromise assessment, wide spread remediation and rapid response. Specifically, we examine the process of going from a detection idea, writing the VQL to detect it and then hunting a large network (10k+ hosts) to identify the compromised hosts in minutes. Finally we illustrate how these custom detections can be elevated to real time monitoring rules (also implemented by VQL) to allow the endpoint to autonomously detect future compromises even while being offline!

Velociraptor is the open source DFIR tool the industry has been crying out for - making large scale DFIR fast, efficient and surgical!

Presentation outline

Problem statement
Have you ever tried to hunt a large network to quickly identify and remediate an ongoing attack on your network? You probably found that traditional DFIR techniques, such as parsing the ntfs filesystem for evidence of deleted files, parsing prefetch files for evidence of past program execution or yara scanning large numbers of files simply do not scale to many thousands of endpoints.

Introducing Velociraptor - deployment architecture and overview This talk introduces the new standard in opensource DFIR investigations - Velociraptor. This tool simplifies and streamlines many of the common tasks in traditional DFIR investigation - dealing efficiently with scale.

Example of simple - pre packaged detections - 1 -2 slides Would you like to hunt executions of lolbins (living off the land binaries) within a certain time window and in short succession? No problem - Velociraptor can query all your endpoints and will answer within minutes.

What makes this work? VQL introduction
Velociraptor is driven by a unique query language called VQL. This language underpins all Velociraptor's features and allows users to customize their investigations by applying VQL to both control Velociraptor and to adapt to detecting new adversary tools and techniques.

The real game changer with Velociraptor is enabling defenders to go from a blog post, or some research about a new vulnerability or attack technique to a high quality detection, and then proceed to hunt across a vast network in minutes.

Case studies walk through (each case about 10 min) This talk will walk though some of these examples (specific examples may change/revise before the talk):

Scan the NTFS USN journal for webshell install activity within the past days Build a dynamic file parser in VQL for a new file format just presented by a blog post (e.g. powershell readline history file https://0xdf.gitlab.io/2018/11/08/powershell-history-file.html or a similar example)

The talk will go through the process of building a query from scratch - reading public information about a detection technique, writing some VQL to identify the IOC on a compromised system, then running a hunt on 10k+ machines to identify the compromised hosts. All this will be done using open source tools and freely available resources!

Post hunt analysis - post processing with VQL We then tour the Velociraptor GUI and see how to quickly examine the compromised endpoints for further triage and remediation. We can interactively collect files, registry keys and raw NTFS artifacts directly through a familiar GUI.

VQL event monitoring - unique on host detection (2-3 slides) Finally we discuss VQL's unique real time monitoring capabilities. Unlike other query languages in endpoint tools, the VQL query does not need to have a finite run time. Instead it is possible to write a query which monitors for new events permanently. These "Event Monitoring Queries" can be used to build real time detections for future events.

This novel approach really changes the current state of the art in detection and response. Currently, EDR tools forward events from the endpoint to a central SIEM with backend automated detections raising escalations for operators to manually go back and try to collect additional information from the endpoint or remediate it. This leads to long OODA loop times and increases the time between compromise and response.

VQL event monitoring queries are powerful queries that bring the response to the end point. Once installed, the query codes a "response plan" whereby the endpoint already knows what to do if a certain condition is met, even if the endpoint is offline! We term this an autonomous response plan.

Follow through to implement the above examples as monitoring queries (2 slides per example) In the talk, we will follow through some of these examples into the next logical step, which is to deploy event monitoring queries on all endpoints to prevent future compromise. That is, we go from a detection query that tells us when run if the EP is compromised to an event query that will automatically respond in the future when the EP becomes compromised with the same vector! This is unprecedented!

Conclusion and call to action
Velociraptor is an open source DFIR tool bursting on the scene in 2019 (we initially presented it at the SANS 2019 DFIR summit) but since then, there have been many features added and the tool is now quickly becoming the standard DFIR tool to use for triage, detection and remediation.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

RCV - Friday - 15:20-16:05 PDT

Title: Venator: Hunting & Smashing Trolls on Twitter
When: Friday, Aug 6, 15:20 - 16:05 PDT
Where: Recon Village (Virtual)

SpeakerBio: Mauro Cáseres Rozanowski
Mauro Eldritch is an Argentine Hacker & Speaker, Founder of BCA and DC5411. He was a Speaker at DEF CON (six times!), ROADSEC (LATAM's biggest security conference), DEVFEST Siberia, DragonJAR Colombia (biggest spanish-speaking conference in LATAM), P0SCON Iran, Texas Cyber Summit and EC-Council Hacker Halted among other conferences (25+).

In the past, he worked for many government organisms such as Ministry of Security, Federal Revenue Administration, Ministry of Health, Ministry of Economy, Ministry of Production and both SecBSD & FreeBSD Projects.

Twitter: @mauroeldritch

Description: No Description available

Recon Village talks will stream to YouTube.

YouTube: https://www.youtube.com/c/ReconVillage

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Saturday - 21:00-01:59 PDT

Title: Vetcon Meetup (Hybrid)
When: Saturday, Aug 7, 21:00 - 01:59 PDT
Where: Bally's Skyview 5

Description:

A large friendly gathering of Veterans AND Non-Veterans, to help those who are recent Veterans integrate within our INFOSEC community, to make them feel welcome, and that there are other Veterans and Veteran supporters who are here to help them further their infosec career. Both online and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

Title: Voting Village Keynote Remarks
When: Saturday, Aug 7, 10:00 - 10:30 PDT
Where: Voting Village (Talks - Virtual)

SpeakerBio: Thomas Hicks
Thomas Hicks was nominated by President Barack H. Obama and confirmed by unanimous consent of the United States Senate on December 16, 2014 to serve on the U.S. Election Assistance Commission (EAC). He has served as chairman of the commission for two terms. Commissioner Hicks has focused his efforts on voter access. Under his leadership, the EAC developed a pocket-sized voter card that serves as a guide on voting rights for voters with disabilities. The card is provided in both Braille and large print. The EAC has worked with advocacy groups and election officials to distribute the card.

In addition, Mr. Hicks has addressed the difficulties overseas voters have when requesting and returning their ballots, such as dealing with foreign IP addresses and issues with timely ballot delivery. He worked with key states to set up a help desk. Now, overseas voters receive an email response directing them to the help desk to obtain their ballots.

He serves as the designated federal officer for the Board of Advisors.

Mr. Hicks is a frequent speaker at conferences in the United States and overseas on issues such as voter access and cybersecurity.

Prior to his appointment with EAC, Commissioner Hicks served as a senior elections counsel and minority elections counsel on the U.S. House of Representatives Committee on House Administration, a position he held from 2003 to 2014. In this role, Mr. Hicks was responsible for issues relating to campaign finance, election reform, contested elections and oversight of both the U.S. Election Assistance Commission and the Federal Election Commission. His primary responsibility was advising and providing guidance to the committee members and caucus on election issues. Mr. Hicks has talked with Americans in every state about their voting experiences. In addition, he has worked with state and local election officials across America to address critical election concerns.

Prior to joining the U.S. House of Representatives, Mr. Hicks served as a senior lobbyist and policy analyst from 2001 to 2003 for Common Cause, a nonpartisan, nonprofit organization that empowers citizens to make their voices heard in the political process and to hold their elected leaders accountable to the public interest. Mr. Hicks has enjoyed working with state and local election officials, civil rights organizations and all other stakeholders to improve the voting process.

Mr. Hicks served from 1993 to 2001 in the Clinton administration as a special assistant and legislative assistant in the Office of Congressional Relations for the Office of Personnel Management. He served as agency liaison to the United State Congress and the president’s administration on matters regarding federal personnel policies and regulations.

Mr. Hicks received his J.D. from the Catholic University of America, Columbus School of Law and his B.A. in Government from Clark University (Worcester, MA). He also studied at the University of London (London, England) and law at the University of Adelaide (Adelaide, Australia).

Description: No Description available

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

VMV - Friday - 10:00-10:30 PDT

Title: Voting Village Logistical Information Broadcast (Discord, Youtube, Twitch)
When: Friday, Aug 6, 10:00 - 10:30 PDT
Where: Voting Village (Talks - Virtual)

Description:
Information on how to follow the live conversation on our discord channel

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

Title: Vulnerability Exchange: One Domain Account For More Than Exchange Server RCE
When: Saturday, Aug 7, 18:00 - 18:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Tianze Ding
Tianze Ding is a senior security researcher at Tencent Security Xuanwu Lab. His research focuses on web security, active directory security and red teaming. He reported some vulnerabilities to Microsoft, Apple, Google, etc. He has spoken at BlackHat Asia.
Twitter: @D1iv3

Description:

Microsoft Exchange Server is one of the most famous mail servers in the world. It not only stores a large amount of sensitive corporate information, but also plays an important role in Microsoft Active Directory, so it has become a high-value target for both APT groups and red teams.

In the past few months, some high-risk vulnerabilities in Exchange Server have been exposed, which mainly target vulnerable ASP.NET code. But the architecture of Exchange Server is complicated, and its attack surface is not limited to ASP.NET, this talk will analyze and attack Exchange Server from a different perspective.

I will share the following two new vulnerabilities I found, as well as the new attack surfaces and how I chained several techniques to successfully exploit them in detail.

1. One of them can result in arbitrary mailbox takeover, attackers can read emails, download attachments, send emails, etc. as any Exchange user.
2. The other can lead to remote code execution on Exchange Server, attackers can gain local administrator privileges and execute arbitrary commands. Furthermore, there is an interesting point, even if you have applied the latest Exchange Server patches, your Exchange Server may still be compromised by this type of attack.

For red teams, Exchange Server RCE is only the beginning. Usually, there are some high-privileged domain users and groups on Exchange Server, I will also introduce a new method in depth to help you perform lateral movement and even privilege escalation to Domain Admin after achieving Exchange Server RCE.

These vulnerabilities have been reported to MSRC and the exploit tools will be released after the talk.

References
[1]
https://www.zerodayinitiative.com/blog/2018/12/19/an-insincere-form-of-flattery-impersonating-users-on-microsoft-excha
[2] https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory [3]
https://docs.microsoft.com/en-us/exchange/client-developer/web-service-reference/ews-operations-in-exchange [4]
https://github.com/quickbreach/ExchangeRelayX [5]
https://blog.compass-security.com/2020/05/relaying-ntlm-authentication-over-rpc/ [6]
https://www.crowdstrike.com/blog/cve-2021-1678-printer-spooler-relay-security-advisory/ [7]
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rpce/425a7c53-c33a-4868-8e5b-2a850d40dc73
[8] https://enigma0x3.net/2017/01/05/lateral-movement-using-the-mmc20-application-com-object/ [9]
https://github.com/SecureAuthCorp/impacket [10] https://github.com/gdedrouas/Exchange-AD-Privesc [11]
https://labs.f-secure.com/tools/sharpgpoabuse/

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=7h38rI8KT30

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20T

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

APV - Friday - 11:00-11:45 PDT

Title: Vulnerability Inheritance - Attacking companies and scoring bounties through 3rd party integrations
When: Friday, Aug 6, 11:00 - 11:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Gal Nagli
Gal Nagli is an Application Security researcher at enso.security and a B.Sc computer science student. Most of his time is spent doing Bug bounties on Hackerone, Synack and BugCrowd - where he recently won "Best Collaboration" award during Okta 2021 Bug Bash. He is mainly focused on automation and enjoys the community by publishing writeups on his blogs, helpful tips in twitter and running a Slack community where bounty hunters collab and hang out.

Description:
Time to Sharpen your Bug Bounty Game! In this session the attendees will learn about vulnerabilities around 3rd party integrations, how to improve their reconnaissance flow and how to scan the entire internet for specific vulnerabilities utilizing Nuclei, by observing Proof of Concepts from the presenter journey and practical examples.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Friday - 12:30-13:30 PDT

Title: Walkthrough of DC 28 HHV Challenges
When: Friday, Aug 6, 12:30 - 13:30 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio:rehr
Rehr is an electrical engineering, and long-time Hardware Hacking Village volunteer. He enjoys teaching and creating challenges that help grow and challenge the hardware hacking community.
Twitter: @mediumrehr

Description:
Last year we (the HHV) released a series of hardware hacking challenges for DEF CON attendees to solve during the conference (and after). Many attempted the challenges, but only a few (3) solved all 5! Join us as we will walk through how to solve all 5 of the DC 28 HHV challenges, and attempt to demystify the world of hardware hacking. We may even drop a hint or two for this years' challenges.

#hhv-challenge-text https://discord.com/channels/708208267699945503/739567199647301702

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Saturday - 11:00-11:59 PDT

Title: Walkthrough of DC 28 HHV Challenges
When: Saturday, Aug 7, 11:00 - 11:59 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio:rehr
Rehr is an electrical engineering, and long-time Hardware Hacking Village volunteer. He enjoys teaching and creating challenges that help grow and challenge the hardware hacking community.
Twitter: @mediumrehr

Description:
Last year we (the HHV) released a series of hardware hacking challenges for DEF CON attendees to solve during the conference (and after). Many attempted the challenges, but only a few (3) solved all 5! Join us as we will walk through how to solve all 5 of the DC 28 HHV challenges, and attempt to demystify the world of hardware hacking. We may even drop a hint or two for this years' challenges.

#hhv-challenge-text https://discord.com/channels/708208267699945503/739567199647301702

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

HHV - Sunday - 09:00-09:59 PDT

Title: Walkthrough of DC 28 HHV Challenges
When: Sunday, Aug 8, 09:00 - 09:59 PDT
Where: Hardware Hacking Village (Virtual Talk)

SpeakerBio:rehr
Rehr is an electrical engineering, and long-time Hardware Hacking Village volunteer. He enjoys teaching and creating challenges that help grow and challenge the hardware hacking community.
Twitter: @mediumrehr

Description:

Last year we (the HHV) released a series of hardware hacking challenges for DEF CON attendees to solve during the conference (and after). Many attempted the challenges, but only a few (3) solved all 5! Join us as we will walk through how to solve all 5 of the DC 28 HHV challenges, and attempt to demystify the world of hardware hacking. We may even drop a hint or two for this years' challenges.

#hhv-challenge-text https://discord.com/channels/708208267699945503/739567199647301702

Twitch: https://twitch.tv/dchhv

Hardware Hacking Village talks will be streamed to Twitch.

Twitch: https://www.twitch.tv/dchhv

Return to Index - Add to Google Calendar - ics Calendar file

SOC - Friday - 20:00-21:59 PDT

Title: War Story Bunker
When: Friday, Aug 6, 20:00 - 21:59 PDT
Where: Bally's Skyview 3

Description:

One of our favorite parts of DEF CON every year is hearing about what other hackers have been up to with harrowing tales of red team exercises gone wrong, or so very right. We've also heard of valiant efforts of defense, from our blue team folks while waiting in Linecon. Do you have a cool "war story" to share? Would you like to listen to some fun stories from your fellow hackers? This is the place to be. Join the DEF CON CFP Review Board, Goons, and fellow hackers as we hunker in the (War Story) bunker.

Return to Index - Add to Google Calendar - ics Calendar file

Title: Warping Reality - creating and countering the next generation of Linux rootkits using eBPF
When: Friday, Aug 6, 17:00 - 17:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: PatH
Pat is a loving partner, a comedian to his daughter, and a dedicated ball retriever to his dog.

When he's not spending time being those things, he's a senior security researcher at a public cybersecurity company. Having previously worked as a low-level software dev, he now helps threat hunters uncover and stop advanced actors across the globe.

Twitter: @pathtofile
https://path.tofile.dev/

Description:
With complete access to a system, Linux kernel rootkits are perfectly placed to hide malicious access and activity. However, running code in the kernel comes with the massive risk that any change to a kernel version or configuration can mean the difference between running successfully and crashing the entire system. This talk will cover how to use extended Berkley Packet Filters (eBPF) to create kernel rootkits that are safe, stable, stealthy, and portable.

eBPF is one of the newest additions to the Linux kernel, designed to easily load safe, constrained, and portable programs into the kernel to observe and make decisions about network traffic, syscalls, and more. But that’s not it’s only use: by creating eBPF programs that target specific processes we can warp reality, presenting a version of a file to one program and a different version to another, all without altering the real file on disk. This enables techniques such as presenting a backdoor user to ssh while hiding from sysadmins, or smuggling data inside connections from legitimate programs. This talk will also cover how to use these same techniques in malware analysis to fool anti-sanbox checks.

These ideas and more are explored in this talk alongside practical methods to detect and prevent this next generation of Linux rootkits.

REFERENCES
- DEFCON 27 - Evil eBPF Practical Abuses of In-kernel Bytecode Runtime - A talk about abusing eBPF for exploitation and privilege escalation
    - ◊ eBPF Website
    - ◊ https://ebpf.io
    - ◊ A website by the eBPF community with documentation and links to existing projects
    - ◊ eBPF Slack
    - ◊ https://ebpf.io/slack
    - ◊ A Slack channel run by the eBPF community
    - ◊ Libbpf Bootstrap
    - ◊ https://github.com/libbpf/libbpf-bootstrap
    - ◊ A sample project designed to provide a template to creating eBPF programs with Libbpf

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=g6SKWT7sROQ

Media

(Main Talk)
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%2

(Demo)
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20P

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Friday - 16:30-17:59 PDT

Title: Watch Out! And just skip the packer
When: Friday, Aug 6, 16:30 - 17:59 PDT
Where: Blue Team Village - Workshop Track 2 (Virtual)

SpeakerBio: Felipe Duarte
Malware researcher, CEH, GREM, electronics geek, IoT enthusiast, programmer, drone lover and machine learning fan. Just hunting malware for fun!
Twitter: @dark0pcodes

Description:

Analyzing malware is not an easy task. It is a slow process that becomes even more challenging with all the different protections added by threat actors to hide their secrets.

Several techniques could be used to obscure malicious code, however one of the first and most commonly used are the packers. Nowadays, almost every malicious piece of code uses a packer; so, if you really want to understand its inner workings you must first defeat its packer. But do you know how to get rid of this defense without losing your mind? Well, join me and we will find out.

Malware remains as one of the most effective tools used by cyber criminals to commit fraud. Far from now are the days in which viruses were just jokes. And, it is not me being dramatic, just look at the news and you will see that this situation is getting worse every day.

There are several reasons that make these threats successful, including but not limited to:

Launching a malware attack is NOT rocket science, you can find open source or leaked code on Github and even tutorials on Youtube. They come in different flavors according to your needs, from very simple keyloggers to highly modular botnets that can be updated on the fly. If you don’t want to deal with technical stuff, you can even buy malware-as-a-service (and you could get 24/7 support). For us as defenders, understanding the technical details of these type of threats is not an easy task, it requires specialized tools and skills and even with those, be aware that bad guys will always try to obscure their creations to slow down the analysis. This sounds scary, and especially intimidating if it is your first time dealing with these "creatures"; but it is not the end of the world, we just need to adapt and overcome these challenges.

Join me in this workshop if you want to learn several techniques that will help you to get rid of the first and most common type of defense implemented by malware to hide its secrets (packers/crypters). Let's remove their armors and see what is hidden behind!

