blackhat USA 2016

blackhat USA 2016

BRIEFINGS DAY 1 WEDNESDAY, AUGUST 3, 2016

BRIEFINGS DAY 1 WEDNESDAY, AUGUST 3, 2016

	Level 2					Level 3				
Room	**Lagoon K**	**Mandalay Bay BCD**	**Mandalay Bay EF**	**Mandalay Bay GH**		**Jasmine Ballroom**	**South Seas ABE**	**South Seas CDF**	**South Seas GH**	**South Seas IJ**
06:30-19:00	**Registration // Black Hat Blvd, Level 2**									
08:00-08:50	**Breakfast // Shoreline B, Level 2** *Sponsored by:* QUALYS									
08:50-09:00	**Welcome & Introduction to Black Hat USA 2016 // Oceanside Ballroom, Level 2**									
09:00-10:00	**Keynote Speaker // Dan Kaminsky // Oceanside Ballroom, Level 2**									
10:00-10:20	**Coffee Service // Level 2, 3, Business Hall - Microsoft Networking Lounge** *Sponsored by:* tenable network security									
10:20-11:10	**Abusing Bleeding Edge Web Standards for AppSec Glory** *by Bryant Zadegan + Ryan Lester*	**Breaking Payment Points of Interaction (POI)** *by Nir Valtman + Patrick Watson*	**The Linux Kernel Hidden Inside Windows 10** *by Alex Ionescu*	**Beyond the MCSE: Active Directory for the Security Professional** *by Sean Metcalf*		**Capturing 0day Exploits with PERFectly Placed Hardware Traps** *by Cody Pierce + Matt Spisak + Kenneth Fitch*	**HTTP/2 & QUIC - Teaching Good Protocols To Do Bad Things** *by Catherine Pearce + Carl Vincent*	**Can You Trust Me Now? An Exploration into the Mobile Threat Landscape** *by Josh Thomas + Shawn Moyer*	**A Retrospective on the Use of Export Cryptography** *by David Adrian*	**Augmenting Static Analysis Using Pintool: Ablation** *by Paul Mehta*
11:10-11:30	**Coffee Service // Level 2, 3, Business Hall - Microsoft Networking Lounge** *Sponsored by:* LogRhythm The Security Intelligence Company									
11:30-12:20	**Hackproofing Oracle eBusiness Suite** *by David Litchfield*	**Memory Forensics Using Virtual Machine Introspection for Cloud Computing** *by Tobias Zillner*	**$hell on Earth: From Browser to System Compromise** *by Matt Molinyawe + Jasiel Spelman + Abdul-Aziz Hariri + Joshua Smith*	**Subverting Apple Graphics: Practical Approaches to Remotely Gaining Root** *by Liang Chen + Qidan He + Marco Grassi + Yubin Fu*		**A Journey from JNDI/LDAP Manipulation to Remote Code Execution Dream Land** *by Alvaro Munoz + Oleksandr Mirosh*	**Exploiting Curiosity and Context: How to Make People Click on a Dangerous Link Despite Their Security Awareness** *by Zinaida Benenson*	**Applied Machine Learning for Data Exfil and Other Fun Topics** *by Matt Wolff + Brian Wallace + Xuan Zhao*	**Measuring Adversary Costs to Exploit Commercial Software: The Government-Bootstrapped Non-Profit C.I.T.L.** *by Mudge + Sarah Zatko*	**Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS** *by Sean Devlin + Hanno Böck + Aaron Zauner*
12:20-13:50	**Lunch Break // Shoreline B, Level 2** *Sponsored by:* FireEye SECURITY REIMAGINED									
13:50-14:40	**Drone Attacks on Industrial Wireless: A New Front in Cyber Security** *by Jeff Melrose*	**Towards a Holistic Approach in Building Intelligence to Fight Crimeware** *by Dhia Mahjoub + Mykhailo Sakaly + Thomas Mathew*	**Secure Penetration Testing Operations: Demonstrated Weaknesses in Learning Material and Tools** *by Wesley McGrew*	**Xenpwn: Breaking Paravirtualized Devices** *by Felix Wilhelm*		**Adaptive Kernel Live Patching: An Open Collaborative Effort to Ameliorate Android N-Day Root Exploits** *by Yulong Zhang + Tao Wei*	**HEIST: HTTP Encrypted Information can be Stolen Through TCP-Windows** *by Tom Van Goethem + Mathy Vanhoef*	**CANSPY: A Platform for Auditing CAN Devices** *by Jonathan-Christofer Demay + Arnaud Lebrun*	**GATTacking Bluetooth Smart Devices - Introducing a New BLE Proxy Tool** *by Slawomir Jasek*	**Certificate Bypass: Hiding and Executing Malware from a Digitally Signed Executable** *by Tom Nipravsky*

