





































































































WED. JULY 31

07:00-17:00	REGISTRATION									
08:00-08:50	BREAKFAST Sponsored by  LOOKINGGLASS / Forum Ballroom									
ROOM	Roman II	Roman IV	Roman I / III	Palace II	Palace III	Augustus V / VI	Palace I	Augustus I / II	Augustus III / IV	
08:50-09:00	Welcome & Introduction to Black Hat USA 2013 / Augustus Ballroom									
09:00-10:00	Keynote Speaker: General Keith B. Alexander / Augustus Ballroom									
10:00-10:15	Break									
10:15-11:15	Mainframes: The Past Will Come to Haunt You (Philip Young) 	BlackberryOS 10 From a Security Perspective (Ralf-Philipp Weinmann)  	With BIGDATA comes BIG responsibility: Practical exploiting of MDX injections (Dmitry Chastuhin) 	New Trends in FastFlux Networks (Wei Xu + Xinran Wang)  CrowdSource: An Open Source, Crowd Trained Machine Learning Model for Malware Detection (Joshua Saxe) 	Lessons from Surviving a 300Gbps Denial of Service Attack (Matthew Prince)  	Combating the Insider Threat at the FBI: Real-world Lessons Learned (Patrick Reidy) 	Beyond the Application: Cellular Privacy Regulatory Space (Christie Dudley)    Legal Considerations for Cellular Research (Marcia Hofmann)   	Java Every-Days: Exploiting Software Running on Three Billion Devices (Brian Gorenc + Jasiel Spellman)  	How to Build a SpyPhone (Kevin McNamee)  	
11:15-11:45	Coffee Service Sponsored by  / Octavius Ballroom									
11:45-12:45	Black-box Assessment of Pseudorandom Algorithms (Derek Soeder + Christopher Abad + Gabriel Acevedo)   	Shattering Illusions in Lock-Free Worlds: Compiler/Hardware Behaviors in OSes and VMs (Marc Blanchou)  Password Hashing: The Future is Now (JP Aumasson)  	Power Analysis Attacks for Cheapskates (Colin O'Flynn)  	Denying Service to DDoS Protection Services (Allison Nixon)  Denial of Service as a Service - Asymmetrical Warfare at its Finest (Robert Masse) 	What Security Researchers Need to Know About Anti-Hacking Law (Marcia Hofmann) 	Just-In-Time Code Reuse: The More Things Change, the More They Stay the Same (Kevin Snow + Lucas Davi)  	A Tale of One Software Bypass of Windows 8 Secure Boot (Yuriy Buligin + Oleksandr Bazhaniuk + Andrew Furtak)  	TLS 'Secrets' (NextGen\$)  	Million Browser Botnet (Jeremiah Grossman + Matt Johansen)  	
12:45-14:15	Lunch Sponsored by  QUALYS / Forum Ballroom									
14:15-15:15	End-to-end Analysis of Domain Generating Algorithm Malware Family (Jason Geffner) 	Pass the Hash and Other Credential Theft and Reuse: Mitigating the risk of Lateral Movement and Privilege Escalation (Mark Simos + Patrick Jungles)  	Flying In the Dark - All the Things Not to Do When Hacking Hardware (Matthew Watchinski) 	Universal DDoS Mitigation Bypass (Tony Miu + Albert Hui + Wai Leng)  	Legal Aspects of Full-spectrum Computer Network (Active) Defense (Robert Clark) 	BIOS Security (John Butterworth + Corey Kallenberg + Xeno Kovah)  	I Can Hear You Now: Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell (Tom Ritter + Doug DePerry + Andrew Rahimi) 	Lawful Access Panel (Matt Blaze & Brewster Kahle & Jennifer Valentino-DeVries & Alan Davidson)	Evading Deep Inspection for Fun and Shell (Opi Niemi + Antti Levomäki)  	
15:15-15:30	Break									
15:30-16:30	JavaScript Static Security Analysis Made Easy with JSPrime (Nishant Das Patnaik + Sarathi Sabyasachi Sahoo)  	How to grow a TREE (Taint-Enabled Reverse Engineering Environment) from a CBASS (Cross-platform Binary Automated Symbolic-execution System) (Nathan Li + Loc Nguyen + Xing Li + James Just)  	Maltego Tungsten As a Collaborative Attack Platform (Roelof Temmingh + Andrew MacPherson) 	Untwining Twine (Jon Chittenden + Anson Gomes)  LTE Booms with Vulnerabilities (Ankit Gupta)   	A Practical Attack Against MDM Solutions (Daniel Brodie + Michael Shaulov)  	TOR... ALL-THE-THINGS! (Jason Geffner)    Truncating TLS Sessions to Violate Beliefs (Ben Smyth + Alfredo Pironti)   	Buying into the Bias: Why Vulnerability Statistics Suck (Jericho + Steve Christey) 	Clickjacking Revisited: A Perceptual View of UI Security (Devdatta Akhawe)   OPSEC Failures of Spies (Matthew Cole) 	Let's Get Physical: Breaking Home Security Systems and Bypassing Building Controls (Drew Porter + Stephen Smith)   	
16:30-17:00	Coffee Service Sponsored by  CISCO / Octavius Ballroom									
17:00-18:00	The Web IS Vulnerable: XSS Defense on the BattleFront (Greg Wroblewski + Ryan Barnett)   Malicious File for Exploiting Forensic Software (Takahiro Haruyama + Hiroshi Suzuki)   	Predicting Susceptibility to Socialbots on Twitter (Chris Sumner + Randall Wald) 	BinaryPig - Scalable Malware Analytics in Hadoop (Zachary Hanif + Telvis Calhoun + Jason Trost) 	Smashing the Font Scaler Engine in Windows Kernel (Ling Chuan Lee + Lee Yee Chan)  	Pixel-Perfect Timing Attacks with HTML5 (Paul Stone) 	Hacking, Surveilling, and Deceiving Victims on Smart TV (SeungJin 'Beist' Lee)  	How CVSS is DOSSing Your Patching Policy (and wasting your money) (Luca Allodi + Fabio Massacci) 	Hiding @ Depth - Exploring, Subverting, and Breaking NAND Flash Memory (Josh 'mOnk' Thomas)  	Mactans: Injecting Malware Into iOS Devices via Malicious Chargers (Billy Lau + Yeongjin Jang + Chengyu Song)   	
17:30-19:00	Sponsor Hall Reception Sponsored by: Diamond, Platinum Plus, Platinum Sponsors / Octavius Ballroom									
18:30-19:30	PWNIE Awards / Augustus III/IV									