Return to Index - Add to Google Calendar - ics Calendar file

PHV - Friday - 09:00-10:59 PDT

Title: Web App Penetration Testing Workshop
When: Friday, Aug 6, 09:00 - 10:59 PDT
Where: Packet Hacking Village - Workshops (Virtual)

SpeakerBio: Sunny Wear , WEB SECURITY ARCHITECT AND PENETRATION TESTER
Dr. Sunny Wear (Twitter: @SunnyWear) is a Web Security Architect and Penetration Tester. She provides secure coding classes, creates software, and performs penetration testing against web/API and mobile applications. Sunny has more than 25 years of hands-on software programming, architecture and security experience and holds a Doctor of Science in Cybersecurity. She is a published author, "Burp Suite Cookbook", a developer of mobile apps, such as the “Burp Tool Buddy,” and is a Pluralsight content creator, "Burp Suite for Beginners/Advanced/Writing Plugins". She regularly speaks and holds classes at security conferences such as Defcon, Hackfest, and BSides.
Twitter: @SunnyWear

Description:
Gain hands-on experience learning how to perform web application penetration testing in this two-hour workshop with the author of the Burp Suite Cookbook, Dr. Sunny Wear. Students will learn Injections attacks such as Cross-site Scripting and SQL Injection attacks, brute-forcing tactics, and optimization techniques for Burp Suite including configurations and macros.

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Saturday - 10:00-10:15 PDT

Title: Welcome Note
When: Saturday, Aug 7, 10:00 - 10:15 PDT
Where: Blockchain Village / Paris Vendome B
Speakers: Nathan,Ron Stoner

SpeakerBio: Nathan
No BIO available

SpeakerBio: Ron Stoner
No BIO available

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Sunday - 10:00-10:15 PDT

Title: Welcome Note
When: Sunday, Aug 8, 10:00 - 10:15 PDT
Where: Blockchain Village / Paris Vendome B
Speakers: Nathan,Ron Stoner

SpeakerBio: Nathan
No BIO available

SpeakerBio: Ron Stoner
No BIO available

Description: No Description available

This content will be presented live and in-person.

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 09:00-09:30 PDT

Title: Welcome to AI Village
When: Saturday, Aug 7, 09:00 - 09:30 PDT
Where: AI Village (Virtual)

SpeakerBio: AI Village Organizers
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 10:00-10:59 PDT

Title: Welcome To DEF CON - Dark Tangent & Making the DEF CON 29 Badge
When: Friday, Aug 6, 10:00 - 10:59 PDT
Where: Track 1 Live; DCTV/Twitch #1 Live
Speakers: Dark Tangent,Katie Whiteley,Michael Whiteley

SpeakerBio: Dark Tangent
No BIO available

SpeakerBio: Katie Whiteley
Katie is a wife, mother, and graphic designer. She likes long walks on the beach because there's no internet connection.

Together with Michael, they are MK Factor, a husband/wife badgemaker team. They've created badges for many conferences and groups like OpenWest, Saintcon, DC801, Car Hacking Village, and many unofficial DEF CON badges. Together they earned a black badge for Car Hacking at DEF CON 24.

Twitter: @ktjgeekmom

SpeakerBio: Michael Whiteley
Michael is a husband, father, and electronics geek. He doesn't like long walks on the beach, but prefers to be indoors with a fast internet connection.

Together with Katie, they are MK Factor, a husband/wife badgemaker team. They've created badges for many conferences and groups like OpenWest, Saintcon, DC801, Car Hacking Village, and many unofficial DEF CON badges. Together they earned a black badge for Car Hacking at DEF CON 24.

Twitter: @compukidmike

Description: No Description available

This talk will be given live in Track 1, and will be streamed to DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 09:00-09:59 PDT

Title: Welcome to Discord
When: Friday, Aug 6, 09:00 - 09:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: Dark Tangent
No BIO available

Description: No Description available

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Friday - 11:00-11:30 PDT

Title: Welcome to Gold Bug
When: Friday, Aug 6, 11:00 - 11:30 PDT
Where: Crypto & Privacy Village (Virtual)

Description:

Description:Join puzzlemasters Maya & Kevin to kick off this year's Gold Bug puzzle challenge!

Crypto & Privacy Village will be streaming their events to YouTube and Twitch.

Twitch: https://www.twitch.tv/cryptovillage

YouTube: https://www.youtube.com/c/CryptoVillage

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 09:00-09:30 PDT

Title: Welcome. A Short Tour of Good and Bad AI in 2021
When: Friday, Aug 6, 09:00 - 09:30 PDT
Where: AI Village (Virtual)

SpeakerBio:AI Village Organizers
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

PYV - Friday - 13:00-13:59 PDT

Title: What happens when businesses decide to enroll cryptocurrency cards
When: Friday, Aug 6, 13:00 - 13:59 PDT
Where: Payment Village (Virtual)

SpeakerBio: Timur Yunusov
No BIO available

Description:
Cryptocurrencies are the new black. They are everywhere, and even your grandparents may now be gossiping about them. In this talk we will make an overview of risks that your brand new cryptocurrency card may carry with it.

Payment Village events will stream to Twitch and YouTube.

--

Twitch: https://www.twitch.tv/paymentvillage

YouTube: https://www.youtube.com/c/PaymentVillage

Return to Index - Add to Google Calendar - ics Calendar file

CCV - Saturday - 10:00-10:15 PDT

Title: What Is Zero Knowledge
When: Saturday, Aug 7, 10:00 - 10:15 PDT
Where: Cryptocurrency Village (Onsite - Paris Champagne Ballroom 1)

SpeakerBio: Sarang Noether, Ph.D.
Sarang Noether is a researcher who focuses on privacy-preserving cryptographic constructions and protocols.

Description:

Lightning overview of the basics of zero knowledge proofs and transaction protocols, and how they relate (or don't) to each other. A Q&A session will follow.

The Cryptocurrency Village is built around conversations and events, not formal talks. Stop by any time to speak with knowledgeable individuals! This village focuses on the security and privacy side of cryptocurrencies, not the investment side.

The Cryptocurrency Village is conveniently located in Paris Champagne Ballroom 1.

Return to Index - Add to Google Calendar - ics Calendar file

Title: What Machine Learning Can and Can't Do for Security
When: Saturday, Aug 7, 11:30 - 11:59 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Wendy Edwards
Wendy is a software developer interested in the intersection of cybersecurity and data science. She’s involved in the NASA Datanauts program and participated in the SANS Women’s Academy, earning GIAC GSEC, GCIH, and GCIA certifications. She has masters degrees in computer science and library and information science from the University of Illinois. She has spoken at Summercon, BSides Chicago, The Diana Initiative, Hackfest Canada, Circle City Con, and DEFCON Ethics Village. In her spare time, she enjoys Scrabble and swimming and has a lively flat-coated retriever named Ciaran.
Twitter: @wayward710

Description:

What can machine learning do for security? A number of things. One major challenge is determining what’s normal and what’s malicious. Machine learning can help with this. For example, ML techniques are used in spam filtering scan email. Machine learning is also being applied to other areas like network traffic monitoring and malware analysis and has potential to detect zero days exploits. However, machine learning isn't magic. We discuss some of the limitations of machine learning, and how problems like false positives can be mitigated.

Most of us have heard vendors promoting products that use "machine learning." But what does that mean? This is a general introduction to machine learning concepts and a discussion of applications to security. We begin by talking about commonly used terminology – what are artificial intelligence, neural networks, machine learning, and deep learning? How do they work?

What can machine learning do for security? A number of things. One major challenge is determining what’s normal and what’s malicious. Machine learning can help with this. For example, ML techniques are used in spam filtering scan email. Large email providers, e.g., Google and Yahoo, have intelligent systems that can create new spam filtering rules based on automated learning.

Machine learning is also being applied to other areas like network traffic monitoring and malware analysis. Traditional network intrusion detection (NIDS) and malware identification involve rules and signatures, where behavior associated with known threats is identified. But what about new threats, such as zero-day exploits? Anomaly-based detection compares traffic to normal behavior, and has the potential to detect previously unknown attacks with no established signature. We present some examples of freely available machine learning software and walk through some simple use cases.

However, machine learning isn't magic, and it has its limitations. The quality of the training data significantly affects the quality of the results, and training data needs to be updated to reflect changes in relationships and new data points. False positives can consume a lot of analysts' time and lead to alert fatigue. We discuss some techniques, e.g. cross-domain correlation, to reduce the number of false positives.

What is "machine learning?" * Definition * How does it work? * What is a neural network? * Common machine learning terminology explained * Supervised vs unsupervised learning * Different kinds of machine learning * Examples of machine learning and security Classification problem * What’s normal? What’s malicious? * Example: spam filtering * Example: network traffic analysis * Traditional NIDS involves rules/signatures * Anomaly detection NIDS (ADNIDS) compares traffic to normal patterns * Example: Behavior-based Malware Analysis * Common AV malware detection involves signatures (patterns related to known behavior) * What about zero-day exploits or malware that can morph? Attack behaviors are different from normal behaviors * Unusual system calls * Writing stolen data to files, registry manipulation, etc * Unusual network traffic (e.g. command and control) * Destinations (lots of unexplained traffic to a particular destination) * Payloads (C&C traffic likely has similar structure) * Software currently using machine learning for security * Examples: spam filters, Splunk Limitations of machine learning * Training data * False positives / alert fatigue * Mitigating false positives Future directions in machine learning and security

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

APV - Saturday - 13:00-13:45 PDT

Title: When nothing goes right, push left. Designing logs for future breach investigations
When: Saturday, Aug 7, 13:00 - 13:45 PDT
Where: AppSec Village (Virtual)

SpeakerBio: Vee
No BIO available

Description:

If we do not have it we should build it.- If nothing goes right, push left.

TL;DR: Your logs should be simple, and structured, they should also contain enough information without disclosing sensitive data. Often accidental information disclosure within the logs can lead to future breaches. This talk focuses on the process of building logs taking into consideration the attack, the defense, and the investigation of breaches. Using the ideals from The Unicorn and The Phoenix project to develop the "Five Philosophies of Logging". This talk explores different aspects of logging pulling from years of experience of breach investigations and magic-wielding.

AppSec Village events will be streamed to YouTube.

YouTube: https://www.youtube.com/c/appsecvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Friday - 10:00-10:30 PDT

Title: When Penetration Testing Isn’t Penetration Testing At All
When: Friday, Aug 6, 10:00 - 10:30 PDT
Where: IoT Village (Talk - Virtual)

SpeakerBio: Ted Harrington
Ted Harrington is the #1 best selling author of HACKABLE: How to Do Application Security Right, and the Executive Partner at Independent Security Evaluators (ISE), the company of ethical hackers famous for hacking cars, medical devices, web applications, and password managers. He’s helped hundreds of companies fix tens of thousands of security vulnerabilities, including Google, Amazon, and Netflix. Ted has been featured in more than 100 media outlets, including The Wall Street Journal, Financial Times, and Forbes. His team founded and organizes IoT Village, an event whose hacking contest is a three-time DEF CON Black Badge winner. He hosts the Tech Done Different podcast.

Description:

When companies want to build secure IoT systems, they know they need to test their system for security flaws, which typically leads them to seek out “penetration testing.” However, this term has become so misused across the security community that it’s hard to decipher what is really happening.

So where does that leave you? What is your security testing program actually doing (and not doing)?

In this keynote, you’ll learn the often widely misunderstood difference about what penetration testing is (and is not). Drawing insights from the #1 bestselling book Hackable, you’ll learn why the distinction matters, and you’ll get an insight into the more advanced tactics used by ethical hackers, such as functionality abuse and exploit chaining. By design, this keynote is more strategic rather than technical, and will equip you with insights to think differently about your security testing program. As a result, you’ll leave with new ideas about how to build better, more secure systems.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 16:00-16:30 PDT

Title: Where We’re Going We Don’t Need Labels: Anomaly Detection for 2FA
When: Saturday, Aug 7, 16:00 - 16:30 PDT
Where: AI Village (Virtual)
Speakers: Rebecca Lynch,Stefano Meschiari

SpeakerBio: Rebecca Lynch
No BIO available

SpeakerBio: Stefano Meschiari
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Saturday - 13:00-13:30 PDT

Title: Who's Afraid of Thomas Bayes?
When: Saturday, Aug 7, 13:00 - 13:30 PDT
Where: AI Village (Virtual)

SpeakerBio: Erick Galinkin
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Friday - 14:05-14:35 PDT

Title: WhoC - Peeking under the hood of CaaS offerings
When: Friday, Aug 6, 14:05 - 14:35 PDT
Where: Cloud Village (Virtual)

SpeakerBio: Yuval Avrahami
Yuval Avrahami is a Principal Security Researcher at Palo Alto Networks, dealing with hacking and securing anything related to containers and cloud. Yuval is a veteran of the Israeli Air Force, where he served in the role of a researcher.
Twitter: @yuval_avrahami

Description:

Running your business-critical applications on the public cloud involves trust. You trust your cloud provider to separate your workloads from other customers' workloads. You trust your cloud provider to patch and update their software and hardware stack. For those of us with trust issues, blindly running our applications in the public cloud can be tough. Fortunately, trust can be earned through visibility, and that's where WhoC can help. WhoC provides a bit of visibility into how Container-as-a-Service (CaaS) offerings run our containers. WhoC (Who Contains) is a container image that upon execution extracts the underlying container runtime. It doesn't try to identify the underlying runtime based on the container's cgroup configuration, the existence of a '.dockerenv' file or any other known trick. WhoC exfiltrates the actual container runtime binary from the underlying host. In this talk Yuval will walk you through how WhoC works and show a demo running WhoC in a popular CaaS offering. You'll learn a surprising truth: Linux containers can actually access one host file - the container runtime.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

CON - Friday - 22:00-23:59 PDT

Title: Whose Slide Is It Anyway
When: Friday, Aug 6, 22:00 - 23:59 PDT
Where: See Description

Description:

For more information, see https://forum.defcon.org/node/237295 or https://twitter.com/whoseslide

This event will be held in Track 1, Bally's

Return to Index - Add to Google Calendar - ics Calendar file

DC - Sunday - 13:00-13:45 PDT

Title: Why does my security camera scream like a Banshee? Signal analysis and RE of a proprietary audio-data encoding protocol

When: Sunday, Aug 8, 13:00 - 13:45 PDT

Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Rion Carter

Rion likes to solve interesting problems- the more esoteric and niche the better! He has varied interests ranging from software development and reverse-engineering to baking and recipe hacking. Rion currently works in DevSecOps where he and his colleagues wonder how they'll be rebranded next (DevSecBizFinOps?). Rumor has it that he bakes a mean batch of fudge brownies.

Description:

All I wanted was a camera to monitor my pumpkin patch for pests, what I found was a wireless security camera that spoke with an accent and asked to speak with my fax machine. Join me as I engage in a signals analysis of the Amiccom 1080p Outdoor Security Camera and hack the signal to reverse engineer the audio tones used to communicate and configure this inexpensive outdoor camera. This journey takes us through spectrum-analysis, APK decompiling, tone generation in Android and the use of Ghidra for when things REALLY get hairy.

REFERENCES

> - JADX: Dex to Java Decompiler - https://github.com/skylot/jadx - Efficiency: Reverse Engineering with ghidra - http://wapiflapi.github.io/2019/10/10/efficiency-reverse-engineering-with-ghidra.html - Guide to JNI (Java Native Interface) - https://www.baeldung.com/jni - JDSP - Digital Signal Processing in Java - https://psambit9791.github.io/jDSP/transforms.html - Understanding FFT output - https://stackoverflow.com/questions/6740545/understanding-fft-output - Spectral Selection and Editing - Audacity Manual - https://manual.audacityteam.org/man/spectral_selection.html - Edit>Labelled Audio>everything greyed out - https://forum.audacityteam.org/viewtopic.php?t=100856 - Get a spectrum of frequencies from WAV/RIFF using linux command line - https://stackoverflow.com/questions/21756237/get-a-spectrum-of-frequencies-from-wav-riff-using-linux-command-line - How to interpret output of FFT and extract frequency information - https://stackoverflow.com/questions/21977748/how-to-interpret-output-of-fft-and-extract-frequency-information?rq=1 - Calculate Frequency from sound input using FFT - https://stackoverflow.com/questions/16060134/calculate-frequency-from-sound-input-using-fft?rq=1 - Intorduction - Window Size - https://support.ircam.fr/docs/AudioSculpt/3.0/co/Window%20Size.html - Android: Sine Wave Generation - https://stackoverflow.com/questions/11436472/android-sine-wave-generation - Android Generate tone of a specific frequency - https://riptutorial.com/android/example/28432/generate-tone-of-a-specific-frequency - Android Tone Generator - https://gist.github.com/slightfoot/6330866 - Android: Audiotrack to play sine wave generates buzzing noise - https://stackoverflow.com/questions/23174228/android-audiotrack-to-play-sine-wave-generates-buzzing-noise

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=JpL3lySZNeM

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20R

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

BICV - Friday - 10:30-10:30 PDT

Title: Why don’t we have IoT, daddy?
When: Friday, Aug 6, 10:30 - 10:30 PDT
Where: Blacks in Cyber

SpeakerBio: Jessica Hoffman
Jessica Hoffman is an IT Audit manger and partner of her Black owned audit and compliance firm. She provides Readiness assessments and audits mainly to the federal healthcare sector but also service various public/private sector fields. She has been in Cybersecurity for 10 years and IT for over 15 years. Prior to starting her small business, she was a federal and state employee; Public service and giving back to the community are two areas that she is dedicated to and she excels in as a dedicated volunteer, mentor, professor and advocate.
Twitter: @JHoBootyFat

Description: No Description available

Blacks in Cyber talks will be streamed on YouTube.

YouTube: https://www.youtube.com/c/BlacksInCybersecurity

Return to Index - Add to Google Calendar - ics Calendar file

Title: Why Hacking Voters Is Easier Than Hacking Ballots

When: Saturday, Aug 7, 13:30 - 13:59 PDT

Where: Voting Village (Talks - Virtual)

SpeakerBio: Maurice Turner

Maurice Turner is the Cybersecurity Fellow at the Alliance for Securing Democracy (ASD) at the German Marshall Fund of the United States (GMF). Turner is a recognized public interest technologist and cybersecurity expert focused on developing strategies to secure critical infrastructure and deter cyber operation escalation. He has been regularly featured in national and international media including the Washington Post, Wall Street Journal, Bloomberg, Fox News, and Reuters. He has also provided testimony before the United States Congress, shared his insights with the European Union, and spoken at numerous security conferences. Turner most recently served as Senior Advisor to the Executive Director at the United States Election Assistance Commission (EAC) providing subject matter expertise in support of local, state, and federal partners to administer elections fairly and securely. Prior to that Turner was Deputy Director of the Internet Architecture project at the Center for Democracy & Technology (CDT) where he led the Election Security and Privacy Project, identifying and updating election cybersecurity practices and infrastructure through multi-sector partnerships. Turner also served as a TechCongress Congressional Innovation Fellow assigned to the U.S. Senate Homeland Security and Governmental Affairs Committee, where he shaped policy and oversaw the preparation of memos, briefings, and hearings on federal IT systems, cybersecurity threats, and cybersecurity regulations.