LEGEND

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

	Level 2					Level 3				
Room	Lagoon K	Mandalay Bay BCD	Mandalay Bay EF	Mandalay Bay GH		Jasmine Ballroom	South Seas ABE	South Seas CDF	South Seas GH	South Seas IJ
14:40-15:00	Break									
15:00-15:50	**An Insiders Guide to Cyber-Insurance and Security Guarantees** *by Jeremiah Grossman*	**Pwning Your Java Messaging with Deserialization Vulnerabilities** *by Matthias Kaiser*	**Does Dropping USB Drives in Parking Lots and Other Places Really Work?** *by Elie Bursztein*	**AMSI: How Windows 10 Plans to Stop Script-Based Attacks and How Well It Does It** *by Nikhil Mittal*		**Intra-Process Memory Protection for Applications on ARM and x86: Leveraging the ELF ABI** *by Sergey Bratus + Maxwell Koo + Julian Bangert*	**1000 Ways to Die in Mobile OAuth** *by Yuan Tian + Yutong Pei*	**Recover a RSA Private Key from a TLS Session with Perfect Forward Secrecy** *by Marco Ortisi*	**I Came to Drop Bombs: Auditing the Compression Algorithm Weapon Cache** *by Cara Marie*	**Into The Core - In-Depth Exploration of Windows 10 IoT Core** *by Paul Sabanal*
15:50-16:20	**Smoothie Social // Business Hall - Microsoft Networking Lounge // Bayside AB, Level 1** *Sponsored by:* ALIEN VAULT, CARBON BLACK ARM YOUR ENDPOINTS, CISCO, CITRIX, CROWDSTRIKE, CYLANCE									
16:20-17:10	**Design Approaches for Security Automation** *by Peleus Uhley*	**Crippling HTTPS with Unholy PAC** *by Itzik Kotler + Amit Klein*	**Access Keys Will Kill You Before You Kill the Password** *by Loic Simon*	**Account Jumping, Post Infection Persistency & Lateral Movement in AWS** *by Dan Amiga + Dor Knafo*		**Captain Hook: Pirating AVs to Bypass Exploit Mitigations** *by Udi Yavo + Tomer Bitton*	**Using EMET to Disable EMET** *by Abdulellah Alsaheel + Raghav Pande*	**Viral Video - Exploiting SSRF in Video Converters** *by Nikolay Ermishkin + Maxim Andreev*	**GreatFET: Making GoodFET Great Again** *by Michael Ossmann*	**Breaking Kernel Address Space Layout Randomization (KASLR) with Intel TSX** *by Yeongjin Jang + Sangho Lee + Taesoo Kim*
17:10-17:30	**Networking Break // Business Hall // Bayside AB, Level 1** *Sponsored by:* CloudPassage, CODE42, CORE SECURITY, DARKMATTER, f5, IBM									
17:30-18:00	**Watching Commodity Malware Get Sold to a Targeted Actor** *by Israel Barak*	**Building a Product Security Incident Response Team: Learnings from the Hivemind** *by Kymberlee Price*	**Unleash the Infection Monkey: A Modern Alternative to Pen-Tests** *by Ofri Ziv*	**Security Through Design - Making Security Better by Designing for People** *by Jelle Niemantsverdriet*		**Brute-Forcing Lockdown Harddrive PIN Codes** *by Colin O'Flynn*	**Cyber War in Perspective: Analysis from the Crisis in Ukraine** *by Kenneth Geers*	**Side-Channel Attacks on Everyday Applications** *by Taylor Hornby*	**AVLeak: Fingerprinting Antivirus Emulators for Advanced Malware Evasion** *by Alexei Bulazel*	**The Risk from Power Lines: How to Sniff the G3 and Prime Data and Detect the Interfere Attack** *by Lei Ji*
17:30-19:00	**Business Hall Reception Bayside AB, Level 1** *Sponsored by:* ALIEN VAULT, CARBON BLACK ARM YOUR ENDPOINTS, CISCO, CITRIX, CROWDSTRIKE, CYLANCE, DIGITAL GUARDIAN, Fidelis Cybersecurity, FireEye SECURITY REIMAGINED, FORCEPOINT FORTINET, Hewlett Packard Enterprise, LOCKHEED MARTIN, LogRhythm The Security Intelligence Company, paloalto NETWORKS, QUALYS CONTINUOUS SECURITY, RSA, Symantec, tenable network security, WEBROOT Smarter Cybersecurity									
18:30-19:30	**Pwnie Awards // Mandalay Bay D, Level 2**									

