★ THE WORLD'S LARGEST & MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING ★

SANS EMEA

EUROPEAN DFIR SUMMIT 2016 PRAGUE

9TH OCTOBER, 2016

SUMMIT AGENDA

CHAIR: JESS GARCIA

Sunday, 9 October	
9:00-9:45am	***Investigating Intrusions at Adversary Speed*** The speed at which an adversary can compromise a single host, pivot into your environment, and move laterally is astounding. It isn't uncommon to see the typical smash and grab operation take 15-30 minutes and compromise 10-20 hosts. An organization's ability to quickly respond is reliant on their ability to thoroughly investigate these occurrences. Proper measures cannot be taken without having a full understanding of what happened during that time. Traditional investigation methods are light years behind the speed and efficiency an attacker can move. This talk will discuss both tools (open source\commercial) and techniques for rapidly investigating intrusions at the scope and scale adversaries create them. ***Christopher Witter**, @mr_cwitter, Manager Falcon OverWatch, CrowdStrike*
9:45-10:30am	***iOS Forensics: Where Are We Now; And What Are We Missing?*** In the last two years several things have changed in the world of iOS forensics, both in terms of acquisition and in terms of analysis. The objective of this presentation is to provide an overview of the state of the art in terms of acquisition techniques and overcoming of the device's protection mechanisms, in particular the access code chosen by the user. In addition, the presentation aims to highlight what information we are missing by using the techniques and tools available on the market and what are the alternative paths we can use to overcome this problem. ***Mattia Epifani**, @mattiaep, Digital Forensics Specialist, REALITY NET Snc* ***Pasquale Stirparo**, @pstirparo, Cyber Threat Intelligence Analysist & Incident Responder, UBS*
10:00-10:20am	**Networking Break**
11:00-11:45am	***PowerShell obFUsk8tion Techniques & How To (Try To) D""e`Tec`T 'Th'+'em'*** The very best attackers hide their commands from A/V and application whitelisting technologies using encoded commands and memory-only payloads to evade detection. These techniques thwart Blue Teams from determining what was executed on a target system. However, network defenders are catching on, and state-of-the-art detection tools now monitor the command line arguments for powershell.exe either in real-time or from event logs. We need new avenues to remain stealthy in a target environment. So, this talk will highlight a dozen never-before-seen techniques for obfuscating PowerShell command line arguments. As an incident responder at Mandiant, I have seen attackers use a handful of these methods to evade basic command line detection mechanisms. I will share these techniques already being used in the wild so you can understand the value each technique provides the attacker. ***Daniel Bohannon**, @danielhbohannon, Consultant, Mandiant*
11:45am-12:15pm	***Digital Forensics: The Missing Piece of Internet of Things Promise*** Every new device we create, every sensor we deploy, every byte we synchronize to other locations will at some point come under scrutiny in the course of investigations and legal matters. Yet no reliable forensics applications nor digital forensics guidance exists to retrieve the data from IoT devices in the event of a cyber event, an active investigation or a litigation request. The digital forensics of internet of things (IoT) technologies is the missing conversation in our headlong rush to the promise of connecting every device on the planet. This presentation discuss about issues and importance of further development in this field and elaborates on how forensics practitioners, device manufacturers and legal authorities could share the efforts and minimise this gap. ***Dr. Ali Dehghantanha**, @alidehghantanha , Marie-Curie International Incoming Fellow in Cyber Forensics, University of Salford*
12:15-1:30pm	**Lunch**