He holds an MA in Public Administration from the University of Southern California, an BA in Political Science from California State University Fullerton, and a Certificate in Cybersecurity Strategy from Georgetown University.

Description:

Vulnerabilities in US election infrastructure not only expose the nation’s elections to hybrid physical and network attacks, but its voters to influence campaigns designed to cast doubt in the process itself. Authoritarian regimes such as Russia, Iran, and China are capable of conducting both sophisticated disinformation operations and cyber campaigns, and using both methods can be a particularly effective strategy for disrupting an election. Despite significant attention and more (but insufficient) funding in recent years, the overall defensive posture of election infrastructure operators lags behind the offensive cyber capabilities of sophisticated adversaries and criminals.

Elections are not alone. Other critical infrastructure sectors have sustained major disruptions because of cyber attacks like ransomware. However, elections are unique in that a sizable segment of the American public views the electoral process suspiciously and is primed to believe any errors or inconsistencies presented that supports that belief. As a result, adversaries now have at least three distinct attack strategies at their disposal: quietly change enough actual ballots to alter the outcome of a contest, loudly manipulate a small number of ballots to provide “evidence” of a systemic failure to suspicious voters, or launch a pure perception hack through the dissemination of false information to convince voters of widespread fraud absent any evidence.

By analyzing state-backed government messaging across various information mediums using a tool called Hamilton, researchers can track narratives and topics promoted by Russian, Chinese, and Iranian government officials and state-funded media. These trends can help provide context and insights into publicly-available information of breaches, ransomware, or other related attacks against election infrastructure. Election officials and network defenders can work together to improve the resilience of the most important component of the electoral system: voters.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

DC - Saturday - 11:00-11:59 PDT

Title: Wibbly Wobbly, Timey Wimey – What's Really Inside Apple's U1 Chip
When: Saturday, Aug 7, 11:00 - 11:59 PDT
Where: DCTV/Twitch #3 Pre-Recorded
Speakers: Alexander Heinrich,jiska

SpeakerBio: Alexander Heinrich
Alexander is a security researcher at the Secure Mobile Networking Lab at the Technical University of Darmstadt. Before he joined the university as a researcher he gained a lot of experiences an an app developer on Apple operating systems starting with iOS 5. This deep understanding of the systems naturally resulted in a focus on those systems in his security research. He joined the Secure Mobile Networking Lab 2020 as a PhD student right after his Master Thesis on the security of Apple’s Handoff and Universal Clipboard features. After working with a team of skilled researchers on AirDrop and Apple’s Find My network his focus now shifted to the security and privacy of ultra-wideband and Apple U1 chip.
Twitter: @Sn0wfreeze

SpeakerBio:jiska
jiska breaks things.
Twitter: @naehrdine

Description:
Apple introduced an Ultra Wideband (UWB) chip in the iPhone 11. Its cryptographically secured spatial measurement capabilities are accessible via the Nearby Interaction framework since iOS 14. As of now, it only supports interaction with other Apple devices including the latest Apple Watch and HomePod mini. These are the first steps to support UWB in a larger ecosystem, as measuring precise distance and direction can be an enabler for various future applications. The automotive industry already announced UWB support for mobile car keys on the iPhone.

But what’s really inside Apple’s U1 chip, internally called Rose? In this talk, we will travel through time, space, firmware and kernel components—and fight daemons to modify firmware interaction from user space. This will not only cover one or two, but three firmwares that process or forward each Rose time measurement: The Rose Digital Signal Processor (DSP), Rose Application Processor (AP), and the Always-On Processor (AOP).

REFERENCES

> There's almost nothing known about UWB on the iPhones... So the only reference is this:
> https://support.apple.com/guide/security/ultra-wideband-security-sec1e6108efd/web

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=k1H7fiVlTPA

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20J

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

Title: WiFi Kraken Lite
When: Saturday, Aug 7, 14:00 - 15:50 PDT
Where: DemoLab Video Channel 2

SpeakerBio: Henry Hill
Henry Hill is an expert with computer hardware and is able to design and build the most bleeding edge systems that are the fastest in the world. His internal knowledge of architecture and system bottlenecks help him build systems capable of extreme processing and even faster storage. Henry is also an expert with mechanical engineering and fabrication. When his modifications aren't appearing in d4rkm4tter's projects, they can be seen in his race car at the track.

Description:

Tool or Project Name: The WiFi Kraken Lite

Short Abstract:
D4rkm4tter and Henry have been obsessed with monitoring wireless networks and have built hardware to meet the challenges of scanning and testing in the most busy and client dense environments. The WiFi-Kraken Lite contends with these issues in a smaller package without sacrificing any monitoring performance. This project is the results of years of research into the most effective way to scan and audit wireless in a single box that can be easily deployed or used as a hardened terminal in the most rugged conditions.

The WiFi-Kraken Lite consists of a single-board computer which connects 12 wireless radios that enables scanning and auditing WiFi, Bluetooth, LoRaWAN and other commonly used wireless protocols. The number of wireless devices is growing as well as the way those devices are being connected. Having an all-in-one wireless monitoring solution will give you the ability to track this data across these bands and give you the best picture of what's happening in the air around you.

This demonstration will provide you the information so that you can build your own all-in-one monitoring device. You will also gain an overview of capture technologies including Kismet that will help you perform this type of analysis in your own environments. Finally once the data is capture, you will get an understanding of efficient data processing using tools like Wireshark and d4rkm4tter's own PCAPinator tool.

Short Developer Bio:
Mike Spicer (d4rkm4tter) is a mad scientist hacker who likes to meddle with hardware and software. He is particularly obsessed with wireless. He has a degree in computer science which he has put to use building and breaking a wide array of systems. These include web application pentesting, wireless monitoring and tracking as well as reverse engineering. He is the creator of the #WiFiCactus and has been seen presenting and demoing at a number of conferences including DEF CON. He is a Kismet cultist and active in the wireless and wardriving communities.

Henry Hill is an expert with computer hardware and is able to design and build the most bleeding edge systems that are the fastest in the world. His internal knowledge of architecture and system bottlenecks help him build systems capable of extreme processing and even faster storage. Henry is also an expert with mechanical engineering and fabrication. When his modifications aren't appearing in d4rkm4tter's projects, they can be seen in his race car at the track.

URL to any additional information:
Palshack.org/wifi-kraken-lite (Site will be online for DEF CON)

Detailed Explanation of Tool:
The WiFi-Kraken Lite is a wireless monitoring system that is a rugged box with a single board computer and 12 wireless devices that are capable of simultaneously monitoring a large number of frequencies and protocols while storing that data in real time. The primary motivation for this project was to be able to gain visibility into as much of the wireless spectrum as possible in very congested networks in a small rugged form factor. Networks with a large number of clients that have a large number of access points can be difficult to perform analysis on. These networks typically have clients who switch between

networks and can switch frequencies lending to more confusion when tracking with only a single radio. By increasing the number of radios as well as adding support for other protocols beyond just WiFi, a more complete understanding of the wireless environment can be documented. This information can then be used for defenders or penetration testers to identify vulnerable networks, vulnerable clients, or verify security that can be easily documented and audited.

The hardware is set up so that it minimizes the number of bottlenecks between the actual frames in the air and when it writes the data to disk. It does this by taking advantage of the high-bandwidth PCI-express bus to connect wireless devices. From there the data transfers to a high-speed NVMe storage device. The operating system is Linux which allows us to take advantage of a number of open source tools and projects that help us capture the data. These projects include Kismet, BlueZ, btscanner, and Feather TFT LoRa Sniffer. Custom scripts help us manage and easily configure The WiFi-Kraken Lite for the desired mode.

The buildout of the project uses a hardened Pelican like case which provides the ruggedness and physical security so that the system can be left in harsh environments. Inside the case is a mounted LCD screen that gives the user easy access to make changes in the field if necessary. The electronic components including the single board computer wireless cards are all mounted inside to protect them. The project also features battery packs so that it can run for up to 24 hours or longer depending on the monitoring task.

Data captured with the system can be stored on disk or be analyzed in real time thanks to the internally mounted LCD. Data can also be analyzed remotely by using one of the radios to connect to a nearby laptop. This can be useful in scenarios where the WiFi-Kraken Lite needs to be concealed. The form factor was chosen for not only its strength but also for being inconspicuous especially at conferences where lots of large polycarbonate cases can be seen.

Further data analysis can be performed in real time thanks to Kismet's fully featured web dashboard. Additionally post monitoring analysis can be performed using Wireshark or d4rkm4tter's PCAPinator tool which is a multithreaded wrapper around tshark to optimize queries on large datasets. The wireless data captured in this type of analysis can help to determine vulnerabilities which then you can use The WiFi-Kraken Lite to attack what you found.

This tool can be used entirely passively as a silent listener to validate bring your own device (BYOD) policies, monitor if wireless attacks are happening against your infrastructure, see if there are strange behaviors happening in your wireless network due to misconfiguration or maliciousness, or track devices as they moved throughout the networks so that you can have a better understanding of client flow. It can be used to perform a number of active attacks including impersonation, evil twin and other common wireless attacks.

It has never been more important to perform wireless assessments and continual monitoring of your infrastructure considering the number of wireless enabled devices increases daily. Rolling out new wireless infrastructure is costly and implementing the most secure system is daunting for even the most seasoned network integrators. This leads to misconfiguration and sub optimal security settings which are still connected to important infrastructure. For the defender this project brings clarity to the risks and also provides information into the most important mitigations that should be implemented. For the attacker this tool provides valuable recon that will allow them to focus solely on the vulnerable target making as little noise as possible all from it a single box.

Target Audience:
Offense, Defense and Hardware

By bringing equipment that can monitor the latest in wireless technologies, including WiFi 6, this project will shed light on a new and up and coming standard of technology that is slowly being rolled out across the world. With new technology, new tools are required so that research can be conducted to find flaws and validate the real world applications. The WiFi Kraken Lite will bring an enhanced perspective to the wireless monitoring in a box with new tools, new wireless bands captured, and new data processing.

This content will be presented on a Discord video channel.

#dl-video2-voice: https://discord.com/channels/708208267699945503/734027778646867988

Return to Index - Add to Google Calendar - ics Calendar file

Title: WiFi Kraken Lite
When: Saturday, Aug 7, 14:00 - 15:50 PDT
Where: Palace 3+4+5

SpeakerBio: Henry Hill
Henry Hill is an expert with computer hardware and is able to design and build the most bleeding edge systems that are the fastest in the world. His internal knowledge of architecture and system bottlenecks help him build systems capable of extreme processing and even faster storage. Henry is also an expert with mechanical engineering and fabrication. When his modifications aren't appearing in d4rkm4tter's projects, they can be seen in his race car at the track.

Description:

Tool or Project Name: The WiFi Kraken Lite

Short Abstract:
D4rkm4tter and Henry have been obsessed with monitoring wireless networks and have built hardware to meet the challenges of scanning and testing in the most busy and client dense environments. The WiFi-Kraken Lite contends with these issues in a smaller package without sacrificing any monitoring performance. This project is the results of years of research into the most effective way to scan and audit wireless in a single box that can be easily deployed or used as a hardened terminal in the most rugged conditions.

The WiFi-Kraken Lite consists of a single-board computer which connects 12 wireless radios that enables scanning and auditing WiFi, Bluetooth, LoRaWAN and other commonly used wireless protocols. The number of wireless devices is growing as well as the way those devices are being connected. Having an all-in-one wireless monitoring solution will give you the ability to track this data across these bands and give you the best picture of what's happening in the air around you.

This demonstration will provide you the information so that you can build your own all-in-one monitoring device. You will also gain an overview of capture technologies including Kismet that will help you perform this type of analysis in your own environments. Finally once the data is capture, you will get an understanding of efficient data processing using tools like Wireshark and d4rkm4tter's own PCAPinator tool.

Short Developer Bio:
Mike Spicer (d4rkm4tter) is a mad scientist hacker who likes to meddle with hardware and software. He is particularly obsessed with wireless. He has a degree in computer science which he has put to use building and breaking a wide array of systems. These include web application pentesting, wireless monitoring and tracking as well as reverse engineering. He is the creator of the #WiFiCactus and has been seen presenting and demoing at a number of conferences including DEF CON. He is a Kismet cultist and active in the wireless and wardriving communities.

Henry Hill is an expert with computer hardware and is able to design and build the most bleeding edge systems that are the fastest in the world. His internal knowledge of architecture and system bottlenecks help him build systems capable of extreme processing and even faster storage. Henry is also an expert with mechanical engineering and fabrication. When his modifications aren't appearing in d4rkm4tter's projects, they can be seen in his race car at the track.

URL to any additional information:
Palshack.org/wifi-kraken-lite (Site will be online for DEF CON)

Detailed Explanation of Tool:
The WiFi-Kraken Lite is a wireless monitoring system that is a rugged box with a single board computer and 12 wireless devices that are capable of simultaneously monitoring a large number of frequencies and protocols while storing that data in real time. The primary motivation for this project was to be able to gain visibility into as much of the wireless spectrum as possible in very congested networks in a small rugged form factor. Networks with a large number of clients that have a large number of access points can be difficult to perform analysis on. These networks typically have clients who switch between

networks and can switch frequencies lending to more confusion when tracking with only a single radio. By increasing the number of radios as well as adding support for other protocols beyond just WiFi, a more complete understanding of the wireless environment can be documented. This information can then be used for defenders or penetration testers to identify vulnerable networks, vulnerable clients, or verify security that can be easily documented and audited.

The hardware is set up so that it minimizes the number of bottlenecks between the actual frames in the air and when it writes the data to disk. It does this by taking advantage of the high-bandwidth PCI-express bus to connect wireless devices. From there the data transfers to a high-speed NVMe storage device. The operating system is Linux which allows us to take advantage of a number of open source tools and projects that help us capture the data. These projects include Kismet, BlueZ, btscanner, and Feather TFT LoRa Sniffer. Custom scripts help us manage and easily configure The WiFi-Kraken Lite for the desired mode.

The buildout of the project uses a hardened Pelican like case which provides the ruggedness and physical security so that the system can be left in harsh environments. Inside the case is a mounted LCD screen that gives the user easy access to make changes in the field if necessary. The electronic components including the single board computer wireless cards are all mounted inside to protect them. The project also features battery packs so that it can run for up to 24 hours or longer depending on the monitoring task.

Data captured with the system can be stored on disk or be analyzed in real time thanks to the internally mounted LCD. Data can also be analyzed remotely by using one of the radios to connect to a nearby laptop. This can be useful in scenarios where the WiFi-Kraken Lite needs to be concealed. The form factor was chosen for not only its strength but also for being inconspicuous especially at conferences where lots of large polycarbonate cases can be seen.

Further data analysis can be performed in real time thanks to Kismet's fully featured web dashboard. Additionally post monitoring analysis can be performed using Wireshark or d4rkm4tter's PCAPinator tool which is a multithreaded wrapper around tshark to optimize queries on large datasets. The wireless data captured in this type of analysis can help to determine vulnerabilities which then you can use The WiFi-Kraken Lite to attack what you found.

This tool can be used entirely passively as a silent listener to validate bring your own device (BYOD) policies, monitor if wireless attacks are happening against your infrastructure, see if there are strange behaviors happening in your wireless network due to misconfiguration or maliciousness, or track devices as they moved throughout the networks so that you can have a better understanding of client flow. It can be used to perform a number of active attacks including impersonation, evil twin and other common wireless attacks.

It has never been more important to perform wireless assessments and continual monitoring of your infrastructure considering the number of wireless enabled devices increases daily. Rolling out new wireless infrastructure is costly and implementing the most secure system is daunting for even the most seasoned network integrators. This leads to misconfiguration and sub optimal security settings which are still connected to important infrastructure. For the defender this project brings clarity to the risks and also provides information into the most important mitigations that should be implemented. For the attacker this tool provides valuable recon that will allow them to focus solely on the vulnerable target making as little noise as possible all from it a single box.

Target Audience:
Offense, Defense and Hardware

By bringing equipment that can monitor the latest in wireless technologies, including WiFi 6, this project will shed light on a new and up and coming standard of technology that is slowly being rolled out across the world. With new technology, new tools are required so that research can be conducted to find flaws and validate the real world applications. The WiFi Kraken Lite will bring an enhanced perspective to the wireless monitoring in a box with new tools, new wireless bands captured, and new data processing.

Return to Index - Add to Google Calendar - ics Calendar file

Title: WiFi Kraken Lite
When: Friday, Aug 6, 10:00 - 11:50 PDT
Where: Palace 3+4+5
Speakers: Mike Spicer,Henry Hill

SpeakerBio: Mike Spicer
Mike Spicer (d4rkm4tter) is a mad scientist hacker who likes to meddle with hardware and software. He is particularly obsessed with wireless. He has a degree in computer science which he has put to use building and breaking a wide array of systems. These include web application pentesting, wireless monitoring and tracking as well as reverse engineering. He is the creator of the #WiFiCactus and has been seen presenting and demoing at a number of conferences including DEF CON. He is a Kismet cultist and active in the wireless and wardriving communities.

SpeakerBio: Henry Hill
Henry Hill is an expert with computer hardware and is able to design and build the most bleeding edge systems that are the fastest in the world. His internal knowledge of architecture and system bottlenecks help him build systems capable of extreme processing and even faster storage. Henry is also an expert with mechanical engineering and fabrication. When his modifications aren't appearing in d4rkm4tter's projects, they can be seen in his race car at the track.

Description:
Tool or Project Name: The WiFi Kraken Lite

Short Abstract:
D4rkm4tter and Henry have been obsessed with monitoring wireless networks and have built hardware to meet the challenges of scanning and testing in the most busy and client dense environments. The WiFi-Kraken Lite contends with these issues in a smaller package without sacrificing any monitoring performance. This project is the results of years of research into the most effective way to scan and audit wireless in a single box that can be easily deployed or used as a hardened terminal in the most rugged conditions.

The WiFi-Kraken Lite consists of a single-board computer which connects 12 wireless radios that enables scanning and auditing WiFi, Bluetooth, LoRaWAN and other commonly used wireless protocols. The number of wireless devices is growing as well as the way those devices are being connected. Having an all-in-one wireless monitoring solution will give you the ability to track this data across these bands and give you the best picture of what's happening in the air around you.

This demonstration will provide you the information so that you can build your own all-in-one monitoring device. You will also gain an overview of capture technologies including Kismet that will help you perform this type of analysis in your own environments. Finally once the data is capture, you will get an understanding of efficient data processing using tools like Wireshark and d4rkm4tter's own PCAPinator tool.