BRIEFINGS DAY 2: THURSDAY, AUGUST 4, 2016

BRIEFINGS DAY 2: THURSDAY, AUGUST 4, 2016

Level 2						Level 3				
Room	Lagoon K	Mandalay Bay BCD	Mandalay Bay EF	Mandalay Bay GH		Jasmine Ballroom	South Seas ABE	South Seas CDF	South Seas GH	South Seas IJ
08:30-17:00	Registration // Black Hat Blvd, Level 2									
08:00-08:50	Breakfast // Shoreline B, Level 2 *Sponsored by:* FORCEPOINT									
09:00-09:25	**How to Build the Immune System for the Internet** *by Xiaodun Fang*	**A Lightbulb Worm?** *by Colin O'Flynn*	**BadTunnel: How Do I Get Big Brother Power?** *by Yang Yu*	**Dungeons, Dragons and Security** *by Tiphaine Romand Latapie*		**PINdemonium: A DBI-Based Generic Unpacker for Windows Executable** *by Sebastiano Mariani + Lorenzo Fontana*	**Samsung Pay: Tokenized Numbers, Flaws and Issues** *by Salvador Mendoza*	**Blunting the Phisher's Spear: A Risk-Based Approach for Defining User Training and Awarding Administrative Privileges** *by Arun Vishwanath*	**What's the DFIRence for ICS?** *by Chris Sistrunk + Josh Triplett*	**Keystone Engine: Next Generation Assembler Framework** *by Nguyen Anh Quynh*
09:25-09:45	Break									
09:45-10:35	**The Remote Malicious Butler Did It!** *by Tal Be'ery + Chaim Hoch*	**Ouroboros: Tearing Xen Hypervisor with the Snake** *by Shangcong Luan*	**TCP Injection Attacks in the Wild - A Large Scale Study** *by Gabi Nakibly*	**Advanced CAN Injection Techniques for Vehicle Networks** *by Charlie Miller + Chris Valasek*		**Understanding HL7 2.x Standards, Pen Testing, and Defending HL7 2.x Messages** *by Anirudh Duggal*	**The Art of Defense - How Vulnerabilities Help Shape Security Features and Mitigations in Android** *by Nick Kralevich*	**Windows 10 Segment Heap Internals** *by Mark Vincent Yason*	**Defense at Hyperscale: Technologies and Policies for a Defensible Cyberspace** *by Jason Healey*	**HTTP Cookie Hijacking in the Wild: Security and Privacy Implications** *by Suphannee Sivakorn + Jason Polakis*
10:35-11:00	Coffee Service // Level 2, 3, Business Hall - Microsoft Networking Lounge *Sponsored by:* Hewlett Packard Enterprise									
11:00-11:50	**Demystifying the Secure Enclave Processor** *by Tarjei Mandt + Mathew Solnik + David Wang*	**Next-Generation of Exploit Kit Detection by Building Simulated Obfuscators** *by Tongbo Luo + Xing Jin*	**Investigating DDOS - Architecture, Actors, and Attribution** *by Elliott Peterson + Andre Correa*	**Analysis of the Attack Surface of Windows 10 Virtualization-Based Security** *by Rafal Wojtczuk*		**O-checker: Detection of Malicious Documents Through Deviation from File Format Specifications** *by Yuhei Otsubo*	**Hacking Next-Gen ATMs: From Capture to Cashout** *by Weston Hecker*	**Language Properties of Phone Scammers: Cyberdefense at the Level of the Human** *by Judith Tabron*	**The Tao of Hardware, the Te of Implants** *by Joe FitzPatrick*	**Cunning with CNG: Soliciting Secrets from Schannel** *by Jake Kambic*
11:50-12:10	Break									
12:10-13:00	**Hardening AWS Environments and Automating Incident Response for AWS Compromises** *by Andrew Krug + Alex McCormack*	**badWPAD** *by Maxim Goncharov*	**When the Cops Come A-Knocking: Handling Technical Assistance Demands from Law Enforcement** *by Jennifer Granick + Riana Pfefferkorn*	**Windows 10 Mitigation Improvements** *by Matt Miller + David Weston*		**Discovering and Exploiting Novel Security Vulnerabilities in Apple ZeroConf** *by Luyi Xing + Xiaolong Bai*	**Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter** *by John Seymour + Philip Tully*	**Horse Pill: A New Type of Linux Rootkit** *by Michael Leibowitz*	**SGX Secure Enclaves in Practice: Security and Crypto Review** *by Jean-Philippe Aumasson + Luis Merino*	**AirBnBeware: Short Term Rentals, Long Term Pwnage** *by Jeremy Galloway*