KEY:  AppSec  DDoS  Malware  Cellular  Hardware/Low Level  Social  Mobile  SCADA/ICS  Network  Defense  Exploit Development  Management  Crypto  Consumer




















































































WED. JULY 31

Workshops			Sponsored Workshops			Arsenal Presentations		
ROOM	Pompeian	Florentine	Milano Ballroom VII	Milano Ballroom VIII	Milano Ballroom III	Milano Ballroom		
10:15-11:15	Practical Pentesting of ERPs and Business Applications <i>(Alexander Polyakov + Alexey Tyurin)</i> 	Methodologies of Hacking Embedded Security Appliances <i>(Rob Bathurst + Mark Carey)</i> 	Wireless Penetration Testing with the Pwn Pad <i>Sponsored by: Pwnie Express</i>	Defense Evasion Modeling – Bypassing the Cyber Kill Chain: What's Getting Past Your Layered Security? <i>Sponsored by: NSS Labs</i>	How to Avoid Becoming the Next Watering Hole <i>Sponsored by: RiskIQ</i>	ThreadFix <i>by Dan Cornell</i>		
11:15-11:45			Coffee/Refreshments Break - Sponsored Workshop & Arsenal Reception Room					Xenotix xBOT <i>by Ajin Abraham</i>
11:45-12:45			How to Pentest 1000 Branch Offices <i>Sponsored by: Pwnie Express</i>	Defense Evasion Modeling – Bypassing the Cyber Kill Chain: Tracking & Understanding Modern Malware & Exploits <i>Sponsored by: NSS Labs</i>	Demystifying Mobile Application Security: Improve Your Approach to Blacklisting Apps <i>Sponsored by: RiskIQ</i>	SocialKlepto <i>by Jason Ding</i>		
12:45-14:15	Lunch		Lunch/Learn Mixer - Sponsored Workshop & Arsenal Reception Room <i>Sponsored by: NSS Labs, RiskIQ</i>					
14:15-15:15	Embedded Devices Security and Firmware RE <i>(Jonas Zaddach + Andrei Costin)</i> 	PDF Attack: A Journey from the Exploit Kit to the Shellcode <i>(Jose Miguel Esparza)</i> 	The Spikes Challenge: Solving the Browser Malware Epidemic <i>Sponsored by: Spikes</i>	The Hangover Cyber Espionage Report – Tools, Tactics and Tracking <i>Sponsored by: Norman Shark</i>	“Kaizen” a CTF <i>Sponsored by: Booz Allen Hamilton</i>	iMAS - iOS Mobile Application Security Libraries <i>by Gregg Ganley</i>		
15:15-15:30			Coffee/Refreshments Break - Sponsored Workshop & Arsenal Reception Room					Vscan <i>by Federico Massa</i>
15:30-16:30				The Spikes Challenge: Solving the Browser Malware Epidemic <i>Sponsored by: Spikes</i>	The Hangover Cyber Espionage Report – Tools, Tactics and Tracking <i>Sponsored by: Norman Shark</i>	“Kaizen” a CTF <i>Sponsored by: Booz Allen Hamilton</i>	ShellNoob <i>by Yanick Fratantonio</i>	
16:30-18:00	17:00-18:00 To be Announced		Afternoon Mixer - Sponsored Workshop & Arsenal Reception Room <i>Sponsored by: NSS Labs, RiskIQ, Norman's SHARK, Spikes</i>				Dude, WTF in My Car? <i>By Alberto Garcia Illera + Javier Vazquez Vidal</i>	