Short Developer Bio:
Mike Spicer (d4rkm4tter) is a mad scientist hacker who likes to meddle with hardware and software. He is particularly obsessed with wireless. He has a degree in computer science which he has put to use building and breaking a wide array of systems. These include web application pentesting, wireless monitoring and tracking as well as reverse engineering. He is the creator of the #WiFiCactus and has been seen presenting and demoing at a number of conferences including DEF CON. He is a Kismet cultist and active in the wireless and wardriving communities.

Henry Hill is an expert with computer hardware and is able to design and build the most bleeding edge systems that are the fastest in the world. His internal knowledge of architecture and system bottlenecks help him build systems capable of extreme processing and even faster storage. Henry is also an expert with mechanical engineering and fabrication. When his modifications aren't appearing in d4rkm4tter's projects, they can be seen in his race car at the track.

URL to any additional information:
Palshack.org/wifi-kraken-lite (Site will be online for DEF CON)

Detailed Explanation of Tool:
The WiFi-Kraken Lite is a wireless monitoring system that is a rugged box with a single board computer and 12 wireless devices that are capable of simultaneously monitoring a large number of frequencies and protocols while storing that data in real time. The primary motivation for this project was to be able to gain visibility into as much of the wireless spectrum as possible in very congested networks in a small rugged form factor. Networks with a large number of clients that have a large number of access points can be difficult to perform analysis on. These networks typically have clients who switch between networks and can switch frequencies lending to more confusion when tracking with only a single radio. By increasing the number of radios as well as adding support for other protocols beyond just WiFi, a more complete understanding of the wireless environment can be documented. This information can then be used for defenders or penetration testers to identify vulnerable networks, vulnerable clients, or verify security that can be easily documented and audited.

The hardware is set up so that it minimizes the number of bottlenecks between the actual frames in the air and when it writes the data to disk. It does this by taking advantage of the high-bandwidth PCI-express bus to connect wireless devices. From there the data transfers to a high-speed NVMe storage device. The operating system is Linux which allows us to take advantage of a number of open source tools and projects that help us capture the data. These projects include Kismet, BlueZ, btscanner, and Feather TFT LoRa Sniffer. Custom scripts help us manage and easily configure The WiFi-Kraken Lite for the desired mode.

The buildout of the project uses a hardened Pelican like case which provides the ruggedness and physical security so that the system can be left in harsh environments. Inside the case is a mounted LCD screen that gives the user easy access to make changes in the field if necessary. The electronic components including the single board computer wireless cards are all mounted inside to protect them. The project also features battery packs so that it can run for up to 24 hours or longer depending on the monitoring task.

Data captured with the system can be stored on disk or be analyzed in real time thanks to the internally mounted LCD. Data can also be analyzed remotely by using one of the radios to connect to a nearby laptop. This can be useful in scenarios where the WiFi-Kraken Lite needs to be concealed. The form factor was chosen for not only its strength but also for being inconspicuous especially at conferences where lots of large polycarbonate cases can be seen.

Further data analysis can be performed in real time thanks to Kismet's fully featured web dashboard. Additionally post monitoring analysis can be performed using Wireshark or d4rkm4tter's PCAPinator tool which is a multithreaded wrapper around tshark to optimize queries on large datasets. The wireless data captured in this type of analysis can help to determine vulnerabilities which then you can use The WiFi-Kraken Lite to attack what you found.

This tool can be used entirely passively as a silent listener to validate bring your own device (BYOD) policies, monitor if wireless attacks are happening against your infrastructure, see if there are strange behaviors happening in your wireless network due to misconfiguration or maliciousness, or track devices as they moved throughout the networks so that you can have a better understanding of client flow. It can be used to perform a number of active attacks including impersonation, evil twin and other common wireless attacks.

It has never been more important to perform wireless assessments and continual monitoring of your infrastructure considering the number of wireless enabled devices increases daily. Rolling out new wireless infrastructure is costly and implementing the most secure system is daunting for even the most seasoned network integrators. This leads to misconfiguration and sub optimal security settings which are still connected to important infrastructure. For the defender this project brings clarity to the risks and also provides information into the most important mitigations that should be implemented. For the attacker this tool provides valuable recon that will allow them to focus solely on the vulnerable target making as little noise as possible all from it a single box.

Target Audience:
Offense, Defense and Hardware

By bringing equipment that can monitor the latest in wireless technologies, including WiFi 6, this project will shed light on a new and up and coming standard of technology that is slowly being rolled out across the world. With new technology, new tools are required so that research can be conducted to find flaws and validate the real world applications. The WiFi Kraken Lite will bring an enhanced perspective to the wireless monitoring in a box with new tools, new wireless bands captured, and new data processing.

Return to Index - Add to Google Calendar - ics Calendar file

BCV - Thursday - 21:00-20:59 PDT

Title: Will Secure Element Really Help Strengthen the Security of Cryptocurrency Wallets?
When: Thursday, Aug 5, 21:00 - 20:59 PDT
Where: Blockchain Village (YouTube)

SpeakerBio: Byeongcheol Yoo , Graduate Student
Byeongcheol Yoo is a master's student at the School of Cybersecurity in Korea University and his research areas focus on security engineering, blockchain, and IoT security.

In addition to being a master's student, he has been working as a senior researcher at Keypair Inc. which is a Korean company that specializes in blockchain and IoT security. He is a lead developer of an NFC-enabled card-type cryptocurrency wallet called 'KeyWallet Touch' in the company.

Description:

Cryptocurrency wallets are used to store the public and private keys of your account, keep track of the balance, conduct transactions in sending and receiving the currencies, as well as other functions with the blockchain. Wallets are divided into two types: software (a.k.a. hot) wallets and hardware (a.k.a. cold) wallets. Software wallets are accounts on cryptocurrency exchanges or accounts based on online websites. Hardware wallets are accounts stored on an offline means.

In this talk, we deal with a comparative analysis of all categories of these wallets. For this, first, we present a systematic method to evaluate the risk of cryptocurrency wallets, and then we review two hardware wallets ('Ledger Nano S' and 'Trezor One', both of which are the world's best-selling wallet) and four software wallets ('Bread', 'Trust Wallet' for mobile, and 'Copay', 'Electrum' for PC).

This talk is now available on YouTube: https://www.youtube.com/watch?v=bim4q1G3_c0

Return to Index - Add to Google Calendar - ics Calendar file

Title: Windows Forensics 101 (Beginner)
When: Friday, Aug 6, 10:45 - 12:15 PDT
Where: Blue Team Village - Workshop Track 2 (Virtual)

SpeakerBio: Surya Teja Masanam
Surya found his passion for cybersecurity during his college days where out of curiosity he figured out how a malware was spreading actively in the college computers and found a remediation technique. From then onwards his cybersecurity journey started. Digital Forensics and Malware Analysis are his all-time favorites. Surya is a Security Engineer with 5+ years of experience in performing both offensive and defensive activities. Engaging, understanding, and knowledgeable technical trainer, having expertise in training small and large groups across diverse industries. LinkedIn:
https://www.linkedin.com/in/suryatejam/
Twitter: @surya4n6
https://www.linkedin.com/in/suryatejam/

Description:
Are you fascinated with Sherlock Holmes stories?

In your lifetime, have you ever come across the word Forensics? Most of us might have seen in the movies like, After a crime, Police visits the crime scene and says “Call the Forensics Team”

Did you ever feel CURIOUS about that?

Technology is evolving, so are the attacks and investigation techniques.

If you are interested in Digital Forensics and have questions like:

How to start?
What skills are required?
What tools to use?
Then this workshop is the right place for you.

This intro-level workshop covers topics present in Digital Forensics LifeCycle like Evidence Collection and Investigation on a Windows machine, of a Windows machine. Attendees will be provided with the necessary lab instructions and evidence files to perform forensic analysis practically and be confident and clear on how to apply the knowledge gained here to investigate some real-world scenarios.

Attendees will learn:

Skills required for a Forensic Examiner Build their own forensics toolkit with free and open-source tools Evidence Collection --> On Live and Dead Machines, Do’s and Dont’s Investigation --> Windows Artifact analysis, Internet History & Application Analysis, Data Carving, Memory Analysis Opportunities and challenges in this field Attendees will be provided with:

Evidence Files
Lab instructions to perform forensic analysis Access to the Windows Forensics Artifact Library of the Speaker Useful resources for further practice and exploration after this workshop Lab Requirements:

OS: Windows 7 and above [Win10 recommended] If you are on Linux or Mac, Install Windows using VirtualBox RAM: Min. 4GB [8GB recommended]
Disk Space: 50 GB
Note: Download links for the labs will be shared before the workshop

Pre-requisites
- Familiarity with Windows Operating System. - Curiosity, Willingness, and of course, the Lab requirements too ;-)

Return to Index - Add to Google Calendar - ics Calendar file

WS - Friday - 15:00-18:59 PDT

Title: Windows Internals
When: Friday, Aug 6, 15:00 - 18:59 PDT
Where: Workshops - Jubilee 1 (Onsite Only)
Speakers: Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman

SpeakerBio: Sam Bowne , Proprietor, Bowne Consulting
Sam Bowne has been teaching computer networking and security classes at CCSF since 2000. He has given talks and hands-on trainings at DEF CON, DEF CON China, HOPE, BSidesSF, BSidesLV, RSA, and many conferences and colleges.

SpeakerBio: Elizabeth Biddlecome , Consultant and Part-Time Instructor
Elizabeth Biddlecome is a consultant and a part-time instructor at City College San Francisco, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

SpeakerBio: Irvin Lemus , Cybersecurity Professor
Irvin Lemus has been in the industry for 10+ years as an MSP technician, consultant, instructor and coordinator. He is currently the cybersecurity professor at Cabrillo College in Santa Cruz, CA. He also is the Bay Area Cyber Competitions Regional Coordinator as well as the contest creator for SkillsUSA CA and FL. Irvin has spoken at various cybersecurity and educational conferences. Irvin holds a CISSP and a Bachelor's Degree in Information Security.

Irvin Lemus is an instructor at Cabrillo College, teaching cyber security courses for 3 years. Irvin runs the cybersecurity competition program for the Bay Area Community Colleges. He also creates the SkillsUSA Cybersecurity contests for California and Florida. He has Security+, CySA+, WCNA, CISSP.

SpeakerBio: Kaitlyn Handelman , Hacker
I like to hack stuff, and I'm like really good at computers.

Description:
Explore the structure of Windows executable files and the operating system itself, to better understand programs, services, malware, and defenses. Projects include: cheating at games, building malicious DLL libraries, stealing passwords from the API, building a keylogger, and debugging a driver. Tools used include FLARE-VM, pestudio, API Monitor, Visual Studio, OllyDbg, IDA Pro, Ghidra, and WinDbg. No previous experience with programming is required.

To prepare for this workshop, please prepare a FLARE-VM in advance, as explained here:
https://samsclass.info/126/proj/PMA40.htm

Registration Link: https://www.eventbrite.com/e/windows-internals-jubilee-1-tickets-162217227093

Prerequisites
Previous experience troubleshooting Windows is helpful but not required

Materials needed:
A computer that can run virtual machines locally, or a few dollars to rent cloud servers

Return to Index - Add to Google Calendar - ics Calendar file

WS - Sunday - 10:00-13:59 PDT

Title: Windows Internals
When: Sunday, Aug 8, 10:00 - 13:59 PDT
Where: Workshops - Jubilee 1 (Onsite Only)
Speakers: Sam Bowne,Elizabeth Biddlecome,Irvin Lemus,Kaitlyn Handelman

SpeakerBio: Sam Bowne , Proprietor, Bowne Consulting
Sam Bowne has been teaching computer networking and security classes at CCSF since 2000. He has given talks and hands-on trainings at DEF CON, DEF CON China, HOPE, BSidesSF, BSidesLV, RSA, and many conferences and colleges.

SpeakerBio: Elizabeth Biddlecome , Consultant and Part-Time Instructor
Elizabeth Biddlecome is a consultant and a part-time instructor at City College San Francisco, delivering technical training and mentorship to students and professionals. She leverages her enthusiasm for architecture, security, and code to design and implement comprehensive information security solutions for business needs. Elizabeth enjoys wielding everything from soldering irons to scripting languages in cybersecurity competitions, hackathons, and CTFs.

SpeakerBio: Irvin Lemus , Cybersecurity Professor
Irvin Lemus has been in the industry for 10+ years as an MSP technician, consultant, instructor and coordinator. He is currently the cybersecurity professor at Cabrillo College in Santa Cruz, CA. He also is the Bay Area Cyber Competitions Regional Coordinator as well as the contest creator for SkillsUSA CA and FL. Irvin has spoken at various cybersecurity and educational conferences. Irvin holds a CISSP and a Bachelor's Degree in Information Security.

Irvin Lemus is an instructor at Cabrillo College, teaching cyber security courses for 3 years. Irvin runs the cybersecurity competition program for the Bay Area Community Colleges. He also creates the SkillsUSA Cybersecurity contests for California and Florida. He has Security+, CySA+, WCNA, CISSP.

SpeakerBio: Kaitlyn Handelman , Hacker
I like to hack stuff, and I’m like really good at computers.

Description:

Explore the structure of Windows executable files and the operating system itself, to better understand programs, services, malware, and defenses. Projects include: cheating at games, building malicious DLL libraries, stealing passwords from the API, building a keylogger, and debugging a driver. Tools used include FLARE-VM, pestudio, API Monitor, Visual Studio, OllyDbg, IDA Pro, Ghidra, and WinDbg. No previous experience with programming is required.

To prepare for this workshop, please prepare a FLARE-VM in advance, as explained here:
https://samsclass.info/126/proj/PMA40.htm

Registration Link: https://www.eventbrite.com/e/windows-internals-jubilee-1-tickets-162218647341

Prerequisites
Previous experience troubleshooting Windows is helpful but not required

Materials needed:
A computer that can run virtual machines locally, or a few dollars to rent cloud servers

Return to Index - Add to Google Calendar - ics Calendar file

CLV - Saturday - 10:45-11:30 PDT

Title: Windows Server Containers are Broken - Here's How You Can Break Out

When: Saturday, Aug 7, 10:45 - 11:30 PDT

Where: Cloud Village (Virtual)

SpeakerBio: Daniel Prizmant

Daniel started out his career developing hacks for video games and soon became a professional in the information security field. He is an expert in anything related to reverse engineering, vulnerability research and the development of fuzzers and other research tools. To this day Daniel is passionate about reverse engineering video games at his leisure. Before joining Palo Alto Networks Daniel was employed at CheckPoint, KayHut and Nyotron. Daniel holds a Bachelor of Computer Science from Ben Gurion University.
Twitter: @pushrsp

Description:

A container packages up code and its dependencies, creating a minimal computing environment that can be cloned quickly and reliably across the ever-changing variety of operating system distributions. Originally available for Linux alone, containerized software will always run the same, regardless of the infrastructure. Microsoft teamed up with Docker to offer a container solution for Windows. Support for containers was added in 2016, but little documentation on the internal implementation was released. It was necessary to reverse engineer some of the components of Windows in order to better understand the kernel implementation. How does Windows prevent containers from running system calls that may allow attackers to escape containers? How does Windows prevent containers from accessing sensitive files outside the container, on the host? Why go through all this trouble? A vulnerability in the low level implementation of containers could impact hundreds of thousands of affected instances. Not to mention a full escape from the container to its host machine. How would such an escape vulnerability affect Kuberenetes and Azure services? In this presentation I will show you how to fully escape a Windows container and gain full access to the host’s file system. I will discuss why Microsoft originally didn’t consider this a vulnerability, but do now. I will also show the use of this vulnerability in the wild by a malware.

Cloud Village activities will be streamed to YouTube.

YouTube: https://www.youtube.com/cloudvillage_dc

Return to Index - Add to Google Calendar - ics Calendar file

VMV - Friday - 11:30-11:59 PDT

Title: Wireless Odyssey or why is the federal government permitting devices with wireless networking capability in federally certified voting machines?

When: Friday, Aug 6, 11:30 - 11:59 PDT

Where: Voting Village (Talks - Virtual)

SpeakerBio: Susan Greenhalgh

Susan Greenhalgh is the Senior Advisor on Election Security for Free Speech For People. Ms. Greenhalgh has previously served as vice president of programs at Verified Voting and at the National Election Defense Coalition, advocating for secure election protocols, paper ballot voting systems and post-election audits. Recognized as an expert on election security, she has been invited to testify before the U.S. Commission on Civil Rights and has been an invited speaker at meetings of the MITRE Corporation, the National Conference of State Legislatures, the Mid-West Election Officials Conference, the International Association of Government Officials, the Election Verification Network and the E-Vote-ID conference in Bregenz, Austria. She is a frequent source for reporters from The New York Times, The Washington Post, The Wall Street Journal, Politico, USA Today, Associated Press, National Public Radio and other leading news outlets. She has appeared on CNN and MSNBC's The Rachel Maddow Show, and various other television news shows. She has a BA in Chemistry from the University of Vermont.

Description:

In February, the U.S. Election Assistance Commission (EAC) passed new voting system standards, the federal voluntary voting system guidelines or VVSG 2.0. The new guidelines that were presented to the EAC, voted on, and adopted, had a significant change in them from the guidelines that had gone through the federally mandated public hearing and comment period. The new standards, that had not been vetted publicly, suddenly allowed the inclusion of wireless networking devices like modems, chips or radios.

This presentation aims to tell the story of how the computer security community successfully advocated for the federal voting system standards to ban all wireless networking capability in federally certified voting systems, only to have the EAC change the publicly vetted version of the standards, in secret, behind closed doors, at the eleventh hour, at the request of the voting system vendors, to allow wireless devices.

Voting Village talks will be streamed to YouTube and Twitch.

Twitch: https://www.twitch.tv/votingvillagedc

YouTube: https://www.youtube.com/channel/UCnDevqsxt3sO8chqS5MGvwg

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Saturday - 09:00-10:30 PDT

Title: Wireshark for Incident Response & Threat Hunting
When: Saturday, Aug 7, 09:00 - 10:30 PDT
Where: Blue Team Village - Workshop Track 1 (Virtual)

SpeakerBio: Michael Wylie
Michael Wylie, MBA, CISSP is the Sr. Manager of a 24/7/365 global managed threat hunting team. Prior to his current role, he was the Director of Cybersecurity at a top 100 CPA firm where he built out the offensive/defensive security service practice. Michael has developed and taught numerous courses for the U.S. Department of Defense, DEFCON, Colleges, and for clients around the world. Michael is the winner of numerous SANS challenge coin and holds the following credentials: CISSP, CCNA R&S, GPEN, GMON, GCFE, TPN, CEH, CEI, VCP-DCV, CHPA, PenTest+, CNVP, Microsoft Azure, and more.
Twitter: @themikewylie

Description:
This workshop will take student's Wireshark skills to the next level with a heavy emphasis on incident response, threat hunting, and malicious network traffic analysis. We will begin with a brief introduction to Wireshark and other Network Security Monitoring (NSM) tools/concepts. Placement, techniques, and collection of network traffic will be discussed in detail.