Sunday, 9 October	
1:30-2:15pm	***Targeted SOC Use Cases for effective Incident Detection and Response*** SOC Use Cases are a tactical tool in the hands of SOC management, but their design and implementation must be framed into a strategic plan adopted to detect and respond to security incident across the organization. The two goals of our session are (a) to define a practical framework for Use Case design and implementation inside a SOC and (b) to present a threat centric methodology to build an organization's Use Case library. The proposed Use Case framework aims to provide SOC staff with a pragmatic, repeatable process that can be used to implement detection and response capabilities and to strengthen the SOC ability to leverage threat indicators for intelligence decision making. An effective Use Case library can be created starting from an attacker centric Threat Model specifically crafted for the organization. Once defined, the Threat Model can be used to derive a set of specific Attack Scenarios describing threat actors, their motives, their goals and the related actions to achieve them. Once Threat Actor actions have been documented, the technologies able to detect them can be identified ("detect" phase in the defensive course of action). With this information at hand, SOC Analysts and Content Engineers are better prepared to design Use Cases targeted for their organization instead of relying on generic and out-of-the-box detection rules and incident response procedures provided by security vendors. ***David Gray**, @D4VID_GRAY, Consultant, RSA Advanced Cyber Defense Practice EMEA* ***Angelo Perniola**, @AngeloPerniola, Senior Consultant, RSA Advanced Cyber Defense Practice EMEA*
2:15-3:00pm	***VolatilityBot*** Part of the work security researchers have to go through when they study new malware or wish to analyse suspicious executables is to extract the binary file and all the different satellite injections and strings decrypted during the malware's execution. Usually, this initial process is done manually, and it can be lengthy or even end up incomprehensible, in case some actions the malware has taken are not traced back to it. Enter VolatilityBot. This is a tool I have developed myself, leveraging the Volatility Framework. This new automation tool for researchers cuts all the guesswork and manual tasks out of the binary extraction phase. Not only does it automatically extract the executable (exe), but it also fetches all new processes created in memory, code injections, strings, IP addresses and so on. Beyond the obvious value of having a complete extraction automated and produced in under a minute, VolatilityBot is highly effective against a wide variety of malware codes and their respective load techniques. It can take on complex malware including banking trojans such as ZeuS, Ramnit, and Dyre, just as easily as it extracts payloads from downloaders such as Upatre and Pony, or even from targeted malware like Havex. Once VolatilityBot has finished the extraction, it can further automate repair or prepare the extracted elements for the next step in analysis – for example, by fixing the Portable Executable (PE), preparing for static analysis via tools like IDA, performing a YARA scan, etc. The Volatility Framework at the core of this automation tool is an open-source framework for memory analysis and forensics; it analyses the runtime state of a system using the data found in volatile storage (RAM). You can find out more about Volatility at **http://www.volatilityfoundation.org**. ***Martin Korman**, Incident Responder & Forensic Investigator, Team8*
3:00-3:30pm	**Networking Break**

Sunday, 9 October

3:30-4:15pm	***I Thought I Saw a |-|4><0.-*** Threat Hunting refers to proactively and iteratively searching through networks or datasets to detect and respond to advanced threats that evade traditional rule- or signature-based security solutions. But what does that really mean? And what real impact does it have on the security team? Can we use threat hunting provide a process to better detect and understand when you've been breached? More and more security data is being produced and usually aggregated into a central location or body to hopefully take quick and informed decisions on attacks or compromises amongst a mountain of data. When you start to include data gathered from your endpoints the amount of data starts to explode exponentially. This level of data provides us with a large amount of visibility. But is having visibility enough? What if a more thoughtful and intelligent way of generating alerts could draw an analyst attention to the right place at the right time? This would provide context or even provide a flag indicated suspicious behaviour that can become the starting point of a hunt. In this talk, we will explore this theory and establish working foundations of what threat hunting is and look at some of the challenges associated with gathering large data sets. This will give us a foundation to look at who we can improve and explore implementing an intelligent threat hunting model to drive the investigation process. ***Thomas V. Fischer**, @FVT, Global Security Advocate & Threat Researcher, Digital Guardian*
4:15-5:00pm	***How to Rock with DNS: Patterns for Detection and Faster Spotting of Malicious Activities*** DNS is one of the most important support services of IP-based networks: it is essential a vast amount services and applications, from surfing the web to connecting to a domain-controller or database server. From the defensive perspective, DNS provides a clear overview/snapshot of your network activities. The drawbacks of applying DNS-based analysis are the amount of data generated and that often there is no clear starting point (traffic baseline) to enable detection of anomalies and malicious activities. This talk aims at providing a solid starting point to incident responders and security analysis on how to leverage DNS-based analysis to quickly find out the most eminent threats in the shortest time possible. It also provides detection use-cases, a summary of methods and tools for usage by an incident responder or threat hunter. Besides, it highlights the importance of DNS for Incident Detection and discusses common malware families using DNS to communicate with the attack infrastructure. ***Joao Collier de Mendonca**, @sec_joao, GIAC GCFA, GIAC GNFA, MSc. Digital Media, BSc. Computer Sciences, CISSP, CISA, Cyber Defense Center, Deutsche Telekom AG, Germany*

SUMMIT SPEAKERS

Daniel Bohannon, @danielhbohannon, Consultant, Mandiant

Daniel Bohannon is an Incident Response Consultant at MANDIANT with over six years of operations and information security experience. Mr. Bohannon received a Master of Science in Information Security from the Georgia Institute of Technology and a Bachelor of Science in Computer Science from The University of Georgia.