black hat USA 2016 black hat USA 2016

BRIEFINGS DAY 2: THURSDAY, AUGUST 4, 2016

BRIEFINGS DAY 2: THURSDAY, AUGUST 4, 2016

	Level 2					Level 3				
Room	Lagoon K	Mandalay Bay BCD	Mandalay Bay EF	Mandalay Bay GH		Jasmine Ballroom	South Seas ABE	South Seas CDF	South Seas GH	South Seas IJ
13:00-14:30	**Lunch Break // Shoreline B, Level 2** *Sponsored by:* RSA									
14:30-15:20	**Iran's Soft-War for Internet Dominance** *by Claudio Guarnieri + Collin Anderson*	**The Year in Flash** *by Natalie Silvanovich*	**Bad for Enterprise: Attacking BYOD Enterprise Mobile Security Solutions** *by Vincent Tan*	**VOIP WARS: The Phreakers Awaken** *by Fatih Ozavci*		**OSS Security Maturity: Time to Put On Your Big Boy Pants!** *by Jake Kouns + Christine Gadsby*	**Web Application Firewalls: Analysis of Detection Logic** *by Vladimir Ivanov*	**Pangu 9 Internals** *by Tielei Wang + Hao Xu + Xiaobo Chen*	**Breaking FIDO: Are Exploits in There?** *by Jerrod Chong*	**PLC-Blaster: A Worm Living Solely in the PLC** *by Maik Bruggemann + Hendrik Schwartke + Ralf Spenneberg*
15:20-15:50	**Ice Cream Social // Business Hall - Microsoft Networking Lounge // Bayside AB, Level 1** *Sponsored by:* Digital Guardian, Fidelis Cybersecurity, Fortinet, Lockheed Martin, paloalto networks, Symantec, Webroot Smarter Cybersecurity									
15:50-16:40	**Breaking Hardware-Enforced Security with Hypervisors** *by Joseph Sharkey*	**The Beast Within - Evading Dynamic Malware Analysis Using Microsoft COM** *by Ralf Hund*	**When Governments Attack: State Sponsored Malware Attacks Against Activists, Lawyers, and Journalists** *by Cooper Quintin + Eva Galperin*	**Dark Side of the DNS Force** *by Erik Wu*		**The Art of Reverse Engineering Flash Exploits** *by Jeong Wook Oh*	**Using an Expanded Cyber Kill Chain Model to Increase Attack Resiliency** *by Sean Malone*	**Timing Attacks Have Never Been So Practical: Advanced Cross-Site Search Attacks** *by Nethanel Gelernter*	**DPTrace: Dual Purpose Trace for Exploitability Analysis of Program Crashes** *by Rodrigo Branco + Rohit Mothe*	**Crumbling the Supercookie, and Other Ways the FCC Protects Your Internet Traffic** *by Travis LeBlanc + Jonathan Mayer*
16:40-17:00	**Networking Break // Business Hall, Bayside AB, Level 1** *Sponsored by:* iboss Cybersecurity, Optiv, proofpoint, Raytheon Foreground Security, SentinelOne, tripwire									
17:00-18:00	**An AI Approach to Malware Similarity Analysis: Mapping the Malware Genome With a Deep Neural Network** *by Konstantin Berlin*	**An Inconvenient Trust: User Attitudes Toward Security and Usability Tradeoffs for Key-Directory Encryption Systems** *by Patrick Gage Kelley*	**Pay No Attention to That Hacker Behind the Curtain: A Look Inside the Black Hat Network** *by Neil Wyler + Bart Stump*	**Attacking SDN Infrastructure: Are We Ready for the Next-Gen Networking?** *by Changhoon Yoon + Seungsoo Lee*		**Over the Edge: Silently Owning Windows 10's Secure Browser** *by Erik Bosman + Cristiano Giuffrida*	**Using Undocumented CPU Behavior to See into Kernel Mode and Break KASLR in the Process** *by Anders Fogh + Daniel Gruss*	**Call Me: Gathering Threat Intelligence on Telephony Scams to Detect Fraud** *by Aude Marzuoli*	**Dangerous Hare: Hanging Attribute References Hazards Due to Vendor Customization** *by Nan Zhang*	**Building Trust & Enabling Innovation for Voice Enabled IoT** *by Lynn Terwoerds*