This workshop will take student's Wireshark skills to the next level with a heavy emphasis on incident response, threat hunting, and malicious network traffic analysis. We will begin with a brief introduction to Wireshark and other Network Security Monitoring (NSM) tools/concepts. Placement, techniques, and collection of network traffic will be discussed in detail. Throughout the workshop, we'll examine what different attacks and malware look like in Wireshark. Students will then have hands-on time in the lab to search for Indicators of Compromise (IOCs) and a potential breach to the network. There will be plenty of take home labs for additional practice.

Attendees will learn:
- How to build traffic specific Wireshark profiles - How to setup Wireshark for threat hunting - How to enrich packets with threat intel - How to identify IOCs in a sea of packets - How to tap networks and where to setup sensors - NSM techniques - Techniques to quickly identify evil on a network

Students are provided with PCAPs of incidents starting with 8 packets and growing to 10,000+ packet captures where students need to build a timeline of a breach.

Return to Index - Add to Google Calendar - ics Calendar file

CPV - Saturday - 10:00-17:30 PDT

Title: Workshop & CTF: Practical Cryptographic Attacks
When: Saturday, Aug 7, 10:00 - 17:30 PDT
Where: See Description

SpeakerBio: Daniel Crowley
Daniel Crowley is the head of research and a penetration tester for X-Force Red. Daniel denies all allegations regarding unicorn smuggling and questions your character for even suggesting it. Daniel is the primary author of both the Magical Code Injection Rainbow, a configurable vulnerability testbed, and FeatherDuster, an automated cryptanalysis tool. Daniel enjoys climbing large rocks and is TIME magazine's 2006 person of the year. Daniel has been working in the information security industry since 2004 and is a frequent speaker at conferences including Black Hat, DEF CON, Shmoocon, and SOURCE. Daniel does his own charcuterie and brews his own beer. Daniel's work has been included in books and college courses. Daniel also holds the noble title of Baron in the micronation of Sealand.

Description:
While new cryptographic attacks are regularly published, there are a series of common, practically exploitable mistakes that have been made by application developers at both large and small companies for years when using cryptography. For example, using a hard-coded IV (a common mistake) led to the flaw known as Zerologon, exploiting Microsoft's Netlogon protocol to allow pre-auth domain compromise in 2020. This workshop will provide a working knowledge of cryptography for those unfamiliar, and explain a series of practical attacks against cryptographic mistakes that are common in production systems today, accompanied by practical challenges in the form of a CTF.

CTF URL: https://crypto.iscool.af/
Python3 module for crypto exploit writing: https://github.com/unicornsasfuel/cryptanalib3.

Recommended for rapid exploit writing: pwntools -- install docs at: https://docs.pwntools.com/en/stable/install.html

This talk will be streamed at https://www.twitch.tv/DrSensualPotatoPhD

Return to Index - Add to Google Calendar - ics Calendar file

AIV - Friday - 15:30-16:30 PDT

Title: Workshop on Microsoft Counterfit
When: Friday, Aug 6, 15:30 - 16:30 PDT
Where: AI Village (Virtual)

SpeakerBio: Will Pearce
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

Title: Workshop: Practically Protecting Phone Privacy (Pre-registration required)
When: Sunday, Aug 8, 10:00 - 13:59 PDT
Where: See Description
Speakers: Mauricio Tavares,Matt Nash

SpeakerBio: Mauricio Tavares
Mauricio has worked in the credit card and medical industry, which led to an interest in the behavioral aspect of data security and privacy. He has published in topics ranging from aerospace engineering to computer automation and data privacy. Currently, he is the senior security engineer of some multinational research project or another, helping craft the policies and procedures and advise IT staff to effectively protect it, shiny thingies, and laser pointers. And maybe user and data privacy in the process.

He only knows two facts about geese, both of which are wrong.

SpeakerBio: Matt Nash
Matt Nash breaks things (sometimes intentionally)

As a security consultant, Matt works in a variety of realms, including: internal/external network infrastructure, cloud environments, web applications, automated teller machines (ATMs), physical security, social engineering, digital forensics and incident response, mobile, and wireless. As well, these assessments span a number of sectors: energy, utility, manufacturing, software development, financial, retail, municipal, and medical.

Matt holds a B.S. in Food and Resource Economics, and is therefore totally qualified to speak on the tasty topics of security and privacy.

Description:

This workshop will be held on Zoom. Join here:
https://unc.zoom.us/j/9853325800?pwd=WTlDYlRPM1ZTUEtkOG5uelc5Rk5Ddz09 Meeting ID: 985 332 5800
Passcode: 800855

Your phone is a little snitch. For as long as it is turned on, it is monitoring your activities (physical and digital). It knows where you go, who else may be around, and likely what you are doing. Further, it shares (at least some of) the information with different organizations - which then sell or directly aggregate the data to profile you for fun and profit. The modern phone compromises your privacy by design.

To add insult to injury, you do not have a say on it. Or do you?

If you're willing to put in some effort, you can do something about it. But, it will require more than just installing some app with a big Easy Button. If we can do it, so can you!

Takeaways

Attendees will come out of this workshop with a privacy mindset:

- Appreciating the privacy and security implications of using a smart phone in general -- specifically consumer Android devices.
- Knowing how to achieve two different levels privacy in their phones and understanding the costs and benefits of each approach.
- Understanding what "attribution of traffic" tying IP to a person through a VPN is.

- Finding out which apps are privacy-respecting, and how to contain those untrusted apps you need to have

Who should take this workshop:

- Privacy-conscious smartphone users who would like to understand and control what their mobile devices share about them.

Audience Skill Level:

Beginner/Intermediate

Attendees' requirements:

- An understanding of basic Linux commands
- Comfortable with the idea of installing an aftermarket firmware/OS ("ROM") on a mobile device. Soft/hard "bricking" is a possibility, so having a spare phone may be a good investment.

What student should bring:

- A phone that has support for the latest version of LineageOS - as of this writing, 18.1 (Android 11). It does not need to be the "latest and greatest", most expensive flagship device. In fact, we will compare and contrast the effectiveness and viability of higher-end and inexpensive models. We will not cover iPhones or other Apple products here.

INSTRUCTIONS

https://github.com/matthewnash/building-phone-privacy

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 12:30-12:50 PDT

Title: Worming through IDEs
When: Friday, Aug 6, 12:30 - 12:50 PDT
Where: DCTV/Twitch #3 Pre-Recorded

SpeakerBio: David Dworken
David is a bug bounty hunter turned software engineer turned security engineer. He started in security in high school hacking on bug bounties and then spent four years learning how to be an effective software engineer. He's worked on five different product security teams ranging from startups to large corporations. He previously published a research paper on tracking malicious proxies in ACSAC. Currently, he works as a security engineer at Google working on deploying an alphabet soup of security headers across hundreds of services.
Twitter: @ddworken
daviddworken.com

Description:
You might think that as long as you never hit run, opening up that interesting new POC in your IDE and checking out the code is safe. But it isn't. IDEs and developer tools are complex pieces of software that have vulnerabilities, just like everything else.

We'll start by discussing what a reasonable threat model is for IDEs. How do companies threat model their IDEs? What do users expect of their IDEs? Is viewing a file equivalent to executing it?

Then we'll dive into the reality of it. Nearly every IDE examined was trivially vulnerable. But there were also a variety of subtle bugs lying underneath. We'll look at bugs in both local IDEs (like VSCode and IntelliJ) and cloud-based IDEs (like AWS Cloud9 and Github Codespaces).

Finally, we'll show how an attacker could make a worm that would spread through attacking IDEs. View a malicious project? Let's automatically backdoor every project on a computer and keep spreading.

REFERENCES

https://github.com/numirias/security/blob/master/doc/2019-06-04_ace-vim-neovim.md
https://nvd.nist.gov/vuln/detail/CVE-2012-3479
http://blog.saynotolinux.com/blog/2016/08/15/jetbrains-ide-remote-code-execution-and-local-file-disclosure-vulnerability-
https://www.cvedetails.com/vulnerability-list/vendor_id-15146/product_id-49160/year-2019/Jetbrains-Intellij-Idea.html

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=pzqu_qaoNuY

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20D

This talk has been pre-recorded and will be released to the DEF CON Media Server, torrents, and YouTube. At the time of this event, it will also stream on DCTV3, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_three

AIV - Sunday - 13:00-13:59 PDT

Title: Wrap Up
When: Sunday, Aug 8, 13:00 - 13:59 PDT
Where: AI Village (Virtual)

SpeakerBio:AI Village Organizers
No BIO available

Description: No Description available

AI Village events will be streamed to Twitch, and later be made available as videos on YouTube.

Speakers will be made available on DEF CON's Discord, in #aiv-general-text.

Twitch: https://www.twitch.tv/aivillage

YouTube: https://www.youtube.com/c/aivillage

#aiv-general-text: https://discord.com/channels/708208267699945503/732733090568339536

Return to Index - Add to Google Calendar - ics Calendar file

WS - Friday - 15:00-18:59 PDT

Title: Writing Golang Malware
When: Friday, Aug 6, 15:00 - 18:59 PDT
Where: Workshops - Las Vegas 5+6 (Onsite Only)

SpeakerBio: Benjamin Kurtz , Hacker
Ben Kurtz is a hacker, a hardware enthusiast, and the host of the Hack the Planet podcast (https://symbolcrash.com/podcast). After his first talk, at DefCon 13, he ditched development and started a long career in security. He has been a pentester for IOActive, head of security for an MMO company, and on the internal pentest team for the Xbox One at Microsoft. Along the way, he volunteered on anti-censorship projects, which resulted in his conversion to Golang and the development of the ratnet project (https://github.com/awgh/ratnet). A few years ago, he co-founded the Binject group to develop core offensive components for Golang-based malware, and Symbol Crash, which focuses on sharing hacker knowledge through trainings for red teams, a free monthly Hardware Hacking workshop in Seattle, and podcasts. He is currently developing a ratnet-based handheld device for mobile encrypted mesh messenging, planned for release next year.
Twitter: @symbolcrash1
symbolcrash.com

Description:
Participants will learn how to design and build their own multi-platform Golang-based implants and c2 frameworks by building on samples provided.

Topics will include:

- Communication between the implant and the command and control system including encrypted darknets with pluggable transports, covert exfiltration methods, detection evasion, and fault tolerant infrastructure design.
- Binary transformation techniques designed to allow offensive practitioners the freedom of writing conventional binaries, yet maintaining the mobility of shellcode-like operating conditions.
- Parsing and rewriting all binary formats to inject shellcode using a variety of reconfigurable methods.
- On-the-wire modification of binaries and archives from a man-in-the-middle or malicious server perspective.
- Methods of avoiding EDR with your implant, including loading modules direct from the c2 to memory without touching disk (on all platforms), customizable encrypting packers, and direct system calls/DLL unhooking (on Windows).

Registration Link: https://www.eventbrite.com/e/writing-golang-malware-las-vegas-5-6-tickets-162217403621

Prerequisites
Programming experience required, some experience with Golang would be helpful.

Materials needed:
Laptop (any operating system)

Return to Index - Add to Google Calendar - ics Calendar file

BTV - Sunday - 12:30-12:59 PDT

Title: Year of Mentoring: BTV’s Meet-a-Mentor Turns One
When: Sunday, Aug 8, 12:30 - 12:59 PDT
Where: Blue Team Village - Main Track (Virtual)

SpeakerBio:muteki
muteki is the Meet-a-Mentor Lead as well as a director of Blue Team Village, a not-for-profit organization bringing free Blue Team talks, workshops and more to the broader InfoSec community.

Description:
Blue Team Village's Meet-a-Mentor program turns 1 year old at DEF CON 29! Join us as we share all the work we've done and what we've learned in the past year, and also listen to three mentor-mentee matches share their experiences with us.

Visit https://www.blueteamvillage.org/meet-a-mentor/ for more info on the program.

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

Title: Yeet the leet with Osquery (Effective Threathunting Without Breaking Bank)

When: Friday, Aug 6, 09:30 - 10:30 PDT

Where: Blue Team Village - Main Track (Virtual)

SpeakerBio: Sebastiaan Provost

Sebastiaan is the Lead Security Engineer at Beacon and has worked in information security for across both offensive and defensive domains. He specializes in protecting business critical assets by applying technology in creative ways and is particularly interested in Threat Hunting in Zero Trust Environments. In his free time, he enjoys the gym, he tries to hone his infosec knives, and tries to visit as many countries as possible. He has previously given talks at SHA2017 and BsidesNCL 2019.
Twitter: @Stekkz

Description:

EDR/MDR/XDR is touted as the panacea, a one-stop-shop of security. However, there is no certainty on how well those solutions protect us. Companies throw money at them because they get promised complete protection. EDR solutions, no matter how expensive, still miss common techniques and payloads. This talk will show the audience how they can use the power of OSQuery to add additional monitoring to their systems in addition to keeping their EDR solutions honest. The talk will focus on detections of common command & control (C2) frameworks using OSQuery in addition to EDR.

What will be learned throughout the talk: - What is Osquery
- How to detect potential IOCs with Osquery - How to detect C2 payloads with Osquery - How to detect reverse shells with Osquery - How to combine this with a good alerting setup for the chance of a quick intervention - Potential automation past the alerting

Description/Flow
1. Intro
I will introduce myself, talk about my background, what I do and what my motivation is for this talk. I will also explain what can be expected and give a quick overview of the journey that we will follow. 2. Osquery & Why it was chosen
Osquery has been around for a few years now. It is a piece of software that allows you to describe anything related to a device with simple SQL commands that leverage a relational data-model. A short intro will be given about what it actually does, what its capabilities are, who is behind it, and what it can be used for. This will be followed up by a list of examples to show the power of osquery, to give the audience an initial view on how far you can go with it. Lastly, I will use a few examples that will show how you can use the power of osquery to detect potential IOCs.

Payloads and Reverse Shells
C2 Payloads
In this part I will take the audience on a journey of hunting for C2 payloads & processes. I will go over a few off-the-shelf C2 frameworks that can be found on Github, what kind of payloads they provide and how easy/difficult it is to set them up. From there I will show the audience how we can catch the payloads/processes of these C2 frameworks with a few SQL queries in Osquery. Reverse Shells
In this part I will guide the audience through a series of examples on how reverse shells can be launched and how their connections can be detected. From there I will show the audience how we can catch those connections and reverse shells with a few simple SQL queries. Alerting
After I’ve shown the audience what the capabilities are of Osquery, how you can use it to hunt for C2 payloads/processes and for reverse shells, I will guide them on how this can be combined with alerting so analysts can react quickly if something has been found by Osquery. I will use both Splunk and Elasticsearch as an example on how this alerting can look like and will speak a little bit on how we can automate this even more with SOAR platforms. Sitrep
During the sitrep, I will talk briefly about the technologies we’ve encountered. I will also give a brief overview of the things we’ve learned looking back and how this can be extended even more looking forward. The end
This is the part where I would like to thank everyone for listening in and I will happily answer any question that comes my way!

Blue Team Village talks will be streamed to Twitch.

--

Twitch: https://twitch.tv/blueteamvillage

Return to Index - Add to Google Calendar - ics Calendar file

IOTV - Saturday - 11:00-11:45 PDT

Title: You're Doing IoT RNG
When: Saturday, Aug 7, 11:00 - 11:45 PDT
Where: IoT Village (Talk - Virtual)
Speakers: Allan Cecil - dwangoAC,Dan Petro - AltF4

SpeakerBio: Allan Cecil - dwangoAC
Allan Cecil (dwangoAC) is a Security Consultant with Bishop Fox and the President of the North Bay Linux User’s Group. He acts as an ambassador for Tasvideos.org, a website devoted to using emulators to complete video games as quickly as the hardware allows. He participates in Games Done Quick charity speed running marathons using TASBot to entertain viewers with never-before-seen glitches in games.
Twitter: @mrtasbot

SpeakerBio: Dan Petro - AltF4
Dan "AltF4" Petro is Lead Researcher at Bishop Fox. Dan is widely known for the tools he creates: Eyeballer (a convolutional neural network pentest tool), the Rickmote Controller (a Chromecast-hacking device), Untwister (pseudorandom number generator cracker), and SmashBot (a merciless Smash Bros noob-pwning machine).
Twitter: @2600AltF4

Description:
Think of a random number between '0' and infinity. Was your number '0'? Seriously? Crap. Well unfortunately, the hardware random number generators (RNG) used by your favorite IoT devices to create encryption keys may not work much better than you when it comes to randomness.

In this talk, we'll delve into murky design specs, opaque software libraries, and lots of empirical results. We wrote code for many popular IoT SoC platforms to extract gigabytes of data from their hardware RNGs and analyze them. What we found was a systemic minefield of vulnerabilities in almost every platform that could undermine IoT security. Something needs to change in how the Internet of Things does RNG.

The vulnerabilities are widespread and the attacks are practical. RNG is bad out there - "IoT Crypto-pocalypse" bad.

IoT Village talks will be streamed to Twitch. Select speakers may be available in the IoT Village on-site to answer questions.

Twitch: https://www.twitch.tv/iotvillage

Return to Index - Add to Google Calendar - ics Calendar file

DC - Saturday - 17:00-17:45 PDT

Title: You're Doing IoT RNG

When: Saturday, Aug 7, 17:00 - 17:45 PDT

Where: Track 1 Live; DCTV/Twitch #1 Pre-Recorded

Speakers: Allan Cecil - dwangoAC,Dan Petro - AltF4

SpeakerBio: Allan Cecil - dwangoAC
Allan Cecil (dwangoAC) is a Security Consultant with Bishop Fox and the President of the North Bay Linux User’s Group. He acts as an ambassador for Tasvideos.org, a website devoted to using emulators to complete video games as quickly as the hardware allows. He participates in Games Done Quick charity speed running marathons using TASBot to entertain viewers with never-before-seen glitches in games.
Twitter: @mrtasbot

SpeakerBio: Dan Petro - AltF4
Dan "AltF4" Petro is Lead Researcher at Bishop Fox. Dan is widely known for the tools he creates: Eyeballer (a convolutional neural network pentest tool), the Rickmote Controller (a Chromecast-hacking device), Untwister (pseudorandom number generator cracker), and SmashBot (a merciless Smash Bros noob-pwning machine).
Twitter: @2600AltF4

Description:
Think of a random number between '0' and infinity. Was your number '0'? Seriously? Crap. Well unfortunately, the hardware random number generators (RNG) used by your favorite IoT devices to create encryption keys may not work much better than you when it comes to randomness. In this talk, we'll delve into murky design specs, opaque software libraries, and lots of empirical results. We wrote code for many popular IoT SoC platforms to extract gigabytes of data from their hardware RNGs and analyze them. What we found was a systemic minefield of vulnerabilities in almost every platform that could undermine IoT security. Something needs to change in how the Internet of Things does RNG. The vulnerabilities are widespread and the attacks are practical. RNG is bad out there - "IoT Crypto-pocalypse" bad.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=Zuqw0-jZh9Y

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20D

This talk will be given live in Track 1.