Dr. Ali Dehghantanha, @alidehghantanha , Marie-Curie International Incoming Fellow in Cyber Forensics, University of Salford

Dr. Ali Dehghantanha is a Marie-Curie International Incoming Fellow in Cyber Forensics and has served for many years in a variety of research and industrial positions. Other than Ph.D in Cyber Security he holds many professional certificates such as GXPN, GREM, CISM, CISSP, and CCFP. He has served as an expert witness, cyber forensics analysts and malware researcher with leading players in Cyber-Security and E-Commerce. Additional information can be found at http://alid.info

Mattia Epifani, @mattiaep, Digital Forensics Specialist, REALITY NET Snc

Mattia Epifani is partner and founder at REALITY NET – System Solutions, where he works as a senior consultant in Digital Forensics, Forensic Readiness, Mobile Security and Incident Response. He obtained a University Degree in computer science in Genoa (Italy) and a post-graduate course in Computer Forensics and Digital Investigations in Milan. He works as a digital forensics analyst for judges, prosecutors, lawyers and private companies, both as Court Witness Expert and Digital Forensics Expert. He has obtained several certifications in Digital Forensics and Ethical Hacking (GCFA, GREM, GNFA, GMOB, GCWN, CIFI, CEH, CHFI, CCE, ACE, AME, MPSC, ECCE) and he is a regular speaker on Digital Forensics matters in different Italian and European universities (Genova, Milano, Bolzano, Pescara, Salerno, Campobasso, Roma, Camerino, Pavia, Savona, Catania, Lugano, Como, Modena e Reggio Emilia) and events (SANS European Digital Forensics Summit, Security Summit, IISFA Forum, DFA Open Day, DEFT Conference). He is a member of DFA, IISFA, ONIF and T&L Center. Co-author of the book "Learning iOS Forensics" edited by PacktPub in March 2015.

Thomas V. Fischer, @FVT, Global Security Advocate & Threat Researcher, Digital Guardian

With over 25+ years experience, Thomas has a unique view on security in the enterprise with experience in multi domains from policy and risk management, secure development and incident response and forensics. Thomas has held roles varying from security architect in large fortune 500 company to consultant for both industry vendors and consulting organizations. Thomas currently plays a lead role in advising customers while investigating malicious activity and analyzing threats for Digital Guardian.

Thomas is also an active participant in the infosec community not only as a member but also as director of Security BSides London and ISSA UK chapter board member.

David Gray, @D4VID_GRAY, Consultant, RSA Advanced Cyber Defense Practice

David is a Consultant for RSA ACD Practice engaged in Global Incident Response/discovery services, breach readiness, remediation, SOC/CIRC redesign and computer network defense.

SUMMIT SPEAKERS

Martin Korman, Incident Responder & Forensic Investigator, Team8

Martin Korman currently works as an incident responder and forensic investigator at Team8, previously to his work at Team8, Martin worked at IBM Trusteer as part of the research team to investigate and reverse engineer new threats. He is a talented young developer who enjoys creating research tools and contributing to the information security community by sharing his methods and findings. Prior to joining IBM Trusteer, Korman spent five years of service in the IDF, for most of which he served as a NOC manager. He also worked as an incident response officer for the Israeli Air Force's SOC, focusing on malware and forensic analysis. In his free time, you will find Martin reading technical information security literature or playing electric guitar. Martin speaks Spanish, English and Hebrew.

Joao Collier de Mendonca, @sec_joao, GIAC GCFA, GIAC GNFA, MSc. Digital Media, BSc. Computer Sciences, CISSP, CISA, Cyber Defense Center, Deutsche Telekom AG, Germany

João is a senior Incident Responder at the Cyber Defense Center of Deutsche Telekom Group, where he investigates security breaches for companies of various sizes. His work is focused on network-based incident detection and on the setup and improvement of Incident Detection and Response Capabilities across the Deutsche Telekom Group.

Angelo Perniola, @AngeloPerniola, Senior Consultant, RSA Advanced Cyber Defense Practice EMEA

Angelo is a Senior Consultant for RSA ACD practice contributing in engagements of SOC design and implementation, Incident Handling and Threat intelligence program development, breach readiness assessments.

Pasquale Stirparo, @pstirparo, Cyber Threat Intelligence Analysist & Incident Responder, UBS

Pasquale Stirparo is currently working as Cyber Threat Intelligence Analyst and Incident Response Engineer at a Fortune 500 company. Since 2016 he has also been appointed at the Advisory Group on Internet Security at the European Cyber Crime Center (EC3) of Europol and is serving as Incident Handler with the SANS Internet Storm Center (ISC). Pasquale has also been involved in the standardization of Digital Forensics by contributing to the development of the standard ISO/IEC 27037.

Author of many scientific publications and co-author of the book "Learning iOS Forensics" (2015), he has also been invited as speaker to several national and international conferences and seminars on Digital Forensics and lecturer on the same subject for Polytechnic of Milano (CEFRIEL) and United Nations (UNICRI). Pasquale holds a Ph.D. in Computer Security from the Royal Institute of Technology (KTH) of Stockholm and a M.Sc. in Computer Engineering from Polytechnic of Torino, and is certified GCFA, GREM, OPST, OWSE, ECCE.

Christopher Witter, @mr_cwitter, Manger Falcon OverWatch, CrowdStrike

Chris manages a team of intrusion analysts at CrowdStrike where they are responsible for investigating some of the most notorious cyber threats to the US economy. Previously, he held senior roles on the Computer Security and Incident Response Teams at both a top five global bank and at a top ten defense contractor.