SCAN CODE

FOR ALL ABSTRACTS

https://www.blackhat.com/us-16/briefings.html

blackhat USA 2016

ARSENAL DAY 1 WEDNESDAY, AUGUST 3, 2016

ARSENAL DAY 1 WEDNESDAY, AUGUST 3, 2016

Open to all pass types

Open to all pass types

Station	Palm Foyer, Level 3										Station
	1	2	3	4	5	6	7	8	9	10	
08:00-08:50	Breakfast // Shoreline B, Level 2										08:00-08:50
10:00-11:50	**Needle** *by Marco Lancini*	**FakeNet-NG** *by Peter Kacherginsky*	**AVLInsight Mobile Threat Intelligence Platform** *by Tom Pan*	**Voyeur** *by Juan Garrido*	**FingerPrinTLS** *by Lee Brotherston*	**eXpose** *by Joshua Saxe*	**Android-InsecureBankv2** *by Dinesh Shetty*	**SimpleRisk** *by Josh Sokol*	**autoDANE** *by Dane Goodwin*	**Koodous** *by Francisco López + Fernando Denis Ramírez*	10:00-11:50
11:50-12:00	Break										11:50-12:00
12:00-13:50	**SIEMonster** *by Chris Rock*	**Web Service Security Assessment Tool (WSSAT)** *by Mehmet Yalcin YOLALAN + Salih TALAY*	**Enumall - The Ultimate Subdomain Tool** *by Jason Haddix + Leif Dreizler*	**Tintorera: Source Code Intelligence** *by Simon Roses*	**BinProxy** *by Ryan Koppenhaver*	**Burp Extension for Non-HTTP Traffic** *by Josh Summitt*	**Nishang: The Goodness of Offensive PowerShell** *by Nikhil Mittal*	**Brosec** *by Gabe Marshall*	**ShinoBOT** *by Shota Shinogi*	**AndroidTamer** *by Anant Shrivastava*	12:00-13:50
13:50-14:00	Break										13:50-14:00
14:00-15:50	**Dradis Framework** *by Daniel Martin*	**WATOBO - The Web Application TOol BOx** *by Andreas Schmidt*	**Certbot** *by Brad Warren*	**CodexGigas Malware DNA Profiling Search Engine** *by Luciano Martins + Rodrigo Cetera + Javier Bassi*	**SkyPhenomena** *by Zhang Lu + Li Fu + RenXu Ye*	**Accelerating Cyber Hunting, Project ASGARD** *by Joshua Patterson*	**WALB (Wireless Attack Launch Box)** *by Keiichi Horiai + Kazuhisa Shirakami*	**Kung Fu Malware** *by Pablo San Emeterio + Román Ramírez*	**Threat Scanner** *by Brian Codde*	**Highway to the Danger Drone** *by Francis Brown + David Latimer + Dan Petro*	14:00-15:50
15:50-16:00	Break										15:50-16:00
16:00-17:50	**Vulnreport - Pentesting Management and Automation** *by Tim Bach*	**Elastic Handler** *by David Cowen*	**myBFF** *by Kirk Hayes*	**.NET Security Guard** *by Philippe Arteau*	**CrackMapExec** *by Marcello Salvati*	**Rapid Bluetooth Low Energy Testing with BLE-replay and BLESuite** *by Greg Foringer + Taylor Trabun*	**pDNSego** *by Christian Heinrich + Mike Schiffman*	**HoneyPy & HoneyDB** *by Phillip Maddux*	**rastrea2r** *by Ismael Valenzuela*	**Visual Network and File Forensics Using Rudra** *by Ankur Tyagi*	16:00-17:50