This talk has also been pre-recorded and will be broadcast on DCTV1, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_one

Return to Index - Add to Google Calendar - ics Calendar file

DC - Friday - 12:00-12:20 PDT

Title: Your House is My House: Use of Offensive Enclaves In Adversarial Operations
When: Friday, Aug 6, 12:00 - 12:20 PDT
Where: Track 2 Live; DCTV/Twitch #2 Pre-Recorded

SpeakerBio: Dimitry "Op_Nomad" Snezhkov
Dimitry Snezhkov is an Associate Director at Protiviti. In this role he hacks code, tools, networks, apps and sometimes subverts human behavior too. Dimitry has spoken at DEF CON, BlackHat, THOTCON conferences, and presented tools at BlackHat Arsenal.
Twitter: @Op_Nomad

Description:
As developers start to rely more on hardware-based memory encryption controls that isolate specific application code and data in memory - secure enclaves, adversaries can use enclaves to successfully coexist on the host and enjoy similar protections.

In this talk we venture into a practical implementation of such an offensive enclave, with the help of Intel SGX enclave technology, supported on a wide variety of processors present in enterprise data-centers and in the cloud.

We discuss how malware can avoid detection in defensively instrumented environments and protect their operational components from processes running at high privilege levels, including the Operating System. We dive deeper into using enclaves in implants and stagers, and discuss the design and implementation of an enclave that is capable of facilitating secure communication and storage of sensitive data in offensive operations. We cover how the enclaves can be built to help secure external communication while resisting system and network inspection efforts and to achieve deployment with minimal dependencies where possible.

Finally, we release the enclave code and a library of offensive enclave primitives as a useful reference for teams that leverage Intel SGX technology or have the hardware platform capable to support such adversarial efforts.

--

This talk has been released to YouTube and the DEF CON Media server.

YouTube: https://www.youtube.com/watch?v=WWGkaGBtn2Q

Media:
https://media.defcon.org/DEF%20CON%2029/DEF%20CON%2029%20video%20and%20slides/DEF%20CON%2029%20-%20D

This talk will be given live in Track 2.

This talk has also been pre-recorded and will be broadcast on DCTV2, both in local hotels and on Twitch.

DCTV Channel Map: https://dctv.defcon.org/

Twitch: https://www.twitch.tv/defcon_dctv_two

Return to Index - Add to Google Calendar - ics Calendar file

ICSV - Friday - 11:30-12:30 PDT

Title: Your Infrastructure is Encrypted: Protecting Critical Infrastructure from Ransomware
When: Friday, Aug 6, 11:30 - 12:30 PDT
Where: ICS Village (Virtual)
Speakers: David Etue,Ernie Bio,Jamil Jaffer,Jennifer DeTrani

SpeakerBio: David Etue
No BIO available

SpeakerBio: Ernie Bio
No BIO available

SpeakerBio: Jamil Jaffer , National Security Institute
Jamil currently serves as Founder and Executive Director of the National Security Institute and as an Assistant Professor of Law and Director of the National Security Law & Policy Program at the Antonin Scalia Law School at George Mason University. He also currently serves as Vice President for Strategy, Partnerships & Corporate Development at IronNet Cybersecurity, a startup technology firm founded by former NSA Director Gen. (ret.) Keith B. Alexander. Jamil also serves on the Board of Directors for the Greater Washington Board of Trade, is a member of the Board's Smart Region Movement Strategic Advisory Counsel, and is a co-chair of the SRM's Cyber, Data Management, and Privacy Solution Group. Jamil is also an advisor to Beacon Global Strategies, a strategic advisory firm specializing in international policy, defense, cyber, intelligence, and homeland security; 4iQ, a technology startup focused on deep and dark web intelligence and identity theft protection; Duco, a technology platform startup that connects corporations with geopolitical and international business experts; and Amber, a digital authentication and verification startup.
Twitter: @Jamil_n_jaffer

SpeakerBio: Jennifer DeTrani
No BIO available

Description:

The recent attacks against Colonial Pipeline, JBS, and others have made it clear just how vulnerable U.S. Critical Infrastructure is to ransomware. While these attacks have been grabbing headlines, the path forward has not. A variety of tools and approaches will need to be tested by both the government and private sector to push back against the threat of ransomware and protect critical infrastructure from future attacks.

This panel brings together a variety of perspectives from the government, technology, and venture capital sectors to chart the path forward and detail what steps government and the private sector can take individually and together to protect critical infrastructure across the country.

ICS Village will be releasing their events to YouTube at each event's scheduled time. Discussion will be available on Discord in #ics-speaker-questions-and-answers-text.

YouTube: https://www.youtube.com/channel/UCI_GT2-OMrsqqglv0JijHhw

#ics-speaker-questions-and-answers-text: https://discord.com/channels/708208267699945503/735937961908109485

Return to Index - Add to Google Calendar - ics Calendar file

Title: Zuthaka
When: Friday, Aug 6, 14:00 - 15:50 PDT
Where: DemoLab Video Channel 2

SpeakerBio: Lucas Bonastre
Lucas started his career studying Mathematics at the University of Buenos Aires, however when his uncle gave him a C++ book, he realized his true passion for programming and his outstanding ability for problem-solving. He worked across cybersecurity and technology firms and is a vetted developer in many languages such as C/C++, Python, Java, and PHP. Now he is a full time developer and security researcher at Pucara Information Security. In his spare time, he is an expert chess player and he is studying AI to analyze foosball strategies.

Description:
Tool or Project Name: Zuthaka

Short Abstract:
A collaborative free open-source Command & Control development framework that allows developers to concentrate on the core function and goal of their C2. Zuthaka presents a simplified API for fast and clear integration of C2s and provides a centralized management for multiple C2 instances through a unified interface for Red Team operations.

Short Developer Bio:
Lucas started his career studying Mathematics at the University of Buenos Aires, however when his uncle gave him a C++ book, he realized his true passion for programming and his outstanding ability for problem-solving. He worked across cybersecurity and technology firms and is a vetted developer in many languages such as C/C++, Python, Java, and PHP. Now he is a full time developer and security researcher at Pucara Information Security. In his spare time, he is an expert chess player and he is studying AI to analyze foosball strategies.

URL to any additional information:
https://docs.zuthaka.com/-MYVExFNbaf2ARSR5z2e/

Detailed Explanation of Tool:

Problem Statement: The current C2s ecosystem has rapidly grown in order to adapt to modern red team operations and diverse needs (further information on C2 selection can be found here). This comes with a lot of overhead work for Offensive Security professionals everywhere. Creating a C2 is already a demanding task, and most C2s available lack an intuitive and easy to use web interface. Most Red Teams must independently administer and understand each C2 in their infrastructure.

Solution: With the belief that community efforts surpass that of any individual, Zuthaka presents a simplified API for fast and clear integration of C2s and provides a centralized management for multiple C2 instances through a unified interface for Red Team operations.

Zuthaka is more than just a collection of C2s, it is also a solid foundation that can be built upon and easily customized to meet the needs of the exercise that needs to be accomplish. This integration and development framework for C2 allows developers to concentrate on a unique target environment and not have to reinvent the wheel.

Please reefer to the supporting files for more detailed information about Zuthaka.

Supporting Files, Code, etc:
Docs : https://docs.zuthaka.com/-MYVExFNbaf2ARSR5z2e/ Github : https://github.com/pucarasec/zuthaka Demo Video: https://youtu.be/pcW9Hj5Jzu0 Target Audience:
Offensive developers, Red Teamers Operators, C2 Developers

Problem Statement:
The current C2s ecosystem has rapidly grown in order to adapt to modern red team operations and diverse needs (further information on C2 selection can be found here). This comes with a lot of overhead work for Offensive Security professionals everywhere. Creating a C2 is already a demanding task, and most C2s available lack an intuitive and easy to use web interface. Most Red Teams must independently administer and understand each C2 in their infrastructure.

Solutions: With the belief that community efforts surpass that of any individual, Zuthaka presents a simplified API for fast and clear integration of C2s and provides a centralized management for multiple C2 instances through a unified interface for Red Team operations.

Zuthaka is more than just a collection of C2s, it is also a solid foundation that can be built upon and easily customized to meet the needs of the exercise that needs to be accomplish. This integration and development framework for C2 allows developers to concentrate on a unique target environment and not have to reinvent the wheel.

Additional information:
The github repository is private ,until the release of the tool, but we can provide an early access to the repository for the reviewers. All the information is available on: https://docs.zuthaka.com/-MYVExFNbaf2ARSR5z2e/

This content will be presented on a Discord video channel.

#dl-video2-voice: https://discord.com/channels/708208267699945503/734027778646867988

Return to Index - Add to Google Calendar - ics Calendar file

DEF CON 29 Press roundup!

Posted 8.8.21

We're on the last day of DEF CON 29, both in the virtual and physical worlds. There's so much going on it's easy to miss a few things. Here's a brief listing of some of the press coverage of our events this year.

AND!XOR’s DEF CON 29 Electronic Badge Is An Assembly Puzzle
Hackaday

Hands On: DEF CON 29 Badge Embraces The New Normal
Hackaday

Black Hat USA 2021 and DEF CON 29: What to expect from the security events
Tech Republic

Privacy Without Monopoly: DEFCON 29
EFF

We Have Questions for DEF CON's Puzzling Keynote Speaker, DHS Secretary Mayorkas
EFF

Hands-On: Whiskey Pirates DC29 Hardware Badge Blings With RISC-V
Hackaday

#DEFCON: Hacking RFID Attendance Systems with a Time Turner
infosecurity

#DEFCON: Why Social Media Security is Election Security
infosecurity

#DEFCON: A Bad eBook Can Take Over Your Kindle (or Worse) infosecurity

#DEFCON: Ransomware Moves from Nuisance to Scourge
infosecurity

Black Hat USA 2021 & DefCon 29: Hybride IT-Security-Konferenzen starten in Kürze
Heise.de

The Cybersecurity 202: The year’s biggest cybersecurity conferences are back, but limited
The Washington Post

DEF CON 29 Badge Update (The Firmware Kind)!

Posted 8.5.21

In case you didn't know, you can head over to defcon.org/signal for a link to updated badge firmware and instructions! We hope you enjoy DEF CON 29, In-person, or from wherever you may be!

DEF CON 29 In-person Pre-Registration is Closed!

Posted 8.4.21

The DEF CON 29 pre-reg at shop.defcon.org is now closed. You can still get a badge with cash payment onsite while they last, and you can purchase the Human+ Discord role directly on our Discord (discord.gg/defcon) or at plus.defcon.org Thanks to everyone for supporting DEF CON this year, whether you’re attending virtually or here with us in Las Vegas. DEF CON ©‡ U. Tomorrow it begins!

Get the DEF CON 29 Soundtrack!

Posted 8.4.21

Get a head start on DEF CON 29 with this year’s Original Soundtrack! It’s waiting for you on the DEF CON media server right now. Like, right now. You have your assignment.

media.defcon.org/DEF CON 29/

Hackers with Disabilities Guide for DEF CON 29!

Updated 8.2.21

Thanks to @A_P_Delchi and Hackers with Disabilities for creating this helpful accessibility guide to DC29 . Don’t hesitate to reach out if we can help maximize your DEF CON, either through goons or via social media.

DEF CON 29, Now With More Free Black Hat!

Updated 7.30.21

Arriving early in Vegas? Check out Black Hat’s Arsenal and Business Hall for free!

This year, we’ve partnered with our friends at Black Hat to offer a free Black Hat Business Pass to all Def Con In-Person Badge holders. The pass would normally cost $250, but if you fill out their form here, you can get in for free. You’ll just need to show your DEF CON confirmation receipt when you pick up you Black Hat Business Hall pass over at Mandalay Bay.

Black Hat Business Hall hours:
Wednesday, August 4, 10:00 AM - 6:00 PM
Thursday, August 5, 10:00 AM - 4:00 PM

Here’s the full URL for registering: https://blackhat.informatech.com/2021/index/registrations/DEFCON

DEF CON 29 Badges in the Wild!!

Updated 7.23.21

#Badgesighting! #DEFCON29 human badges for Virtual have started to arrive! Join the forums badge hacking thread to compare notes, pictures, and discover puzzles: forum.defcon.org/node/238291 #badgelife

DEF CON 29 Short Story Contest Winners!

Updated 7.23.21

Congratulations to the winners of the DEF CON 29 Short Story Contest!

In FIRST place we have "Networks" by Gwisinkoht!
In SECOND place is "Repository Upload" by Alfred Rowdy!
People's Choice award goes to "FAICT" by Serum!

for the full post: forum.defcon.org/node/238015 #DEFCON

DEF CON 29 In-person Pre-Reg Closes July 29th! Onsite Cash Sales limited!

Updated 7.20.21

Notice for #defcon29 in-person attendees: Online registration closes July 29. That's your last chance to buy a guaranteed badge. After that it's cash at the door, but please know that we’ve only got about 1,000 spaces for cash customers.

To be certain you get in, registering online by the 29th is your best bet. We don’t want to turn anyone away but we will once we reach capacity. Please consider pre-reg at http://shop.defcon.org if you don't want to YOLO it at the door.

Masks and proof of vaccination remain 100% required.

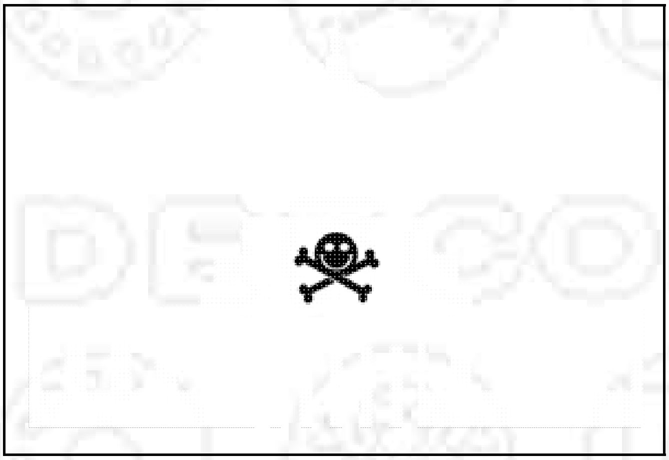
DEF CON 29 Virtual Badges Sold Out! Human Plus coming soon for Discord

Updated 7.16.21

We’ve sold out of badges for online-only attendees. The Human Plus role on the DEF CON Discord (discord.gg/defcon) will be available to purchase soon on the server itself. In the meantime, remember to log in to the Discord to get familiar with the layout and say hi to everyone in the #LineCon channel!

The Policy Dept. is Back for DEF CON 29!

Posted 7.3.21



DEF CON is pleased to announce the return of the Policy Department for DEF CON 29. This means more content for attendees (both in-person and virtual) interested in buidling bridges between the worlds of hackers and policymakers. The Evening Lounge format is back, too! We’ll be posting all the Policy updates at The DEF CON 29 Policy Page , so if this is your thing, make sure to bookmark it and check back often.

Workshops Page is Live!

Posted 7.2.21

Workshops are back for DEF CON 29! We’ve got a wide variety of topics from a great roster of presenters, all of which you can peruse at your leisure on the Workshops page .

If you find a workshop that you want in on, you can sign up starting at 0900 PDT on Tuesday July 6. Seats generally fill quickly, so consider some pre-game finger stretches and warming up your mouse with some light gaming.

It’s July, people. We’re in the home stretch!

Time is Running Out to Vaccinate for DEF CON 29!

Posted 6.29.21

Friendly reminder - if you’re planning to get vaccinated in order to join us for DEF CON 29 in Vegas, there’s only about 5 weeks left until the con. You need about that long from the first shot for the full effect (depending on vendor, of course) so you should get things started.

Vote in the DEF CON 29 Artwork Contest!

Updated 6.28.21

YOU CAN'T STOP THE SIGNAL
DEFCON
DEFCON 29
DEFCON
CAN'T STOP THE SIGNAL

Help us judge the entries to the DEF CON 29 Art contest! Your vote decides the community choice award - so don't let the results be decided without your input! You can see the lineup in the DEF CON Forums at https://forum.defcon.org/node/237564 and you can vote for as many as your heart desires. Shout out to everyone who shared their work!

DEF CON 29 Virtual Badges Sold Out! But Wait...

Updated 6.21.21

DEF CON 29 update update:

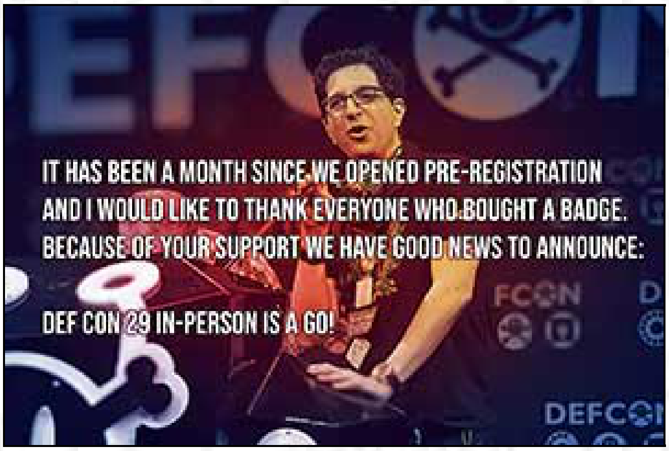
Good news, everyone! We have re-opened badge sales for virtual attendees! The gods of the supply chain have smiled on our undertaking and blessed us with additional stock. Take advantage at shop.defcon.org !

DEF CON 29 update:

We've sold out of the virtual attendee badges for DEF CON 29. Thank you to all the remote attendees who supported us by ordering a badge. Online attendees can still support DEF CON by purchasing a Human+ code at shop.defcon.org .

DEF CON 29 Announcement from DT!

Posted 6.15.21



IT HAS BEEN A MONTH SINCE WE OPENED PRE-REGISTRATION AND I WOULD LIKE TO THANK EVERYONE WHO BOUGHT A BADGE. BECAUSE OF YOUR SUPPORT WE HAVE GOOD NEWS TO ANNOUNCE:

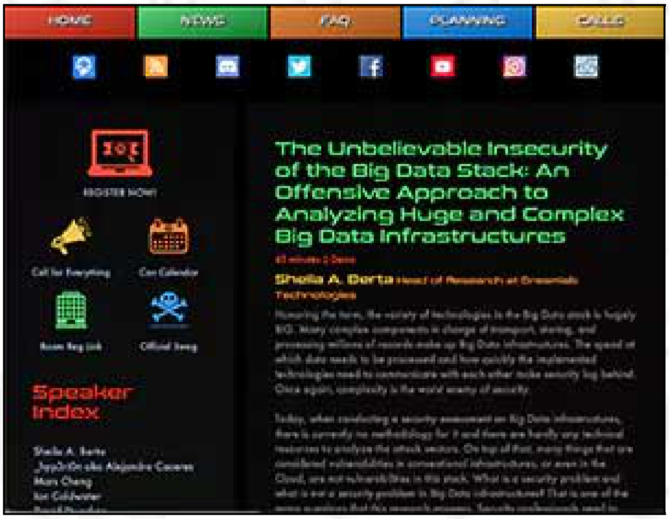
DEF CON 29 IN-PERSON IS A GO!

