FIRESIDES LOUNGE

-THURSDAY-

FRIDAY

DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION

Friday at 20:00 in Sin City Theatre at Planet Hollywood

Christian "quaddi" Dameff, Jeff "r3plicant" Tully MD, Suzanne Schwartz MD, Marie Moe PhD, Billy Rios, Jay Radcliffe

PANEL: DEF CON GROUPS

Friday at 22:15 in Sin City Theatre at Planet Hollywood

Brent White / B1TK1LL3R, Jayson E. Street, Darington, April Wright, Tim Roberts (byt3boy), Casey Bourbonnais, s0ups

SATURDAY

MEET THE EFF - MEETUP PANEL

Saturday at 20:00 in Sin City Theatre at Planet Hollywood

Kurt Opsahl, Camille Fischer, Bennett Cyphers, Nathan 'nash' Sheard, Shahid Buttar

WE HACKED TWITTER! AND THE WORLD LOST THEIR SH*T OVER IT!

Saturday at 22:15 in Sin City Theatre at Planet Hollywood

Mike Godfrey, Matthew Carr

	DC 101 IN TRACK 4
10:00	**Exploiting Windows Exploit Mitigation for ROP Exploits** Omer Yair
11:00	**Breaking Google Home: Exploit It with SQLite (Magellan)** Wenxiang Qian, YuXiang Li, HuiYu Wu
12:00	**Are Quantum Computers Really A Threat To Cryptography? A Practical Overview Of Current State-Of-The-Art Techniques With Some Interesting Surprises** Andreas Baumhof
13:00	**Intro to Embedded Hacking -- How you too can find a decade old bug in widely deployed devices. [REDACTED] Deskphones, a case study.** Philippe Laulheret
14:00	**Web2Own: Attacking Desktop Apps From Web Security's Perspective** Junyu Zhou, Ce Qin, Jianing Wang
15:00 15:30	**DEF CON 101 Panel** Highwiz, Nikita, Will, n00bz, Shaggy, SecBarbie, Tottenkoph

	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	Behind the Scenes of the DEF CON 27 Badge Joe Grand (Kingpin)	Hacking Congress: The Enemy Of My Enemy Is My Friend Former Rep. Jane Harman, Rep. James Langevin, Jen Ellis, Cris Thomas, Rep. Ted Lieu	Behind the Scenes: The Industry of Social Media Manipulation Driven by Malware Olivier Bilodeau, Masarah Paquet-Clouston	Duplicating Restricted Mechanical Keys Bill Graydon, Robert Graydon
11:00	Don't Red-Team AI Like a Chump Ariel Herbert-Voss	The Tor Censorship Arms Race: The Next Chapter Roger Dingledine	All the 4G Modules Could Be Hacked XiaoHuiHui, Ye Zhang, ZhengHuang	Evil eBPF In-Depth: Practical Abuses of an In-Kernel Bytecode Runtime Jeff Dileo
12:00	Process Injection Techniques - Gotta Catch Them All Itzik Kotler, Amit Klein	Phreaking Elevators WillC	Infiltrating Corporate Intranet Like NSA _Pre-auth RCE on Leading SSL VPNs Orange Tsai, Meh Chang	API-Induced SSRF: How Apple Pay Scattered Vulnerabilities Across the Web Joshua Maddux
13:00	HackPac: Hacking Pointer Authentication in iOS User Space Xiaolong Bai, Min (Spark) Zheng	HVACking: Understand the Difference Between Security and Reality! Douglas McKee, Mark Bereza	No Mas—How One Side-Channel Flaw Opens Atm, Pharmacies and Government Secrets Up to Attack phar	More Keys Than A Piano: Finding Secrets In Publicly Exposed Ebs Volumes xBen "benmap" Morris
14:00	Harnessing Weapons of Mac Destruction Patrick Wardle	Are Your Child's Records at Risk? The Current State of School Infosec Bill Demirkapi	How Deep Learning Is Revolutionizing Side-Channel Cryptanalysis Elie Bursztein, Jean Michel Picod	Practical Key Search Attacks Against Modern Symmetric Ciphers Daniel "ufurnace" Crowley, Daniel Pagan
15:00	MOSE: Using Configuration Management for Evil Jayson Grace	Change the World, cDc Style: Cow tips from the first 35 years Joseph Menn, Peiter Mudge Zatko, Chris Dildog Rioux, Deth Vegetable, Omega	100 Seconds of Solitude: Defeating Cisco Trust Anchor With FPGA Bitstream Shenanigans Jatin Kataria, Rick Housley, Ang Cui	Relaying Credentials Has Never Been Easier: How to Easily Bypass the Latest NTLM Relay Mitigations Marina Simakov, Yaron Zinar
16:00	Please Inject Me, a x64 Code Injection Alon Weinberg	I Know What You Did Last Summer: 3 Years of Wireless Monitoring at DEF CON d4rkm4tter (Mike Spicer)	Surveillance Detection Scout - Your Lookout on Autopilot Truman Kain	The JOP ROCKET: A Supremely Wicked Tool for JOP Gadget Discovery, or What to Do If ROP Is Too Easy Dr. Bramwell Brizendine, Dr. Joshua Stroschien
16:30	Poking the S in SD cards Nicolas Oberli	Can You Track Me Now? Why The Phone Companies Are Such A Privacy Disaster U.S. Senator Ron Wyden	Breaking The Back End! It Is Not Always A Bug. Sometimes, It Is Just Bad Design! Gregory Pickett	Re: What's up Johnny?—Covert Content Attacks on Email End-to-End Encryption Jens Müller

