SANS EMEA

SANS DFIR EUROPE SUMMIT

Prague, 11 October 2015

training@sans.org +44 (0)20 3384 3470 www.sans.org/event/dfir-prague-2015 @SANSEMEA

Sunday 11 October, 2015

8:50 – 9:00 am

Welcome & Opening Remarks

Jess Garcia: *Chair, SANS DFIR Europe Summit*

9:00 – 9:45 am

KEYNOTE

There’s Something About WMI

This presentation will describe the purpose and components of Windows Management Instrumentation (WMI) from the incident response and forensics perspectives. Attendees will learn how targeted threats are using WMI during each phase of the compromise, case studies and examples, the artifacts generated by those activities, some of the tools used to interact with WMI, using WMI for persistent access that defeats antivirus and application whitelisting, and the benefits of enabling WMI trace logging for additional detection and improved analysis.

Christopher Glyer: *Technical Director, MANDIANT, a FireEye Company*
Devon Kerr: *Senior Consultant, MANDIANT, a FireEye Company*

9:45 – 10:30 am

Inside Windows Phone 8: Forensic Acquisition and Analysis

A new operating system is growing in the mobile market: Windows Phone 8. Microsoft released this Mobile OS in 2013, and as of May 2015 it was in third position after Android and iOS for number of devices sold. In the last year more and more research has been developed regarding how to acquire data with JTAG techniques or based on BootROM exploit. The aim of this presentation is to illustrate the most commonly used procedures to extract data from Windows Phone 8 devices to obtain, when possible, a complete forensic image of the internal NAND, as well as to provide information about what can be extracted during analysis (internal data structure, file system, native apps, media files, third party apps, forensic artifacts, and so on). The talk will include a compelling case study of a criminal investigation of a home invasion and sexual assault where a Windows Phone 8 device provided crucial evidence resulting in a number of convictions.

Mattia Epifani: *CEO, REALITY NET*
Cindy Murphy: *MSc, Detective, Digital Forensics / Computer Crimes, Madison (WI) Police Department*
Francesco Picasso: *CEO, REALITY NET*

10:30 – 11:00 pm

Networking Break

11:00 – 11:45 am

ReVaulting!: Decryption and Opportunities

Windows credentials manager stores users’ credentials in special folders called vaults. Being able to access such credentials could be truly useful during a digital investigation - for example, to gain access to other protected systems. Moreover, if data is in the cloud, there is the need to have the proper tokens to access it.

This presentation will describe vaults’ internals and how they can be decrypted; the related Python Open Source code will be made publicly available. During the session, credentials and vaults coming from Windows 7, Windows 8.1 and Windows 10 will be decrypted, focusing on particular cases of interest. Finally, the presentation will address the challenges coming from Windows Phone, such as getting system-users’ passwords and obtaining users’ ActiveSync tokens.

Francesco Picasso: *CTO, REALITY NET*

11:45 am – 12:15 pm

Investigating Security Incidents Involving Microsoft Exchange Using In-Mailbox Forensic Artefacts

In most large organisations, Microsoft Exchange is far more than a mail system: it is effectively the organisational memory, storing huge volumes of email interactions as well as calendar data, contacts, notes, task lists and other user data. Security incidents involving Exchange are made more complex by this range of data, for example it can be difficult to determine exactly what mailboxes were compromised and which data within each mailbox might have been accessed.

Fortunately, the number of forensically-valuable artefacts inside Exchange mailboxes is increasing. Recent versions of Exchange store far more data within user mailboxes rather than on end-user devices, and recent versions of Outlook also create useful artefacts in some odd locations within the mailbox. When dealing with a modern Exchange infrastructure, or with Exchange Online in Office 365, these artefacts are rich enough to reconstruct malicious activity down to the level of individual emails accessed. Of particular interest for incident responders, this reconstruction can be done without touching client devices and without reference to Exchange logs or other formal audit trails.

By walking through a specific incident scenario, this session will show some of the in-mailbox artefacts which can be used to investigate malicious activity in Exchange. We will reconstruct a range of attacker actions including initial mailbox compromise, mailbox access and exploration, data extraction and activity monitoring. We will also cover methods for identifying and researching additional artefacts and hopefully provide something of a roadmap for others interested in Exchange forensics.