In partnership with:

NETpeas (re)quest2secure

toolswatch HACKERS ARSENAL

Arsenal Theater					Wednesday, August 3, 2016
11:00-11:45	12:00-12:45	13:00-13:45	14:00-14:45	15:00-15:45	16:00-16:45
Highway to the Danger Drone *by Francis Brown + David Latimer + Dan Petro*	**FakeNet-NG** *by Peter Kacherginsky*	**CrackMapExec** *by Marcello Salvati*	**Aktaion** *by Joseph Zadeh + Rod Soto*	**ShinoBOT** *by Shota Shinogi*	**SIEMonster** *by Chris Rock*

black hat USA 2016

ARSENAL DAY 2 THURSDAY, AUGUST 4, 2016

ARSENAL DAY 2 THURSDAY, AUGUST 4, 2016

Open to all pass types

Open to all pass types

Station	Palm Foyer, Level 3					Palm Foyer, Level 3					Station
	1	2	3	4	5	6	7	8	9	10	
08:00-08:50	Breakfast // Shoreline B, Level 2										08:00-08:50
10:00-11:50	**Serpico** *by Willis Vandevanter + Peter Arzamendi*	**DataSploit** *by Shubham Mittal + Sudhanshu Chauhan + Nutan Kumar Panda*	**Automated Penetration Testing Toolkit (APT2)** *by Adam Compton*	**NetSec-Framework** *by Joshua Ewing*	**Maltego VirusTotal** *by Christian Heinrich + Karl Harnmore*	**Subgraph OS** *by David Mirza Ahmad*	**Maltese (Malware Traffic Emulating Software)** *by Sasi Siddharth*	**OBJECTIVE-SEE'S OS X SECURITY TOOLS** *by Patrick Wardle*	**LAMMA** *by Ajit Hatti*	**Scout2** *by Loic Simon*	10:00-11:50
11:50-12:00	Break										11:50-12:00
12:00-13:50	**FLOSS** *by Moritz Raabe*	**King Phisher** *by Spencer McIntyre*	**DET** *by Paul Amar*	**The Pappy Proxy** *by Rob Glew*	**BurpBUddy** *by Tom Steele*	**V3SPA: A Tool for Visually Analyzing and Diffing SELinux Security Policies** *by Robert Gove*	**AMIRA: Automated Malware Incident Response and Analysis** *by Jakub Sendor*	**Otaku** *by Yoshinori Matsumoto*	**BSOD HD: An FPGA-Based HDMI Injection and Capture Tool** *by Joe Grand + Zoz Brooks*	**Cuckoodroid 2.0** *by Idan Revivo*	12:00-13:50
13:50-14:00	Break										13:50-14:00
14:00-15:50	**gopassivedns** *by Philip Martin*	**CAN Badger** *by Javier Vazquez Vidal + Henrik Ferdinand Noelscher*	**ThreadFix** *by Dan Cornell*	**AppMon** *by Nishant Das Pattanaik*	**Droid-FF: Android Fuzzing Framework** *by Anto Joseph*	**NetNeedle** *by John Ventura*	**WarBerryPi Troops Deployment in Red Teaming Scenarios** *by Yiannis Ioannides*	**BloodHound** *by Andy Robbins*	**Ebowla** *by Travis Morrow*	**Faraday** *by Federico Kirshbaum*	14:00-15:50
15:50-16:00	Break										15:50-16:00
16:00-17:50	**NetDB - The Network Database Project** *by Bertin Bervis + James Jara*	**HL7deep** *by Michael Hudson*	**A Black Path Toward The Sun** *by Ben Lincoln*	**Rainmap lite** *by Paulino Calderon*	**Aktaion** *by Joseph Zadeh + Rod Soto*	**Halcyon** *by Sanoop Thomas*	**ChipWhisperer** *by Colin O'Flynn*	**LOG-MD** *by Michael Gough + Brian Boettcher*	**Browser Exploitation Framework (BeEF)** *by Christian Frichot*	**Shevirah** *by Georgia Weidman*	16:00-17:50
17:00-18:00	Arsenal Happy Hour										17:00-18:00

