BRIEFINGS DAY 1: OCTOBER 16

SCHEDULES

Room	1st Floor			
	E102	E104/E105	E106/E107	Elicium 1
07:30-18:00	Registration // Elicium Lobby - Ground Floor			
08:00-08:50	Continental Breakfast // **Europe Foyer - Ground Floor** // Sponsored by: paloalto networks eitas Reply			
08:50-09:00	Welcome & Introduction To Black Hat Europe 2014 // Elicium 1			
09:00-10:00	Keynote Speaker // Adi Shamir // Elicium 1			
10:00-10:15	Break			
10:15-11:15	Cellular Exploitation on a Global Scale: The Rise and Fall of the Control Protocol *Mathew Solnik*	Network Attached Shell: N.A.S.ty Systems that Store Network Accessible Shells *Jacob Holcomb*	APTs Way: Evading Your EBNIDS *Ali Abbasi + Jos Wetzels*	Bypassing HTTP Strict Transport Security *Jose Selvi*
11:15-11:45	Coffee Service // Sponsored by: endace FireEye Qualys VERACODE			
11:45-12:45	Quantified Self - A Path to Self-Enlightenment or Just a Security Nightmare? *Candid Wüest*	Man in the Binder: He Who Controls IPC, Controls the Droid *Nitay Artenstein + Idan Revivo*	Same Origin Method Execution (SOME) - Exploiting a Callback for Same Origin Policy Bypass *Ben Hayak*	Lights Off! The Darkness of the Smart Meters *Alberto Garcia Illera + Javier Vazquez Vidal*
12:45-14:15	Lunch Break			
14:15-15:15	Hacking the Wireless World with Software Defined Radio - 2.0 *Balint Seeber*	Scala Security: Examining the Play and LiftWeb Frameworks *Erik Cabetas + Paolo Soto*	A Practical Attack Against VDI Solutions *Dan Koretsky*	Quantum Key Distribution and the Future of Encryption *Konstantinos Karagiannis*
				Don't Trust Your USB! How to Find Bugs in USB Device Drivers *Sergej Schumilo + Ralf Spenneberg + Hendrik Schwartke*
15:15-15:30	Break			
15:30-16:30	Hide Android Applications in Images *Axelle Apvrille + Ange Albertini*	The Power of Pair: One Template that Reveals 100+ UAF IE Vulnerabilities *ChienHua Lu + Bo Qu*	Endrun - Secure Digital Communications for Our Modern Dystopia *Brendan O'Connor + Grant Dobbe*	Hack Your ATM with Friend's Raspberry.Py *Alexey Osipov + Olga Kochetova*
	Charge Your Device with the Latest Malware *André Pereira*			
16:30-17:00	Coffee Service // Sponsored by: endace FireEye Qualys VERACODE			
17:00-18:00	DTM Components: Shadow Keys to the ICS Kingdom *Alexander Bolshev + Gleb Cherbov*	Firmware.RE: Firmware Unpacking, Analysis and Vulnerability-Discovery as a Service *Jonas Zaddach*	Attacking the Linux PRNG on Android: Weaknesses in Seeding of Entropic Pools and Low Boot-Time Entropy *Sagi Kedmi*	Blended Web and Database Attacks on Real-Time, In-Memory Platforms *Juan Perez-Etchegoyen + Willis Vandevanter*
18:00-19:30	Business Hall Reception // Elicium 2 // Sponsored by: JUNIPER			

BRIEFINGS DAY 2: OCTOBER 17

SCHEDULES

Room	1st Floor				2nd Floor
	E102	E104/E105	E106/E107	Elicium 1	D203/D204
08:00-18:00	Registration // Elicium Lobby - Ground Floor				
08:00-09:00	Continental Breakfast // **Europe Foyer - Ground Floor** // Sponsored by: paloalto networks eitas Reply				
09:00-10:00	PDF Attack: A Journey from the Exploit Kit to the Shellcode *Jose Miguel Esparza*	Analyzing UEFI BIOSes from Attacker & Defender Viewpoints *Xeno Kovah*	Evasion of High-End IDPS Devices at the IPv6 Era *Antonios Atlasis + Enno Rey + Rafael Schaefer*	Two Factor Failure *Ryan Lackey*	
				SSL Validation Checking vs. Go(ing) to Fail *Thomas Brandstetter*	
10:00-10:15	Break				
10:15-11:15	PDF Attack: A Journey from the Exploit Kit to the Shellcode (continued) *Jose Miguel Esparza*	Lessons Learned from Eight Years of Breaking Hypervisors *Rafal Wojtczuk*	Session Identifier are for Now, Passwords are Forever - XSS-Based Abuse of Browser Password Managers *Sebastian Lekies + Ben Stock*	Gyrophone: Eavesdropping Using a Gyroscope *Gabi Nakibly + Yan Michalevsky*	Roundtable: Defense Post-Snowden moderated *Jeff Moss*
11:15-11:45	Coffee Service // Sponsored by: endace FireEye Qualys VERACODE				
11:45-12:45	Counterfeiting the Pipes with FakeNet 2.0 *Michael Sikorski + Andrew Honig*	A Journey to Protect Points-of-Sale *Nir Valtman*	Revisiting XSS Sanitization *Ashar Javed*	Android Kernel and OS Security Assessment with Iron Crow *Akhil Arora + Sumanth Naropanth*	
				WebKit Everywhere: Secure or Not? *Liang Chen*	
12:45-14:15	Lunch Break				
14:15-15:15	Counterfeiting the Pipes with FakeNet 2.0 (continued) *Michael Sikorski + Andrew Honig*	Abusing Software Defined Networks *Gregory Pickett*	Next Level Cheating and Leveling Up Mitigations *Joel St. John + Nicolas Guigo*	Bringing a Machete to the Amazon *Erik Peterson*	
15:15-15:30	Break				
15:30-16:30	Industrial Control Systems: Pentesting PLCs 101 *Arnaud Soullie*	Hadoop Security: Seven Ways to Kill an Elephant *Davi Ottenheimer*	C++11 Metaprogramming Applied to Software Obfuscation *Sebastien Andrivet*	Exploring Yosemite: Abusing Mac OS X 10.10 *Sung-ting Tsai + Ming-chieh Pan*	
16:30-17:00	Coffee Service // Sponsored by: endace FireEye Qualys VERACODE				
17:00-18:00	Industrial Control Systems : Pentesting PLCs 101 (continued) *Arnaud Soullie*	Freeze Drying for Capturing Environment-Sensitive Malware Alive *Yosuke Chubachi*	ret2dir: Deconstructing Kernel Isolation *Vasileios Kemerlis*	Reflected File Download - A New Web Attack Vector *Oren Hafif*	

LEGEND

	AppSec		Crypto		Embedded		Enterprise
	Exploit		Hardware		Malware		Mobile
	Network		Reverse Engineering		Roundtable		SCADA
	*NIX		Virtualization				