Kevin McGlone: *Digital Evidence Specialist, Cernam*
Owen O'Connor: *VP of Digital Evidence, Cernam*

12:15 – 1:30 pm

Lunch

1:30 – 2:15 pm

New Generation Timeline Tools: A Case Study

A moderately-sized institution of higher learning receives an ominous threat from a shadowy hacker group. A plucky band of misfits, armed only with open source forensic tools is the college's only hope. What happens next? Will our brave band of heroes be able to stop the cyber terrorists in time?

This talk will give you a good understanding of the new features in the Plaso and Timesketch forensic tools, as well as an insight into some of the analysis processes these tools enable. Rather than just talking about these features, you'll see how they're actually deployed in an investigative context.

Daniel White: *Security Engineer, Google*

2:15 – 3:00 pm

Active Defence: Gaining Visibility Into Your Network

Active defence is the process of monitoring for, responding to, and learning from threats. It is not about hack-back, it is simply taking an active approach to defence. The key to being able to implement an active defence is building on the proper foundations of security including the proper architecture and maintenance of the network as well as the appropriate use of passive defences such as firewalls and anti-malware systems. This talk will present a framework to discuss the activities that contribute to cyber security and a strategy for an active defence. It will focus on a key step that contributes to security within a network: asset identification. Understanding the assets, the network itself, and being able to establish baselines of normal activity are all critical components of security. With a good understanding of the network itself and through gaining true network situational awareness, it is possible to implement the style of defence that is required for countering advanced threats.

Robert M. Lee: *Co-Founder, Dragos Security*

3:00 – 3:30 pm

Networking Break

3:30 – 4:15 pm

Back to the Future with Document Malware

Just like fashion, what is old is new again. There has been a resurgence of document based malware this year. Documents are commonly shared over email and make perfect weapons against unsuspecting victims of phishing attacks. The ability to analyse these malicious documents and make them spill all their dirty secrets will provide a huge leg up on your investigations. The most common document formats and the best tools and techniques to analyse them will be covered. We will also look at some recent widespread campaigns and walkthrough how to analyse them and bypass their defences.

Tyler Halfpop: *Threat Researcher, Fidelis Cybersecurity*

4:15 – 5:30 pm

DFIR SANS360

This session features an array of top Digital Forensics and Incident Response experts discussing the coolest forensic technique, plugin, tool, command line, or script they used in the last year. They'll talk about the approach that really changed the outcome of a case they were working on. If you have never been to a lightning talk, it is an eye-opening experience. Each speaker has 10 minutes to deliver his or her message. This format allows SANS to present half a dozen experts in one hour. The compressed format gives you a clear and condensed message eliminating the fluff. If the topic isn't engaging, a new topic is just 10 minutes away.

Baselining Memory for Anomaly Detection
Alissa Torres, Certified Instructor, SANS Institute

Threat Intelligence and Thinking About How to Think
Robert M. Lee, Co-Founder, Dragos Security

What to Expect When You're Expecting Anonymous
Cindy Murphy, MSc, Detective, Digital Forensics /
Computer Crimes, Madison (WI) Police Department

Six Minutes in Mac Heaven
Sarah Edwards, Test Engineer, Parsons Corporation

Temet Nosce : Know Thy Endpoint, Through and Through
Thomas V. Fischer, Principal Threat Researcher, Digital Guardian

You, the BeEF and the Butcher
Pasquale Stirparo, PhD., Sr. Information Security Incident Response Engineer

Speaker Bios:

Jess Garcia

Chair, SANS DFIR Europe Summit; Principal Instructor, SANS Institute; Founder, One eSecurity

Jess Garcia is the founder and technical lead of One eSecurity, a global Information Security company specialised in Incident Response and Digital Forensics. With near 20 years in the field, and an active researcher in the area of innovation for Digital Forensics, Incident Response and Malware Analysis, Jess is today an internationally recognised Digital Forensics and Cybersecurity expert, having led the response and forensic investigation of some of the world's biggest incidents in recent times.

In his career Jess has worked in a miriad of highly sensitive projects with top global customers in sectors such as financial & insurance, corporate, media, health, communications, law firms or government, in other Cybersecurity areas as well such as Security Architecture Design and Review, Penetration Tests, Vulnerability Assessments, etc.

A Principal SANS Instructor with almost 15 years of SANS instructing experience, Jess is also a regular invited speaker at Security and DFIR conferences worldwide. Previously, Jess worked for 10 years as a systems, network and security engineer in the Spanish Space Agency, where he collaborated as a security advisor with the European Space Agency, NASA, and other international organisations.

