

BRIEFINGS DAY 1 THURSDAY, NOVEMBER 3, 2016

Level 2	Auditorium	Gallery Hall	Room A	Room DEFG
08:00-18:30	Registration // Village Green			
09:00-10:00	Continental Breakfast // Location Sponsored by: BOOLEBOX iBOSS nccgroup			
10:00-11:00	Flip Feng Shui: Rowhammering the VM's Isolation <i>by Kaveh Razavi + Ben Gras</i>	WiFi-based IMSI Catcher <i>by Piers O'Hanlon + Ravishankar Borgaonkar</i>	Automating Incident Response: Sit Back and Relax, Bots are Taking Over... <i>by Elvis Hovor + Mohamed El-Sharkawi</i>	Pocket-Sized Badness: Why Ransomware Comes as a Plot Twist in the Cat-Mouse Game <i>by Federico Maggi</i>
11:00-11:15	Coffee Service // Business Hall, Mezzanine Level Sponsored by: BLACKDUCK CARBON BLACK Check Point CHECKMARX			
11:15-12:15	Ghost in the PLC: Designing an Undetectable Programmable Logic Controller Rootkit <i>by Ali Abbasi + Majid Hashemi</i>	50 Thousand Needles in 5 Million Haystacks: Understanding Old Malware Tricks to Find New Malware Families <i>by Veronica Valeros + Karel Bartos + Lukas Machlica</i>	Effective File Format Fuzzing - Thoughts, Techniques and Results <i>by Mateusz Jurczyk</i>	Code Deobfuscation: Intertwining Dynamic, Static and Symbolic Approaches <i>by Robin David + Sebastien Bardin</i>
12:15-12:30	Break			
12:30-13:30	30 MINUTE SESSION I Know What You Saw Last Minute - The Chrome Browser Case <i>by Ran Dubin</i>	Mobile Espionage in the Wild: Pegasus and Nation-State Level Attacks <i>by Max Bazaliy + Seth Hardy + Andrew Blaich</i>	30 MINUTE SESSION Chasing Foxes by the Numbers: Patterns of Life and Activity in Hacker Forums <i>by Christopher Ahlberg</i>	How to Fool an ADC, Part II or Hiding Destruction of Turbine with a Little Help of Signal Processing <i>by Gabriel Gonzalez</i>
12:30-14:30	Lunch Break // Village Green, Ground Floor & Gallery Bays, Level 2			
14:30-15:30	Another Brick Off the Wall: Deconstructing Web Application Firewalls Using Automata Learning <i>by George Argyros + Ioannis Stais</i>	Rooting EVERY Android: From Extension to Exploitation <i>by Di Shen + James Fang</i>	Towards a Policy-Agnostic Control-Flow Integrity Implementation <i>by Dean Sullivan + Orlando Arias + Yier Jin + Ahmad-Reza Sadeghi</i>	Narcos, Counterfeiters and Scammers: An Approach to Visualize Illegal Markets <i>by Andrew Lewman + Stevan Keraudy</i>
15:30-16:00	Coffee Service // Business Hall, Mezzanine Level Sponsored by: CRONUS CYBERGYM ESET exabeam			
16:00-17:00	Cyber Judo: Offensive Cyber Defense <i>by Tal Be'ery + Itai Grady</i>	Attacking Windows by Windows <i>by Yin Liang + Li Zhou</i>	Stumping the Mobile Chipset <i>by Adam Donenfeld</i>	Talking Behind Your Back: Attacks and Countermeasures of Ultrasonic Cross-Device Tracking <i>by Vasilios Mavroudis + Federico Maggi</i>
17:00-18:30	Business Hall Welcome Reception // Mezzanine Level Sponsored by: CYLANCE NAVIGANT QUALYS Raytheon Foreground Security			