Arsenal								
Milano Ballroom					Milano Ballroom			
	Station 1	Station 2	Station 3	Station 4	Station 5	Station 6	Station 7	Station 8
10:00-12:30	OSfooler: Remote OS Fingerprinting is Over <i>by Jaime Sanchez</i>	WebVerify <i>by Luis Antonio Rosales Marco</i>	RAFT 3 <i>by Gregory Fleischer + Nathan Hamiel</i>	PyPTP <i>by Matthew Bergin</i>	Smartphone Pentest Framework <i>by Georgia Weidman</i>	FSFlow <i>by Pat McCoy</i>	ShellNoob <i>by Yanick Fratantonio</i>	Vscan <i>by Federico Massa</i>
12:30-12:45	Break							
12:45-15:15	JMSDigger <i>by Gursev Singh Kalra</i>	ThreadFix <i>by Dan Cornell</i>	Lair <i>by Tom Steele</i>	The Cat's Meow <i>by Taylor Pennington</i>	ThunderCell <i>by Georgia Weidman</i>	Dude, WTF in My Car? <i>by Alberto Garcia Illera + Javier Vazquez Vidal</i>	Automated Electromechanical PIN Cracking: R2B2 and C3B0 <i>by Justin Engler</i>	Xenotix xBOT <i>by Ajin Abraham</i>
15:15-15:30	Break							






KEY:  AppSec  DDoS  Malware  Cellular  Hardware/Low Level  Social  Mobile  SCADA/ICS  Network  Defense  Exploit Development  Management  Crypto  Consumer