In partnership with:

NETpeas (re)quest2secure   toolswatch HACKERS ARSENAL

Arsenal Theater					Thursday, August 4, 2016
11:00-11:45	12:00-12:45	13:00-13:45	14:00-14:45	15:00-15:45	16:00-16:45
Faraday *by Federico Kirshbaum*	**CAN Badger** *by Javier Vazquez Vidal + Henrik Ferdinand Noelscher*	**Subgraph OS** *by David Mirza Ahmad*	**ChipWhisperer** *by Colin O'Flynn*	**BSOD HD: An FPGA-Based HDMI Injection and Capture Tool** *by Joe Grand + Zoz Brooks*	**WarBerryPi Troops Deployment in Red Teaming Scenarios** *by Yiannis Ioannides*

SPONSORED SESSIONS DAY 1 — WEDNESDAY, AUGUST 3, 2016

Open to all pass types

Room	Business Hall - Theater A	Business Hall - Theater B	Reef B
	Session Name / Sponsor	Session Name / Sponsor	Session Name / Sponsor
10:20-11:05	Activated Charcoal – Making Sense of Endpoint Data LogRhythm	Inside Out: Viewing Everyone and Everything as Potential Insider Threats Forcepoint	The Unbearable Lightness of Cyber Security Symantec
11:30-12:15	Overwhelmed by Security Vulnerabilities? Learn How to Prioritize Remediation Qualys	Cloud Changes Everything: Transforming Security for a Scalable, Adaptive Approach tenable network security	Hacking HTTP/2 - New Attacks on the Internets Next Generation Foundation Imperva
12:40-13:25	Developing and Evolving a Threat Intel Program RSA	Beyond Visibility: Collaborative and Actionable Threat Intelligence Fortinet	Cyber Hustles - Lessons Learned from Vegas and Film Arbor Networks
13:50-14:35	Using Analytic Tools to Find Data Breaches: Live Attack Scenarios Hewlett Packard Enterprise	Threat Intelligence Across the Enterprise: Providing a Holistic Security Solution Webroot	Two-Factor Isn't Enough - We Show You Why SecureAuth
15:00-15:45	Defeating Evasive Ransomware: How to Automate Prevention paloalto networks	Pneumonoultramicroscopicsilicovolcanoconiosis & the Threat of Sharing - Should You Share Threat Intelligence? Alien Vault	Interesting Eastern European Cyber-Crime Verisign
16:10-16:55	Prevention Requires Prediction and Visibility in a World of Exponential Devices Cylance	Ten Impossible Things You Can Do with the Right Metadata Fidelis Cybersecurity	91% of Attacks Start with Email: Fix Your Human Firewall Flaws mimecast