Schedule as of October 24, 2016. Subject to Change

BRIEFINGS DAY 2 FRIDAY, NOVEMBER 4, 2016

Level 2	Auditorium	Gallery Hall	Room A	Room DEFG
08:00-16:00	Registration // Village Green			
08:30-09:30	Continental Breakfast // Location Sponsored by: paloalto SentinelOne tenable			
09:30-10:30	Backslash Powered Scanning: Hunting Unknown Vulnerability Classes <i>by James Kettle</i>	ARMageddon: How Your Smartphone CPU Breaks Software-Level Security and Privacy <i>by Moritz Lipp + Clementine Maurice</i>	Breaking BHAD: Abusing Belkin Home Automation Devices <i>by Scott Tenaglia + Joe Tanen</i>	EGO MARKET: When People's Greed for Fame Benefits Large-Scale Botnets <i>by Masarah Paquet-Clouston + Olivier Bilodeau</i>
10:30-10:45	Coffee Service // Business Hall, Mezzanine Level Sponsored by: hp mimecast QA RAPID7			
10:45-11:45	Breaking Big Data: Evading Analysis of the Metadata of Your Life <i>by David Venable</i>	Use-After-Use-After-Free: Exploit UAF by Generating Your Own <i>by Guanxing Wen</i>	Detach Me Not - DoS Attacks Against 4G Cellular Users Worldwide from your Desk <i>by Silke Holtmanns + Siddharth Rao</i>	Witchcraft Compiler Collection : Towards Self Aware Computer Programs <i>by Jonathan Brossard</i>
11:45-12:00	Break			
12:00-13:00	Bypassing Secure Boot using Fault Injection <i>by Niek Timmers + Albert Spruyt</i>	30 MINUTE SESSION Signing into One Billion Mobile App Accounts Effortlessly with OAuth2.0 <i>by Ronghai Wang + Wing Cheong Lau</i>	30 MINUTE SESSION Randomization Can't Stop BPF JIT Spray <i>by Elena Reshetova</i>	CTX: Eliminating BREACH with Context Hiding <i>by Dimitris Karakostas + Eva Sarafianou + Dionysis Zindros</i>
12:00-14:00	Lunch Break // Village Green, Ground Floor & Gallery Bays, Level 2			
14:00-15:00	Bypassing Clang's SafeStack for Fun and Profit <i>by Enes Goktas</i>	(Pen)Testing Vehicles with CANToolz <i>by Alexey Sintsov</i>	Real-World Post-Quantum Cryptography: Introducing the OpenQuantumSafe Software Project <i>by Jennifer Fernick</i>	DRAMA: How Your DRAM Becomes a Security Problem <i>by Michael Schwarz + Anders Fogh</i>
15:00-15:30	Coffee Service // Business Hall, Mezzanine Level Sponsored by: Recorded Future splunk TREND MICRO VERACODE			
15:30-16:00	Inside Web Attacks: The Real Payloads <i>by John Graham-Cumming</i>	AI based Antivirus: Can AlphaAV Win the Battle in which Man Has Failed? <i>by Thomas Lei Wang + Yanyan Ji</i>	GPU Security Exposed <i>by Justin Taft</i>	When Virtualization Encounters AFL: A Portable Virtual Device Fuzzing Framework with AFL <i>by Moony Li</i>
16:00-16:15	Break			
16:15-17:00	Locknote: Conclusions and Key Takeaways from Black Hat Europe 2016 // moderated by Jeff Moss // Location			

LEGEND	Android, iOS and Mobile Hacking	Exploit Development	Malware	Reverse Engineering
	Cryptography	Hardware/Embedded	Network Defense	Smart Grid/Industrial Security
	Data Forensics and Incident Response	Human Factors	Platform Security: VM, OS, Host and Container	Web AppSec
	Enterprise	Internet of Things	Panel	

Open to all pass types

Schedule as of October 24, 2016. Subject to Change

ARSENAL DAY 1					
THURSDAY, NOVEMBER 3, 2016					
Station	Business Hall // Mezzanine Level				
	Station 1	Station 2	Station 3	Station 4	Station 5
10:00-11:50	Yasuo <i>by Saurabh Harit</i>	Dradis: Collaboration and Reporting for InfoSec Teams <i>by Daniel Martin</i>	Koodous <i>by Daniel Vaca</i>	OWASP ZSC <i>by Ali Razmjoo Qalaei + Brian Beaudry</i>	WSSAT - Web Service Security Assessment Tool <i>by Mehmet Yalcin YOLALAN + Salih TALAY</i>
11:50-12:00	Break				
12:00-13:50	DiffDroid <i>by Anto Joseph</i>	Firmware Analysis Toolkit (FAT) <i>by Aditya Gupta</i>	.NET Security Guard <i>by Philippe Arteau</i>	BloodHound <i>by Andy Robbins</i>	CodexGigas Malware DNA Profiling Search Engine <i>by Luciano Martins + Rodrigo Cetera + Javier Bassi</i>
13:50-14:00	Break				
14:00-15:50	OWASP CSRFGuard <i>by Azzeddine RAMRAMI</i>	AMIRA: Automated Malware Incident Response and Analysis for MacOS <i>by Jakub (Kuba) Sendor</i>	APT2 - Automated Penetration Testing Toolkit <i>by Adam Compton + Austin Lane</i>	Fuzzing REST APIs with fuzzapi <i>by Abhijeth Dugginapeddi + Srinivas Kotipalli + Lalith Rallabhandi</i>	JTAGulator <i>by Joe Grand</i>
15:50-16:00	Break				
16:00-17:50	DeepViolet TLS/SSL Scanner <i>by Milton Smith</i>	Faraday <i>by Juan Pablo Daniel Borgna</i>	Nmap on Android <i>by Vlatko Kosturjak</i>	Needle <i>by Marco Lancini</i>	DataSploit <i>by Shubham Mittal + Nutan Kumar Panda</i>
17:00-18:30	Business Hall Welcome Reception // Mezzanine Level				