THU. AUGUST 1

08:00-08:50	BREAKFAST sponsored by ACCUANT / Forum Ballroom								
08:30-16:00	REGISTRATION								
ROOM	Roman II	Roman IV	Roman I / III	Palace II	Palace III	Augustus V / VI	Palace I	Augustus I / II	Augustus III / IV
09:00-10:00	Keynote Speaker: Brian Muirhead / Augustus Ballroom								
10:00-10:15	Break								
10:15-11:15	<p>CMX: IEEE Clean File Metadata Exchange (Mark Kennedy + Igor Muttik)</p>  	<p>Pass-the-Hash 2: The Admin's Revenge (Skip Duckwall)</p>  	<p>Abusing Web APIs Through Scripted Android Applications (Daniel Peck)</p>  	<p>The SCADA That Didn't Cry Wolf - Who's Really Attacking Your ICS Devices - Part Deux! (Kyle Wilhoit)</p>  	<p>Mobile Rootkits: Exploiting and Rootkiting ARM TrustZone (Thomas Roth)</p>  	<p>Fully Arbitrary 802.3 Packet Injection: Maximizing the Ethernet Attack Surface (Andrea Barisani + Daniele Bianco)</p> 	<p>Bluetooth Smart: The Good, the Bad, the Ugly, and the Fix! (Mike Ryan)</p>  	<p>Honey, I'm Home!! - Hacking Z-Wave Home Automation Systems (Behrang Fouladi + Sahand Ghanoun)</p>  	<p>The Factoring Dead: Preparing for Cryptocalypse (Alex Stamos + Thomas Ptacek + Tom Ritter)</p>  
	<p>Mobile Malware: Why the Traditional AV Paradigm is Doomed, and How to Use Physics to Detect Undesirable Routines (Guy Stewart)</p> 		<p>Big Data for Web Application Security (Mike Arpaia + Kyle Barry)</p> 						
11:15-11:45	Coffee Service Sponsored by :#LogRhythm / Octavius Ballroom								
11:45-12:45	<p>Bochspwn: Identifying 0-Days via System-Wide Memory Access Pattern Analysis (Mateusz 'j00ru' Jurczyk + Gynvael Coldwind)</p>  	<p>Energy Fraud and Orchestrated Blackouts: Issues with Wireless Metering Protocols (wM-Bus) (Cyrill Brunschweiler)</p>   	<p>Dissecting CSRF Attacks and Countermeasures (Mike Shema + Sergey Shekhan + Vaagn Toukharian)</p>  	<p>Hunting the Shadows: In-Depth Analysis of Escalated APT Attacks (Fyodor Yarochikin + Jeremy 'Birdman' Chiu + Tsung Pei Kan + Benson Wu)</p> 	<p>The Outer Limits: Hacking The Samsung Smart TV (Aaron Grattafiori + Josh Yavor)</p>  	<p>Revealing Embedded Fingerprints: Deriving Intelligence from USB Stack Interactions (Andy Davis)</p> 	<p>UART THOU MAD? (Toby Kohlenberg + Mickey Shkatov)</p> 	<p>Android: One Root to Own Them All (Jeff Forristal)</p> 	<p>Stepping p3wns: Adventures in Full Spectrum Embedded Exploitation (Ang Cui + Michael Costello + Salvatore Stolfo)</p>  
12:45-14:15	Lunch Sponsored by Microsoft / Forum Ballroom								
14:15-15:15	<p>Using Online Activity as Digital Fingerprints to Create a Better Spear Phisher (Joaquim Espinhara + Ulisses Albuquerque)</p> 	<p>Hot Knives Through Butter: Bypassing Automated Analysis Systems (Abhishek Singh + Zheng Bu)</p> 	<p>Above My Pay Grade: Cyber Response at the National Level (Jason Healey)</p> 	<p>' UNION SELECT 'This_Talk' AS ('New Optimization and Obfuscation Techniques')%00 (Roberto Salgado)</p>  	<p>Out of Control: Demonstrating SCADA Device Exploitation (Brian Meixell)</p> 	<p>Funderbolt: Adventures in Thunderbolt DMA Attacks (Russ Sevinsky)</p>  	<p>Press ROOT to Continue: Detecting OSX and Windows Bootkits with RDFU (Mario Vuksan + Tomislav Pericin)</p>  	<p>What's on the Wire? - Physical Layer Tapping with Project Daisho (Dominic Spill + Michael Ossmann + Michael 'Dragorn' Kershaw)</p>  	<p>Implantable Medical Devices: Hacking Humans (Barnaby Jack)</p>  
15:15-15:30	Break								
15:30-16:30	<p>CreepyDOL: Cheap, Distributed Stalking (Brendan O'Connor)</p> 	<p>Post Exploitation Operations with Cloud Synchronization Services (Jake Williams)</p>  	<p>Virtual Deobfuscator - A DARPA Cyber Fast Track Funded Effort (Jason Raber)</p>  	<p>Is that a Government in Your Network or are you Just Happy to See Me? (Eric Fiterman)</p>  	<p>Compromising Industrial Facilities from 40 Miles Away (Lucas Apa + Carlos Penagos)</p> 	<p>RFID Hacking: Live Free or RFID Hard (Fran Brown)</p>   	<p>SSL, Gone in 30 Seconds - A BREACH beyond CRIME (Angelo Prado + Neal Harris + Yoel Gluck)</p>  	<p>Exploiting Network Surveillance Cameras Like a Hollywood Hacker (Craig Heffner)</p>  	<p>Rooting SIM Cards (Karsten Nohl)</p>  
16:30-17:00	Ice Cream Social Sponsored by [TV] / Octavius Ballroom								
17:00-18:00	<p>OptiROP: Hunting for ROP Gadgets in Style (Nguyen Anh Quynh)</p>   	<p>Defending Networks With Incomplete Information: A Machine Learning Approach (Alexandre Pinto) (Aaron Grattafiori + Josh Yavor)</p> 	<p>Teridian SoC Exploitation: Exploration of Harvard Architecture Smart Grid Systems (Josh 'm0nk' Thomas + Nathan Keltner)</p>  	<p>Bugalyze.com - Detecting bugs using decompilation and data flow analysis (Silvio Cesare)</p>  	<p>Hacking Like in the Movies: Visualizing Page Tables for Local Exploitation (Georg '0x0ff' Wicherski + Alexandru Radocea)</p>  	<p>Home Invasion v2.0 - Attacking Network-Controlled Hardware (Daniel Crowley + David Bryan + Jennifer Savage)</p>  	<p>Multiplexed Wired Attack Surfaces (Michael Ossmann + Kyle 'Kos' Osborn)</p>   	<p>Owning the Routing Table - Part II (Gabi Nakibly)</p>  	<p>Spy-jacking the Booters (Brian Krebs + Lance James)</p> 