-SATURDAY-

	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	Weaponizing Hypervisors to Fight and Beat Car and Medical Devices Attacks Ali Islam, Dan Regalado (DanuX)	Rise of the Hypebots: Scripting Streetwear finalphoenix	Information Security in the Public Interest Bruce Schneier	EDR Is Coming; Hide Yo Sh!t Michael Leibowitz, Topher Timzen
11:00	Your Car is My Car Jmaxxz	HAKC THE POLICE Bill Swearingen	Hacking Your Thoughts - Batman Forever meets Black Mirror Katherine Pratt/GattaKat	Meticulously Modern Mobile Manipulations Leon Jacobs
12:00	How You Can Buy AT&T, T-Mobile, and Sprint Real-Time Location Data on the Black Market Joseph Cox	Defeating Bluetooth Low Energy 5 PRNG for Fun and Jamming Damien Cauquil (virtualabs)	Why You Should Fear Your "mundane" Office Equipment Daniel Romero, Mario Rivas	Zombie Ant Farm: Practical Tips for Playing Hide and Seek with Linux EDRs Dimitry Snezhkov
13:00	RACE - Minimal Rights and ACE for Active Directory Dominance Nikhil Mittal	GSM: We Can Hear Everyone Now! Campbell Murray, Eoin Buckley, James Kulikowski	Tag-side attacks against NFC Christopher Wade	SSO Wars: The Token Menace Alvaro Muñoz, Oleksandr Mirosh
14:00	SELECT code_execution FROM * USING SQLite; -- Gaining code execution using a malicious SQLite database Omer Gull	I'm on your phone, listening - Attacking VoIP Configuration Interfaces Stephan Huber, Philipp Roskosch	Zero bugs found? Hold my Beer AFL! How To Improve Coverage-Guided Fuzzing and Find New 0days in Tough Targets Maksim Shudrak	Next Generation Process Emulation with Binee Kyle Gwinnup, John Holowczak
15:00	Get Off the Kernel if You Can't Drive Jesse Michael, Mickey Shkatov	Reverse-Engineering 4g Hotspots for Fun, Bugs and Net Financial Loss g richter	State of DNS Rebinding - Attack & Prevention Techniques and the Singularity of Origin Gerald Doussot, Roger Meyer	.NET Malware Threats: Internals And Reversing Alexandre Borges
16:00	Reverse Engineering 17+ Cars in Less Than 10 Minutes Brent Stone	NOC NOC. Who's there? All. All who? All the things you wanted to know about the DEF CON NOC and we won't tell you about The DEF CON NOC	Confessions of an Nespresso Money Mule: Free Stuff & Triangulation Fraud Nina Kollars, Kitty Hegemon	Vacuum Cleaning Security: Pinky and the Brain Edition jiska, clou (Fabian Ullrich)
16:30	Unpacking Pkgs: A Look Inside Macos Installer Packages And Common Security Flaws Andy Grant		Go NULL Yourself or: How I Learned to Start Worrying While Getting Fined for Other's Auto Infractions droogie	Apache Solr Injection Michael Stepankin

	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	Backdooring Hardware Devices By Injecting Malicious Payloads On Microcontrollers Sheila Ayelen Berta	Adventures In Smart Buttplug Penetration (testing) smea	Hacking WebAssembly Games with Binary Instrumentation Jack Baker	Your Secret Files Are Mine: Bug Finding And Exploit Techniques On File Transfer App Of All Top Android Vendors Xiangqian Zhang, Huiming Liu
11:00	The ABC of Next-Gen Shellcoding Hadrien Barral, Rémi Géraud-Stewart, Georges-Axel Jaloyan	SDR Against Smart TVs: URL and Channel Injection Attacks Pedro Cabrera Camara	Exploiting Qualcomm WLAN and Modem Over The Air Xiling Gong, Peter Pi	Say Cheese - How I Ransomwared Your DSLR Camera Eyal Itkin
12:00	I'm In Your Cloud... Pwning Your Azure Environement Dirk-jan Mollema	Malproxying: Leave Your Malware at Home Hila Cohen, Amit Waisel	HTTP Desync Attacks: Smashing into the Cell Next Door albinowax	Help Me, Vulnerabilities. You're My Only Hope Jacob Baines
13:00	[MI CASA-SU CASA] My 192.168.1.1 is Your 192.168.1.1 Elliott Thompson	Sound Effects: Exploring Acoustic Cyber-weapons Matt Wixey	Owning The Clout Through Server-Side Request Forgery Ben Sadeghipour, Cody Brocious (Daeken)	Want Strong Isolation? Just Reset Your Processor Anish Athalye
14:00	Firmware Slap: Automating Discovery of Exploitable Vulnerabilities in Firmware Christopher Roberts	Cheating in eSports: How to Cheat at Virtual Cycling Using USB Hacks Brad Dixon	The Ether Wars: Exploits, counter-exploits and honeypots on Ethereum Bernhard Mueller, Daniel Luca	Contests Awards Ceremony Contests & Events
15:00	Closed			
16:00	Closing Ceremonies The Dark Tangent & Goons			