ARSENAL DAY 2

FRIDAY, NOVEMBER 4, 2016

Station	Business Hall // Mezzanine Level				
	Station 1	Station 2	Station 3	Station 4	Station 5
09:00-10:50	WarBerryPi <i>by Yiannis Ioannides</i>	Offense and Defense Toolkits in High/Low Frequency <i>by Haoqi Shan + Yunding Jian + Yang Qing</i>	Lynis <i>by Michael Boelen</i>	FakeNet-NG <i>by Peter Kacherginsky</i>	FLOSS <i>by Moritz Raabe</i>
10:50-11:00	Break				
11:00-12:50	OWASP ZAP <i>by Simon Bennetts</i>	Yaps <i>by Fabio Nigi</i>	Exploit Pack <i>by Juan Sacco</i>	Aktaion <i>by Joseph Zadeh + Rod Soto</i>	Automated Vulnerability Assessment & Penetration Testing Tool <i>by Shaan Mulchandani</i>
12:50-13:00	Break				
13:00-14:50	PowerMemory <i>by Pierre-Alexandre Braeken</i>	From XSS to RCE 2.5 <i>by Hans-Michael Varbaek</i>	HEATHEN Internet Of Things Pentesting Framework <i>by Chiheb Chebbi</i>	CROZONO Framework: Leveraging Autonomous Devices as an Attack Vector on Industrial Networks <i>by Sheila Ayelen Berta + Nicolas Villanueva</i>	AppMon: Runtime Security Testing & Profiling Framework for Native Apps <i>by Nishant Das Patnaik</i>
15:00-16:00	Arsenal Reception // Business Hall				

In partnership with:



Open to all pass types

Schedule as of October 24, 2016. Subject to Change

BUSINESS HALL PRESENTATIONS DAY 1				
THURSDAY, NOVEMBER 3, 2016				
Room	Business Hall Theater A		Business Hall Theater B	
	Session Title	Presented by	Session Title	Presented by
10:15-10:40	Is Your Organization's Confidential Information Secure?	NAVIGANT	Intrusion vs. Breach: Your Fate Will be Determined by Your Speed of Detection and Response	LogRhythm <small>The Security Intelligence Company</small>
10:55-11:20	Overwhelmed by Vulnerabilities? Keep Calm and Prioritize with Qualys	QUALYS <small>CONFIDENTIAL SECURITY</small>	Proactive Security: Building a Successful Threat Hunting Program	Raytheon <small>Foreground Security</small>
11:35-12:00	Teaching Machines Security: Attacking XOR Encryptions	CYLANCE	Accelerating Threat Hunting Maturity - From Adhoc to Advanced Machine Learning	splunk>
12:15-12:40	Hidden Information within Easy Reach - Threat Intelligence	eset <small>ENJOY SAFER TECHNOLOGY</small>	Surviving the Cyber-siege with Combined Security Prevention and Detection Solutions	napatech
12:55-13:20	The State of the IT Security Professional	InformationWeek DARKReading	Traditional AV is Dead? Real-time Machine-learning Detection of Modern Malware Downloads	TREND MICRO
13:35-14:00	Elastic Defense	SentinelOne	Watching Commodity Malware Get Sold to a Targeted Actor	cybereason
14:15-14:40	Ransomware Everywhere: Set Some Traps, it's Hunting Season	paloalto <small>NETWORKS</small>	Enabling Threat Hunting	CARBON BLACK <small>ARM YOUR ENDPOINTS</small>
14:55-15:20	Bridging the Gap Between Security and DevOps	VERACODE	HP Jet Advantage Security - Building Cyber Resiliency into Your Printer Fleet	hp
15:35-16:00	Fighting Organized Cybercrime - The Ransomware-as-a-Service Franchise	Check Point <small>SOFTWARE TECHNOLOGIES LTD</small>	European Trustworthy Privacy and Security Solutions for Cyberspace	elt Digital
16:15-16:40	The Myths and Truths to Building a World-Class Cyber Defense	leidos	How to Take the Next Step in Your IT Security Career	InformationWeek DARKReading

BUSINESS HALL PRESENTATIONS DAY 2

FRIDAY, NOVEMBER 4, 2016

Room	Business Hall Theater A		Business Hall Theater B	
	Session Title	Presented by	Session Title	Presented by
10:15-10:40	Choosing the Right Approach for a Targeted Attack	InformationWeek DARKReading	Anomali: Unburdening Threat Hunters by Operationalizing Threat Intelligence Data	ANOMALI
10:55-11:20	Lessons Learned from a Decade of Website Security Statistics	WhiteHat SECURITY	Bolstering Enterprise Security with a Crowdsourced Army of Elite Hackers	Synack
11:35-12:00	91% of Attacks Start with Email: Fix Your Human Firewall Flaws	mimecast	Machine Learning Use and Validation of Indicators of Compromise for Early Detection	TREND MICRO
12:15-12:40	HP Jet Advantage Security - Building Cyber Resiliency into Your Printer Fleet	hp		
12:55-13:20	Understanding Cybercrime	InformationWeek DARKReading		
13:35-14:00	Malvertising & Ransomware - Breaking the Attack Chain	malwarebytes		
14:15-14:40	Watching Commodity Malware Get Sold to a Targeted Actor	cybereason		
14:55-15:20	Teaching Machines Security: Attacking XOR Encryptions	CYLANCE		