DEF CON 29 in-person update from The Dark Tangent:

In-person DC29 is a GO. Attendance numbers have been cautiously predicted, badge orders are in, conference space footprint is confirmed. Planning at full tilt. Read the whole thing on DT’s blog .

DEF CON 29 Speaker Page is Live!

Posted 6.11.21



Speaker Index

Sheila A. Berta
_hyp3ri0n aka Alejandro Caceres
Mars Cheng
Ian Coldwater

The Unbelievable Insecurity of the Big Data Stack: An Offensive Approach to Analyzing Huge and Complex Big Data Infrastructures

45 minutes | Demo

Sheila A. Berta Head of Research at Dreamlab Technologies

Humoring the term, the variety of technologies in the Big Data stack is hugely BIG. Many complex components in charge of transport, storing, and processing millions of records make up Big Data infrastructures. The speed at which data needs to be processed and how quickly the implemented technologies need to communicate with each other make security lag behind. Once again, complexity is the worst enemy of security.

Today, when conducting a security assessment on Big Data infrastructures, there is currently no methodology for it and there are hardly any technical resources to analyze the attack vectors. On top of that, many things that are considered vulnerabilities in conventional infrastructures, or even in the Cloud, are not vulnerabilities in this stack. What is a security problem and what is not a security problem in Big Data infrastructures? That is one of the many questions that this research answers. Security professionals need to

The first batch of the DEF CON 29 Speaker lineup is live, people. It’s up there on the DC29 website, just waiting to inform your Con decision-making. Don’t let it shine there in vain. Click on over, have a look-see. Get informed, get inspired, and most importantly get amped. DEF CON 29 is just over the horizon now. Hope we’ll see all of you there.

DEF CON 29 Workshops Announced on the Forums!

Posted 6.8.21

DEF CON 29 Update! You can now read all about the the Workshops accepted for DEF CON 29 over on the forums. It's coming together, people.

NOW OPEN! Pre-register for DEF CON 29! UPDATED!

Updated 5.25.21

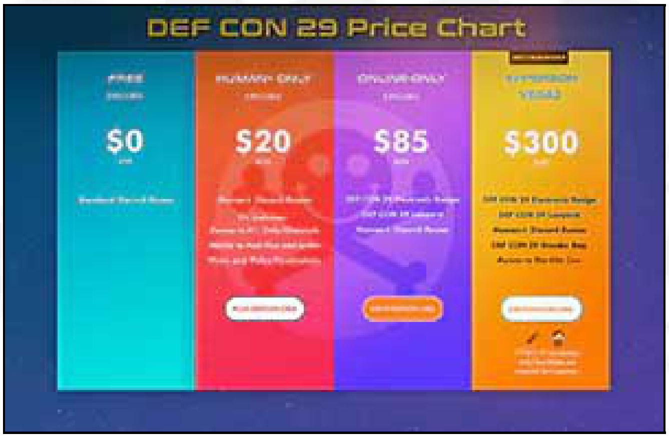
The moment has arrived! You can reserve your badge for DEF CON in Vegas or the DEF CON online-only event right now at shop.defcon.org . Your pre-purchase allows us to accurately predict attendance, and it guarantees you a physical badge and secures your space if the venue is forced to restrict capacity. We thank you for your support and flexibility – hard numbers are the only way we can responsibly make a physical DEF CON happen this year.

Cash at the door will still be honored for as long as spaces last, but there is a chance we'll have to turn away cash customers if we reach capacity for our venues.

For everyone who can't be with us in person, the Safe Mode option continues over on Discord and we expect to start mailing out badges in early July.

We've got an FAQ page for all of your questions , and you can always get in touch with us at info@defcon.org. Thank you again for the support - we can't wait for August 5!

Update! Pricing Chart:


DEF CON 29 Price Chart
FREE
$0
HUMAN+ ONLY
$20
ONLINE-ONLY
$85
$300

DEF CON 29 is our first hybrid con, and the first time we've had more than one price for badges. It's caused a few questions. To answer them, we've created this handy price comparison chart .

If you bought your badge through Black Hat, you've purchased the $300 onsite option. If you haven't signed up yet, badges are available at shop.defcon.org . To upgrade to Human+ status on the Discord, visit plus.defcon.org .

Thank you so much for supporting DEF CON in this crazy time – we can't wait to be together again in August.

New DEF CON 29 Swag in our Shop!

Posted 5.6.21

We’ve got some sparkly new DEF CON 29 items in the shop.defcon.org store! Official Tees in both fitted and straight cut, hoodies and a sticker set. Support DEF CON and get your look right - it’s a win/win.

#cantstopthesignal

DEF CON 29 CTF Quals Results! Congrats PPP!

Posted 5.5.21

The DEF CON 29 quals are complete, the mighty PPP have won the day, and many other teams have qualified. Congratulations to the Plaid Parliament of Pwning and a hearty thank you to all the other teams who participated. Check out the results and challenges !

DEF CON 29 CTF Quals are this Weekend!

Posted 4.29.21

Friendly DEF CON 29 CTF reminder - this weekend the mighty Order of the Overflow is hosting the Qualifier event! It's not often that the path to glory comes into such sharp focus - be ready to meet your destiny. Godspeed to all of the teams who will be battling it out for 48 straight beginning UTC 00:00 May 1st. The information you need is at oooverflow.io and @oooverflow , the courage you need has been inside you all along.

DEF CON 29 is closer than it has ever been. Just let yourself feel it.

DEF CON 29: The Plan So Far

Posted 4.15.21

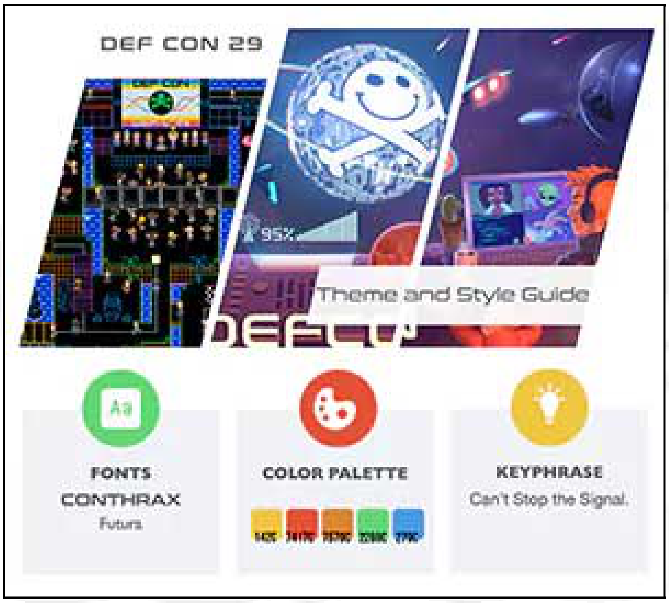
I am announcing this now because the longer we wait and gather data the harder it will be for everyone to make plans, so we are announcing our intentions to kick things off.

DEF CON 29 will be a hybrid conference, partially in-person, and partially online. DEF CON will not be a "normal" con, but more like DEF CON "Different." The situation we face this year is unique and will require us to do things differently, simplify our plans, and in a fast-moving environment be flexible to change.

Read the rest of the Dark Tangent's DEF CON 29 Announcement

DEF CON 29 Theme and Artwork Contest!

Posted 3.28.21



It’s official. DEF CON season has arrived. DEF CON 29 will be happening this August in one form or another and that means it’s time to announce the theme!

The theme for DEF CON 29 is (imagine a drum roll here) ‘You Can’t Stop the Signal’.

The signal can be a few things. It’s the powerful force that draws DEF CON together as a community, across miles, across years, even in global lockdown. It can be the magnet that draws us to the people trying to solve the same puzzles we are, who want to learn how everything works as much as we do. And it’s how we instinctively know that the technology we live with can be better, and we are the ones to figure out how.

We’ve put together a style guide that lays out a bunch of our inspirations for this year, from visual aesthetic to music, to movies and books. We hope it inspires you in whatever you’re creating for DC29, and we hope it gives you the same powerful sense of community and possibility that we feel.

The style guide also governs the Art Contest , so if you're artistically inclined we hope you'll find a nugget or two in there to inspire your entries. We look forward to seeing what you come up with and we thank you for being the kind of amazing, unstoppable community that keeps us coming back.

DEF CON 29 Call for Everything Spotlight—Call for Music and Soundtrack!

Posted 3.10.21

Musicians! Friendly reminder that our DEF CON 29 Call for Music and Soundtrack is open until June 1. If you want to get your sweet sweet choons in front of the DC29 crowd, get up on it!l

DEF CON 29 Call for Everything Spotlight—Call for Contests!

Posted 2.25.21

The DEF CON 29 Call for Everything Spotlight for today is on Call for Contests!

Wanna get your contest into DC29? It’s easy.

1. Have the most incredible idea
2. Submit via the link below
3. See dream realized. Be a legend.

Complete info and guidelines:
https://defcon.org/html/defcon-29/dc-29-cfce.html

DEF CON 29 Call for Everything!

Posted 2.5.21

DEF CON 29 approaches. It looms. Darn near impends. Be still, and you can hear it – the DEF CON Call for Everything ringing though the air.

The CfE is when DEF CON throws open the doors and invites everyone’s best proposals in for a visit. Speaking proposals, ideas for vilages, prospective demo labs, contests, trainings, music, art - literally everything. You write up all the delightful things you want to share with the community, and we find a way to bring the best of them to life at DEF CON.

The Call for Everything page lists all the ways you can participate in the creation of the next DEF CON, along with the relevant details and deadlines, including some new questions intended to get your thoughts on whether this year’s con should be in-person, online or some of both.

So visit the CfE page, read the guidelines, and get your best ideas together. Let’s DO this thing!

Return to Index

DEF CON 29 FAQ

Masks and Vaccination will be required at DEF CON 29 this year, thanks to the complications of COVID-19.

While the virtual portion will largely be the same as DEF CON Safe Mode, in-person DEF CON 29 will be guided by safety and number of attendees.

Vaccination and wearing a mask while in the DEF CON space will be required. No exceptions. Persons who are not vaccinated, including unvaccinated children, will not be admitted.

Vaccinations will be validated by a 3rd party, independent company provided by DEF CON. You must provide an original, signed, vaccination card, with the final dose dated no later than July 22nd, 2021. Photocopies and digital pictures of vaccination cards will not be accepted for anyone, to include Goons and Humans, for entrance to DC29. Once the vaccination record has been verified, participants will receive a wrist band that must be worn at all times during DC29. Participants may then proceed to badge registration to process their barcodes and receive their DC29 Human badge.

Badges may be picked up for others, but the bearer will still need to pass through the vaccination validation and receive a wrist band before they enter the con.

Masks requirements include:

- Mask should be a solid, multi-layer piece of material without slits, exhalation valves, or punctures.
- A properly worn mask completely covers the nose and mouth and is well-fitted.
- May contain filter pockets or sleeves.
- Medical masks and N-95 respirators fulfill the requirements.

The following do not fulfill the mask requirements:

- Face shields or goggles (unless to supplement a proper and properly worn mask)
- Scarves, ski masks, balaclavas, or bandannas
- Shirt or sweater collars pulled up over the mouth and nose.
- Masks made from loosely woven or knitted fabrics that let light pass through
- Masks made from non porous or too dense materials (such as vinyl, plastic or leather)
- Masks that do not fit properly

The guidelines for in-person gatherings is constantly in flux and **we will update our faq on policies and processes, when they will best reflect the most current guidelines that will be necessary during DEF CON**.

FREQUENTLY ASKED QUESTIONS

What is DEF CON doing, and how can I attend?

DEF CON 29 will be a hybrid event this year, we will give hackers a choice in how they wish to experience DEF CON. We will host both an in-person experience in Las Vegas and a virtual con on our official Discord just as we did for DEF CON safe mode in 2020.

Starting mid May we will sell badges online for the conference that we should ship the beginning of July.

For the virtual portion of DEF CON You will need a Discord account.
You can find detailed instructions on getting on the DEF CON Discord server here. There is a FAQ for Humans on Discord as well.

You can support DEF CON and upgrade your account by purchasing the Human Plus role that gives you more permissions than the free "Human" role. Join with the DEF CON Discord Server signup link: https://discord.gg/defcon

If you choose to attend via the DEF CON discord, you will have access to all the online content and pre-recorded talks. There will be contests, villages, DJs, and live chats with hackers all over the globe. You will need to get on the DEF CON Twitch too, for live streamed talk Q&A sessions, evening fireside talks and evening contests. Not to mention the live entertainment and select in-person only villages, events, and contests. Our annual tradition of awarding black badges "Uber" badges for CTF and other select contests, will continue, for in-person events only.

To see what happenings are currently planning to be in-person, hybrid, or virtual only please visit https://forum.defcon.org/node/236142

Can I buy a DEF CON badge with Black Hat?

Yes, it will be an option when you check out at Black Hat.

How much will DEF CON cost?

The price to attend DEF CON in-person will be $300 USD. You may not attend in-person without purchasing a badge. Attending virtual on our Discord will be free, and those with Human+ will have more permissions and access.

You can support DEF CON and upgrade your account by purchasing the Human Plus role.

What if I don't want a Discord Account?

While we don't think you'll get the full experience, all of our content will be released via YouTube and put on the DEF CON Media Server. The Talks for DEF CON will be released during the con on the DEF CON YouTube and Twitch channels.

I have a black badge, do I need to pre-register?

No, just show up on site with your vax card and go to inhuman registration.

Will the content be the same at the in-person event and the virtual event?

Not exactly, there will be unique elements to each, the official DEF CON talks content will be the same for both with the exception of impromptu Q&A or meet and greets. Villages and Contest content may differ, not all events will be held in a hybrid format. See https://forum.defcon.org/node/236142 for a list.

What will capacity look like for the in-person event?

Capacity is currently capped at a maximum of 80% of a given space's fire code standard capacity. Limits will be reviewed and revised at the direction of Southern Nevada Health District (SNHD) and there will be dedicated support onsite to ensure our policies are being followed.

Will DEF CON limit attendance?

YES. If we are near capacity we will limit pre-registration. In the best interest of attendee comfort and safety we would limit attendance to ensure that proper distancing is maintained and locally mandated capacity limits are adhered to. It is recommended that you secure a badge with us when we open the badge pre-registration process.

What health measures/protocols is DEF CON taking to ensure a safe environment on-site?

DEF CON is working closely with Caesar's Entertainment hotels to provide a safe and healthy experience for all. All attendees and staff will need to **be vaccinated** and **wearing a mask**. We will comply with whatever safety measures are required of us.

Currently all of the hotel guidelines that we have gathered are located in the Hotel FAQ.

How do I prove I was vaccinated?

Vaccinations will be validated by a 3rd party, independent company provided by DEF CON. You must provide an original, signed, vaccination card, dated no later than July 22nd, 2021. Photocopies and digital pictures of vaccination cards will not be accepted for anyone, to include Goons and Humans, for entrance to DC29. Once the vaccination record has been verified, participants will receive a wrist band that must be worn at all times during DC29. Participants may then proceed to badge registration to process their barcodes and receive their DC29 Human badge.

What about lines, etc?

Line con, queuing for registration or talks, swag, etc, will have to be planned for in new ways , and the guidelines for gatherings will be in flux for a little while. Just expect "social distanced line con" for the in-person event.

Will I be required to wear a mask? Will medical exceptions be allowed?

Masks will be required for all participants except while eating or drinking, or if presenting as a DEF CON main stage speaker. If you are unable to wear face coverings due to medical reasons, please consider attending virtually.

How will DEF CON maintain social distancing?

Social distancing measures may include distanced seating in event rooms, traffic lanes in the hallways, larger rooms, more strategic areas for food and drinks, dedicated entry and exit points, and more. There will be dedicated support onsite to ensure our rules are being followed.

One of the big visible changes is that we have removed all in-person speaking tracks. Because we don't know how many people are planning to attend we couldn't design the floor plan. By releasing the talks online allows us to complete the floor plan and have attendees focus more on village and events.

Will food be served and what will that look like?

Chill out lounges and other food service may look a little different than previous years in order to adhere to safety measures, but we intend to provide for purchase take away options in a pre-packaged format. No buffet sneezes to worry about.

When & Where will DEF CON be?

August 5, 2021 - August 8, 2021 (Thursday to Sunday)
DEF CON will be located within the Paris and Bally's Hotel and Casinos in Las Vegas, Nevada USA.

Can I book my hotel in Las Vegas now – and how should I do that?

Yes, hotel reservations are being accepted. In order to help us fill our room block with our contracted hotels please book under the DEF CON group room registration.

What happens if DEF CON has to cancel the in-person event or is shut down - can I get a refund?

With the current outlook on vaccine estimations we think that hosting DEF CON in Las Vegas is going to happen, but we know a global pandemic is out of our control. In the event we have to cancel the in-person con we will switch your badge type to "virtual", refund you the difference in price (excluding postage) and mail you your badge, just like we are doing for everyone ordering a virtual-only badge.

Where can I get more information about what's happening?

Check out the following DEF CON Sites & Social Media.
Forums
Groups
Discord
Twitter
Facebook
Reddit
DEF CON YouTube channel
DEF CON Twitch
DEF CON Music Twitch

What's DEF CON's official theme for DEF CON 29?

Glad you asked, our official 2021 theme is "Can't stop the signal." For more information Check out out our DEF CON 29 Theme Guide.

This all sounds great, so how can I contribute to DEF CON this year?

We've always said "DEF CON is what you make it.", and we belive that. If you've got a good idea or want to participate, check out the link for this year's call for everything.

Return to Index

DEF CON FAQ

Frequently asked questions about DEF CON

What is DEF CON?

DEF CON is one of the oldest continuously running hacker conventions around, and also one of the largest.

How did DEF CON start?

Originally started in 1993, it was a meant to be a party for member of "Platinum Net", a Fido protocol based hacking network out of Canada. As the main U.S. hub I was helping the Platinum Net organizer (I forget his name) plan a closing party for all the member BBS systems and their users. He was going to shut down the network when his dad took a new job and had to move away. We talking about where we might hold it, when all of a sudden he left early and disappeared. I was just planning a party for a network that was shut down, except for my U.S. nodes. I decided what the hell, I'll invite the members of all the other networks my BBS (A Dark Tangent System) system was a part of including Cyber Crime International (CCI), Hit Net, Tired of Protection (ToP), and like 8 others I can't remember. Why not invite everyone on #hack? Good idea!

Where did the name come from?

The short answer is a combination of places. There as a SummerCon in the summer, a HoHoCon in the winter, a PumpCon during Halloween, etc. I didn't want any association with a time of year. If you are a Phreak, or just use your phone a lot you'll notes "DEF" is #3 on the phone. If you are into military lingo DEF CON is short for "Defense Condition." Now being a fan of the movie War Games I took note that the main character, David Lightman, lived in Seattle, as I do, and chose to nuke Las Vegas with W.O.P.R. when given the chance. Well I knew I was doing a con in Vegas, so it all just sort of worked out.

There are several resources that will give you an idea of what DEF CON is all about.