SPONSORED SESSIONS DAY 2 — THURSDAY, AUGUST 4, 2016

Open to all pass types

Room	Business Hall - Theater A	Business Hall - Theater B	Reef B
	Session Name / Sponsor	Session Name / Sponsor	Session Name / Sponsor
11:00-11:45	Hacked? Who Cares. You've Mitigated the Effects and You Know It FireEye	Enabling Threat Hunting Carbon Black	Validating Security by Faking It Verisign
12:10-12:55	Incident Responder's Field Guide - Lessons from a Fortune 100 Incident Responder Digital Guardian	Hacking Exposed: The Latest "Living Off The Land" Techniques CrowdStrike	Is Your Data Safe in SaaS, PaaS, and IaaS? skyhigh
13:20-14:05	Behind the Scenes of the Cyber Kill Chain - Revealing Our Greatest Network Defense Stories Lockheed Martin	Driving Global Interdiction Against Major Threat Actors Cisco	Understanding Intel CET - What It Is, and Can You Wait? Check Point
14:30-15:15	TLS is No Longer Optional Citrix	An Innovative Approach to Combatting Ransomware CyberArk	Think Your Network is Safe? Check Your Printers hp
15:40-16:25	Enterprise Controlled Cloud Encryption and Key Management WinMagic Data Security	Threat Environment, Threat Approach, & Threat Mitigation AT&T	Network Virtualization to Enhance Visibility and Containment vmware

SPONSORED WORKSHOPS DAY 1 — WEDNESDAY, AUGUST 3, 2016

Open to all pass types

Room	Mandalay Bay J	Mandalay Bay K	Mandalay Bay L
	Session Name / Sponsor	Session Name / Sponsor	Session Name / Sponsor
10:20-11:10	Breaking the Machine Learning Hype Cycle MASERGY Performance Beyond Expectations	"Impossible is Just the Beginning": Achieving Total Security, Privacy, and Data Control for Government, Military, and Enterprise Communications Systems DARKMATTER GUARDED BY GENIUS	Kaizen Capture the Flag and Hacker Dojo Booz | Allen | Hamilton strategy and technology consultants
11:10-11:30	Break		
11:30-12:20	Building a Corporate Security Program from A to Z MASERGY Performance Beyond Expectations	Cyber Threats within the Middle East and Next Generation Initiatives DARKMATTER GUARDED BY GENIUS	Kaizen Capture the Flag and Hacker Dojo Booz | Allen | Hamilton strategy and technology consultants
12:20-13:50	Lunch		
13:50-14:40	Best Practices for Workload Security Moving to Cloud Environments CloudPassage	Crushing the DNSSEC Paradox When More Security Means More Vulnerability neustar	Kaizen Capture the Flag and Hacker Dojo Booz | Allen | Hamilton strategy and technology consultants
14:40-15:00	Break		
15:00-15:50	Best Practices for Workload Security Moving to Cloud Environments CloudPassage	Crushing the DNSSEC Paradox When More Security Means More Vulnerability neustar	Kaizen Capture the Flag and Hacker Dojo Booz | Allen | Hamilton strategy and technology consultants

SPONSORED WORKSHOPS DAY 2 — THURSDAY, AUGUST 4, 2016

Open to all pass types

Room	Mandalay Bay J	Mandalay Bay K	Mandalay Bay L
	Session Name / Sponsor	Session Name / Sponsor	Session Name / Sponsor
11:00-11:50	Pay Up...or Die! Investigating Advanced Ransomware in Hospitals leidos	Incident Response – Reverse Engineering the Wheel DARKMATTER GUARDED BY GENIUS	VMware NSX: Data Center Security Workshop vmware
11:50-12:10	Break		
12:10-13:00	Pay Up...or Die! Investigating Advanced Ransomware in Hospitals leidos	How to Teach a Hacker New Tricks DARKMATTER GUARDED BY GENIUS	VMware NSX: Data Center Security Workshop vmware
13:00-14:30	Lunch		
14:30-15:20	Healthcare Under Siege TRAPX SECURITY	Choosing the Right Vector for Online Attack InformationWeek DARKReading BOMGAR™	VMware NSX: Data Center Security Workshop vmware
15:20-15:40	Break		
15:40-16:30	Special Presentation: MEDJACK.2 Escalates Attacks on Healthcare Industry TRAPX SECURITY	Using Threat Intelligence to Improve Your Enterprise Defenses InformationWeek DARKReading TERBIUM LABS Data Intelligence	VMware NSX: Data Center Security Workshop vmware