KEY:  AppSec  DDoS  Malware  Cellular  Hardware/Low Level  Social  Mobile  SCADA/ICS  Network  Defense  Exploit Development  Management  Crypto  Consumer

THU. AUGUST 1

Workshops			Arsenal Presentations	
ROOM	Pompeian	Florentine	Milano Ballroom	
10:15-11:15	DO-IT-YOURSELF CELLULAR IDS <i>(Sherri Davidoff + David Harrison +Scott Fretheim)</i> 	Mo' Malware, Mo' Problems - Cuckoo Sandbox to the Rescue <i>(Jurriaan Bremer + Claudio Guarnieri + Mark Schloesser)</i>  	Mandiant Redline <i>by Theodore Wilson</i>	
11:15-11:45			Drozer (formerly known as Mercury) <i>by Tyrone Erasmus + Daniel Bradberry</i>	
11:45-12:45			Break	
	Social-Engineer Toolkit <i>by David Kennedy</i>			
			ModSecurity <i>by Ryan Barnett</i>	
12:45-14:15	Lunch			
14:15-15:15	Network Forensics Sudden Death Workshop <i>(Scott Fretheim + Jonathan Neff)</i> 	JTAGulator: Assisted Discovery of On-Chip Debug Interfaces <i>(Joe Grand)</i> 	Viproxy VoIP Penetration and Exploitation Testing Kit <i>by Fatih Ozavci</i>	
			Armitage - A Scriptable Red Team Collaboration Tool <i>by Raphael Mudge</i>	
15:15-15:30			Break	
15:30-18:00			Smartphone Pentest Framework <i>by Georgia Weidman</i>	
			PHPMap <i>by Matthew Bergin</i>	

Arsenal								
Milano Ballroom					Milano Ballroom			
	Station 1	Station 2	Station 3	Station 4	Station 5	Station 6	Station 7	Station 8
10:00-12:30	Ice-hole by Darren Manners	Armitage - A Scriptable Red Team Collaboration Tool by Raphael Mudge	Information Disclosure in Facebook Graph Api with A.T.H.O.S by Michael Hudson	Binfuzz.js by Artem Dinaburg	HTExploit by Matias Katz	Invoke-ReflectivePELoader PowerShell Script by Joe Bialek	iocwriter_11 by William Gibb	WATOB0 by Andreas Schmidt
12:30-12:45	Break							
12:45-15:15	Sphere of Influence 3.2 by Darren Manners	Social-Engineer Toolkit by David Kennedy	Vega by David Mirza Ahmad	Dependency-Check by Jeremy Long	Drozer (formerly known as Mercury) by Tyrone Erasmus + Daniel Bradberry	IMAS - iOS Mobile Application Security Libraries by Gregg Ganley	Mandiant Redline by Theodore Wilson	OWASP Broken Web Applications VM by Chuck Willis
15:15-15:30	Break							