DEF CON Press: through the prism of the media
DEF CON Groups: Local groups that meet
DEF CON Media Server: DC 1 to the present, captured
Google: always a good research starting point
Just remember, DEF CON is what you make of it.

When and where is DEF CON?

DEF CON is generally in the last week of July or first week of August in Las Vegas. DEF CON 29 will be held August 5th through August 8th. We are gauging interest on what degree of where. Many people arrive a day early, and many stay a day later.

Isn't there a DEF CON FAQ already?

Yes, an unofficial one. It's quite humorous, sometimes informative, and DEF CON takes no responsibility for its content. It can be found at http://defcon.stotan.org/faq/

What are the rules of DEF CON?

Physical violence is prohibited. Harassment of any kind is prohibited. We don't support illegal drug use. Minors should be accompanied by their parent(s) or guardian(s). Please refrain from doing anything that might jeopardize the conference or attendees such as lighting your hair on fire or throwing lit road flares in elevators. DEF CON Goons are there to answer your questions and keep everything moving. Hotel security is there to watch over their property. Each has a different mission, and it is wise to not anger the hotel people. Please be aware that if you engage in illegal activities there is a large contingency of feds that attend DEF CON. Talking about how you are going to bomb the RNC convention in front of an FBI agent is a Career Limiting Move!

You can view the DEF CON Code of Conduct at https://defcon.org/html/links/dc-code-of-conduct.html.

Is DEF CON cancelled?

No, but DEF CON is planning to perform a risk assessment to help us decide, ideally by sometime in April, if we should hold a physical "last known good configuration" conference in Las Vegas for 2021. We would adhere to all health and safety guidelines, so the better we can understand them the more informed our assessment will be.

What is there to do at DEF CON?

DEF CON is a unique experience for each con-goer. If you google around you'll find dozens of write-ups that will give you an idea of what people have experienced at DEF CON. Trust write-ups more than media articles about the con. Some people play capture the flag 24x7, while many people never touch a computer at DEF CON. Some people see every speech they can, while others miss all speeches. Other activities include contests, movie marathons, scavenger hunts, sleep deprivation, lock picking, warez trading, drunken parties, spot the fed contest, the official music events. Because DEF CON is what the attendees make of it, there are more events than even we are aware of. Half the fun is learning what happened at DEF CON after the fact!

I'm not a hacker, should I go to DEF CON?

Many people have different definitions of what is a ‘hacker’. I would recommend looking at previous years speeches, and write-ups from past attendees - this should give you a good idea if DEF CON is for you. This hacker FAQ might give you some insight into the matter as well. If you do not have any technical interests, DEF CON is probably not for you. Sure there is a lot of socializing you can do, but technology and hacking is the core of the con.

Do criminals go to DEF CON?

Yes. They also go to high school, college, work in your workplace, and the government. There are also lawyers, law enforcement agents, civil libertarians, cryptographers, and hackers in attendance. Ssshhh. Don't tell anyone.

What are Goons?

They are the staff at DEF CON. They have many roles including safety, speaker coordination, vendor room coordination, network operations, et cetera... Please try to be helpful to them if they make requests of you. If any goon tells you to move, please do so immediately as there may be safety issues they are attempting to address.

How can I help out or become a Goon?

The staff at DEF CON has grown organically. All positions have some degree of trust associated with them, so typically new goons are ‘inducted’ by friends of existing goons. There are many random points when goons need help and may ask people for help, generally for helping move stuff or other tasks that don't require high amounts of trust or unsupervised work. Just because you help out doesn't make you a goon. If you really want to be a goon, talk with one and see how much work they actually do (Hint: you may want to enjoy being at DEF CON, not working full-time at it). One year the network group got a new Goon when a networking engineer was needed, and he came to the rescue. The intent behind the goons is not to be elitist, but to have a network of trusted people who can help run the conference - please do not feel upset if you are not chosen to be a goon.

How can I help or participate?

DEF CON is not a spectator sport! Before the con, during, and after there are chances for you to get involved. Before the con you can read about the contests and maybe sign up for one like Capture the Flag. There are artwork contests for shirts and posters. You can practice your lock pick skills, or just get your laptop all locked down and ready to do battle. Organize your .mp3s. Check out the DEF CON Forums to see what other people are up to. If you want to create your own event, you can do that as well - you will not get official space or sanctions, but virtually every official event at DEF CON started out as an unofficial event.

I would love to see XYZ event, how do I make this happen?

Virtually all events at DEF CON were conceived by the attendees. The DEF CON forums are a great place for recruiting help for an event you want to put on, and making sure your efforts aren't being duplicated. If it doesn't require resources from DEF CON (space, namely) you generally don't have to ask anyone’s permission. Most events are unofficial until they've been going on for a couple of years. Please let us know if you have an idea for an event, we may help facilitate or promote it. Email [suggestions at DEF CON dot org] to keep us in the loop.

How can I speak at DEF CON?

You can submit a response to our CFP (call for papers). All entries are read and evaluated by a selection committee. We would love to have your submission. The call for papers usually opens in January and closes mid-May.

I'm press, how do I sign up, why can't I get in for free (I'm just doing my job)?

Please email press[at]defcon[d0t]org if you wish press credentials. Lots of people come to DEF CON and are doing their job; security professionals, federal agents, and the press. It wouldn't be fair to DEF CON attendees if we exempted one group from paying. If you are a major network and plan on doing a two minute piece showing all the people with blue hair, you probably shouldn't bother applying for a press pass - you won't get one. If you are a security writer or from a real publication please submit, and someone will respond with an answer.

I want to sell stuff, how do I do this?

If you want a space in our vendor area, you need to apply. Because of limited space and our attempt to have a diversity of vendors, you may not be able to get a booth. It is wise to think of staffing issues - if you are one person do you want to spend your entire time behind a vendors booth?

What are the different price rates?

Everyone pays the same: The government, the media, the ‘well known hackers’, the unknown script kiddies. The only discount is for Goons and speakers, who get to work without paying for the privilege.

How much is admission DEF CON, and do you take credit cards?

The price for DEF CON 29 is TBA. For reference, DEF CON 27 (in person) cost $300 USD Cash for all four days. Do we take credit cards? Are you JOKING? No, we only accept cash - no checks, no money orders, no travelers checks. We don't want to be a target of any State or Federal fishing expeditions.

Does my underage child need a badge?

Children under the age of 8 will not need to purchase a badge.

Can I pre-register for DEF CON?

No. We used to do this a long time ago, but found that managing the registration list, and preventing one 'Dr. Evil' from impersonating another 'Dr. Ev1l' too much of a hassle. Seeing how we would only take cash in the first place, and things becomes time consuming and easy to abuse. Cash at the door works every time.

Can I get a discount on DEF CON badges?

DEF CON charges one price regardless of your social status or affiliation. Please know that we depend on attendee income to pay the costs of the conference and don't have sponsors to help defray the expenses.

We sometimes get requests for discounts [students, veterans, children], unfortunately we don't want to try and validate if you are a current student, look at your ID to determine your age, decode military discharge papers, etc.

If you really want to attend DEF CON for free then do something for the con.

You could:
Submit a CFP and be an accepted speaker or workshop instructor.
Work on a contest, event, or village.

Qualify for CTF/Contests that include entry.
Find a team to become a Goon newbie.
Contribute to content, or perform some entertainment.

I need a letter of invite for my visa application, how do I get that?

In most cases, DEF CON can send a signed letter of invite, usually within a few short business days once we have all the info. If you also require verification of housing, we can put you in touch with someone to help you get your hotel stay organized, let us know if you need that.

Along with your request, please email us the following to info(at)defcon(.)org

Name as is on passport:
Passport number:
Country of issue:
Date of issue:
Date of expiration:
Country of origin:

DEF CON is too expensive, how can I afford it?

DEF CON is cheaper than many concerts, and certainly cheaper than many shows in Vegas. Many people have made an art and science out of coming to DEF CON very cheaply. Here are a couple of tips.

Travel: Buy airfare in advance, go Greyhound, Carpool, hitch-hike. (Note: this may be dangerous and/or illegal.)
Lodging: Share rooms - some people have up to 10 people they share a room with, find a hotel cheaper than the one that the conference is scheduled at, stay up for three days, etc. (note: this can be hazardous to your health.)
Food: Pack food for your trip, go off site to find food, eat in your hotel rooms, and look for cheap Vegas food at Casinos. (Look for deals and specials that are trying to get you in the door to gamble.)
Booze: You don't need to drink. Brew your own and bring it. (It's been done.)
Entrance: Admission can be saved, mow some lawns. Try to go to another 4 day event for cheaper than this that offers so much. We have increased the fees slowly over the years, but also the amount and quality of events have increased.

Inevitably people will try to do some math and pretend that DT gets rich each DEF CON - they seem to lack the ability to subtract.

How many people typically attend DEF CON?

There have been roughly 25-28k attendees in the last few years of DEF CON. DEF CON 27 had a record showing with approximately 30,000.

Is there a network at DEF CON?

Why yes, DEF CON is FULLY network-enabled. Now that we've perfected the art of a stable hacker con network, we're ascending to a higher level - we're providing you a network that you feel SAFE in using! Since DEF CON 18 we're WPA2 encrypted over-the-air, with a direct trunk out to the Internet. No peer-to-peer, no sniffing, just straight to the net (and internal servers). We'll provide login credentials at Registration. We know the LTE airwaves will be saturated so we're putting our own cred on the line to give you a net that even we would put our own mobile phones on.

If you're feeling frisky, we'll still have the traditional "open" network for you - bring your laptop (we'd recommend a clean

OS, fully patched--you know the procedure) because we don't police what happens on that net. Share & enjoy!

What is the age limit?

People have brought children to DEF CON - it is not recommended to do this unless you are going to constantly supervise them. It is generally an ‘adult’ atmosphere (language, booze, et cetera). If you've never been to DEF CON, you may want to refrain from bringing your children (unless they are demanding that you bring them). While there are no age limits, we have consistently cooperated with parents and/or private investigators who are looking for children that ‘ran away from home’ to go to DEF CON. You will have to be 21 to reserve a room.

What is a DEF CON "Black Badge"?

The Black Badge is the highest award DEF CON gives to contest winners of certain events. CTF winners sometimes earn these, as well as Hacker Jeopardy winners. The contests that are awarded Black Badges vary from year to year, and a Black Badge allows free entrance to DEF CON for life, potentially a value of thousands of dollars.

How can I get a hold of DT? I tried to mail him and haven't seen a response yet.

DT doesn't dislike you, isn't trying to hurt your feelings, and bears you no ill will. The fact is he gets an unmanageable load of mail continually. Mailing him again may elicit a response. Try mailing FAQ (at) DEFCON.ORG if you have a general question that isn't answered here or in the forums.

Is it hot in Vegas?

Yes. Bring sunscreen (high SPF), do not fall asleep near the pool (lest you wake up to sunburn), and do not walk far in the sun unless you are experienced in dealing with extreme heat. The sun is dangerous in Las Vegas. Sleeping in lawn chairs is a sure way to wake up to severe burns in the morning when that bright yellow thing scorches your skin. Drink plenty of water and liquids - remember that alcohol will dehydrate you.

What should I bring?

It depends on what you're going to do at DEF CON. This is discussed in quite some depth on the unofficial DC FAQ, as well as a thread in the DC Forums. You may want to bring fancy (or outrageously silly) clothes for the official Music events, on Friday and Saturday nights, where everyone shows off nifty attire.

How much do rooms cost, and how do I reserve a room?

The DEF CON 29 group room registration is now live! We have room rates at seven hotels, until they run out of rooms in our block.

Follow this link: https://book.passkey.com/gt/217951677?gtid=91d4af3428476f6bf43ba59e7f698eac

Do not worry if the form doesn't immediately show the discounted rate. To verify that you're getting our price you can mouse over the dates you've selected or begin the checkout process.

How much is internet access?

We are looking into this. Free (and possibly more dangerous) internet access is available in the convention area.

Will the hotels broadcast the speeches on their cable system?

DEF CON TV has succcessfully streamed all tracks to all the hotels, and a couple of tracks out to the internet, for several years now. We don't expect this will change!

Will we have DEF CON branded poker chips?

You will have to attend DEF CON to find out.

Will conference attendees have entire floors of hotel rooms to themselves?

Probably not. The hotel is very cooperative in attempting to centralize the DEF CON attendees, for their convenience and ours, but there will be non-DEF CON attendees in hotel rooms next to us.

This FAQ didn't answer my questions, or was unclear, how can I get further information?

Check out the DEF CON Forums to ask follow up questions.

Return to Index

Links to DEF CON 29 related pages

Links

DEF CON . org

Main DEFCON site
DEFCON 29 Home Page
DEFCON FAQ
DEFCON 29 FAQ
DEFCON 29 Schedule and Speakers
DEF CON 29 Workshops page
DEF CON 29 Vendors page
DEF CON 29 Demolabs Forums page
DEF CON 29 Parties Forum page
DEF CON 29 Villages Forum page
DEF CON 29 Contests Forum page

Thanks to the InfoBooth crew for providing access to their backend database. <claps> to their hard work!

Villages

Village Name Home Page	Schedule	Forum Link	DC Discord Chan	Video Stream Link/Info	Social Media Links
Adversary Village	Sched	Forum	#adv-general	Link	TW @AdversaryVillag IG @AdversaryVillage LI @adversaryvillage FB @AdversaryVillage TI @AdversaryVillage DC https://discord.gg/GDB3rC7KYz YT link
Aerospace Village	Sched	Forum	#av-lounge-bar-text	Link	TW @secureaerospace LI @aerospace-village TW @hack_a_sat
AI Village	Sched	Forum	#aiv-general-text	Link	TW @aivillage_dc TI @aivillage YT link DC https://aivillage.org/discord-guide
AppSec Village	Sched	Forum	#asv-general-text	Link	TW @AppSec_Village LI @appsecvillage YT https://www.youtube.com/c/AppSecVillage
Blockchain Village	Sched	Forum	#bcv-general-text		TW @BCOSvillage
Blacks in Cybersecurity	Sched	Forum		Link	TW @BlackInCyberCo1 IG @blackincyberconf TI @blacksincybersecurity YT https://youtu.be/YsUw9z_gZzY LI @blackincyberconference PT @blacksincybersecurity FB @blackincyberconf
Bio Hacking Village		Forum	#bhv-orientation-text	Link	TW @dc_bhv LI @biohacking-village

Village Name Home Page	Schedule	Forum Link	DC Discord Chan	Video Stream Link/Info	Social Media Links
					YT http://youtube.com/biohackingvillage TI @biohackingvillage DC https://discord.gg/Q8ubDb5 SP link
Blue Team Village	Sched	Forum	#btv-general-text	Link	TW @BlueTeamVillage TI @blueteamvillage YT https://www.youtube.com/c/blueteamvillage DC https://discord.com/invite/blueteamvillage
Car Hacking Village		Forum	#chv-general-text	Link	TW @CarHackVillage DC https://discord.gg/JWCcTAM
Career Hacking Village		Forum	#cahv-general-text	Link	TW @HackingCareer YT https://www.youtube.com/CareerHackingVil
Cloud Village	Sched	Forum	#cloudv-general-text	Link	TW @cloudvillage_dc YT https://www.youtube.com/cloudvillage_dc
Cryptocurrency Village	Sched	Forum	#cv-general-text		TW @DEFCONCCVillage YT https://www.youtube.com/c/MoneroSpaceWorkg
Crypto Privacy Village		Forum	#cpv-general-text	Link	TW @cryptovillage SL https://cryptovillage.slack.com/ YT link TI @cryptovillage YT link
Data Duplication Village	Sched	Forum	#ddv-general-text		TW @DDV_DC
Hack the Sea Village		Forum	#htsv-general-text	Link	TW @hack_the_sea
Ham Radio Village	Sched	Forum	#hrv-k3k-special-eve...	Link	TW @HamRadioVillage TI @HamRadioVillage DC https://discord.gg/hrv
Hardware Hacking Soldering Skills Village	Sched	Forum	#hhv-welcome-text		TW @DC_HHV
IndustrialControlSystems Village		Forum	#ics-101-text	Link	TW @ICS_Village LI @icsvillage YT link TI @ics_village
InternetOfThings Village	Sched	Forum	#iotv-hangout-zone-text	Link	TW @iotvillage TW @ISEsecurity TW @Villageidiotlab LI @iotvillage TI @iotvillage YT https://www.youtube.com/c/IoTVillage/videc DC https://discord.gg/tmZASSpNnP
Lock Bypass Village	Sched	Forum	#lbv-social-text	Link	TW @bypassvillage TI @bypassvillage
Lock Pick Village	Sched	Forum	#lpv-general-text		TW @toool TI @toool_us YT https://youtube.com/c/TOOOL-US
Packet Hacking Village	Sched	Forum	#phv-infobooth-text	Link	TW @wallofsheep FB @wallofsheep YT https://youtube.com/wallofsheep

Village Name Home Page	Schedule	Forum Link	DC Discord Chan	Video Stream Link/Info	Social Media Links
					TI @wallofsheep PS https://www.periscope.tv/wallofsheep
Password Village	Sched	Forum	#pwdv-general-text	Link	TW @PasswordVillage TI @passwordvillage YT link
Payment Village	Sched	Forum	#payv-labs-text	Link	TW @paymentvillage TI @paymentvillage YT link
Recon Village	Sched	Forum	#rv-general-text	Link	TW @ReconVillage FB @reconvillage
RF Village	Sched	Forum	#rfv-general-text		TW @rfhackers TW @rf_ctf link DC https://discordapp.com/invite/JjPQhKy
Rogues Village		Forum	#rov-general-text	Link	TW @RoguesVillage TI @roguesvillage TW @foursuits_co YT https://www.youtube.com/c/foursuits IG @foursuits_co
Security Leaders Village		Forum			TW @securityleader2 DC https://discord.gg/wn58YfQEND
Social Engineering Village		Forum	#sev-general-text	Link	FB @socialengineerinc TW @humanhacker LI @social-engineer YT https://www.youtube.com/user/SocialEngine
Voting Machine Village	Sched	Forum	#vmhv-general-text	Link	TW @votingvillagedc YT link

Other Interesting Links

@defconparties - calandar
defconmusic - Schedule
DCTV - DEF CON TV
DEF CON 29 badge firmware
#badgelife spreadsheet of unofficial badges for DC29
DEF CON is Cancelled party challange

Other cons during #SummerHackerCamp

Blackhat	T @BlackHatEvents	FB Black Hat Events
BSides Las Vegas	T @BSidesLV	
r00tz Asylum	T @r00tzasylum	
Queercon	T @Queercon	FB @queercon
The Diana Initiative	T @Dianainitiative	FB @dianainitiative

Guides/Tips/FAQs

The Lost Policymaker's Guide to Hacker Summer Camp
Lonely Hackers Club - DEF CON n00b guide - reddit thread
Preparing for "Hacker Summer Camp"
General / previous years
DEF CON for N00bs
JK-47 - BSidesLV & DEFCON Conference Tips
Just another DEF CON guide
HACKER SUMMER CAMP 2018 GUIDE
On Attending DefCon