Jess holds a Masters of Science in Telecommunications Engineering + Computer Science from the Univ. Politecnica de Madrid.

Sarah Edwards

Test Engineer, Parsons Corporation

Sarah is an senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counter intelligence, counter-narcotic, and counter terrorism. Sarah's research and analytical interests include Mac forensics, mobile device forensics, digital profiling and malware reverse engineering. Sarah has presented at many industry conferences including; Shmoocon, CEIC, Bsides*, Defcon and the SANS DFIR Summit. She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Masters in Information Assurance from Capitol College. Sarah is the author of the new SANS Mac Forensic Analysis Course - FOR518.

Mattia Epifani

CEO, Reality Net

Mattia Epifani is CEO at Reality Net – System Solutions, an Italian consulting company involved in InfoSec and Digital Forensics. He works as a digital forensics analyst for judges, prosecutors, lawyers and private companies, both as Court Witness Expert and Digital Forensics Expert. He obtained a University Degree in computer science in Genoa (Italy) and a post-graduate course in Computer Forensics and Digital Investigations in Milan. In the last few years he has obtained several certifications in Digital Forensics and Ethical Hacking (GNFA, GREM, GCFA, GMOB, CIFI, CEH, CHFI, ACE, AME, ECCE, CCE, MPSC) and took various SANS classes. He is a regular speaker on Digital Forensics matters in different Italian and European universities and events. Author of the book "Learning iOS Forensics" edited by PacktPub in March 2015. He is also a member of DFA, IISFA, ONIF and T&L Center.

Thomas V. Fischer

Principal Threat Researcher, Digital Guardian

With over 20+ 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 organisations. Thomas currently plays a lead role in malicious activity and threat analysis for Digital Guardian. Thomas holds CISSP, ITIL and GCIH certifications.

Christopher Glyer

Technical Director, Mandiant

Christopher Glyer is a Technical Director at Mandiant with over ten years' experience in computer and information security. Mr. Glyer leads Mandiant investigative teams performing enterprise-wide incident response and forensic analysis for global companies possessing tens of thousands of computer systems throughout the world. Mr. Glyer has significant experience working with the defence industrial base, financial industry, manufacturing industry, technology industry, pharmaceutical industry, and Fortune 500 companies.

Mr. Glyer helps define feature, architecture, and design requirements for Mandiant's enterprise investigative tools including Mandiant Intelligent Response (MIR). He routinely trains both commercial and federal professionals on computer forensics and incident response including teaching Mandiant's Incident Response - Black Hat Edition course.

Tyler Halfpop

Threat Researcher, Fidelis Cybersecurity

Tyler is a threat researcher for Fidelis Cybersecurity. Tyler's main research interests are in reverse engineering and malware analysis. He is currently working on his doctorate in computer science. He is a SANS Lethal Forensicator and has several industry certifications including the CISSP and GREM. He likes to stay involved in the security community through several organisations and has spoken at various conferences and meetings.

Devon Kerr

Principal Consultant, Mandiant

Devon Kerr is a Principal Consultant in Mandiant's Alexandria office. Mr. Kerr has led and participated in threat assessments, incident response engagements, forensic analysis, education, and proactive assessments. Mr. Kerr is an OpenIOC knowledge developer within the Mandiant professional services organisation and has developed internal coursework relating to IOC creation and utilization.

Mr. Kerr has worked with clients in financial services, defence, manufacturing, aerospace, telecommunications, media, and infrastructure. Many of those clients rank in the Fortune 50 or Fortune 100. Mr. Kerr has been instrumental in developing the incident response capabilities of clients and providing strategic remediation guidance following investigations.

Prior to joining Mandiant in 2011, Mr. Kerr spent more than a decade in Network Operations and ISP infrastructure. During that time, Mr. Kerr spent three years investigating the compromise of UNIX and Linux servers.

David Kovar

Senior Manager, Ernst & Young

David Kovar is a senior manager in EY's Cybersecurity practice. He's also been an entrepreneur, ediscovery consultant, software engineer, SAR incident commander, executive protection agent, and lethal forensicator. He has collected images in China, rescued wayward Americans in Australia, and conducted disaster preparedness assessments in Tajikistan. Oh, and he flies sailplanes, fixed wings, helicopters, and drones...

Robert M. Lee

Co-Founder, Dragos Security LLC

Robert M. Lee is a co-founder at the critical infrastructure cyber security company Dragos Security LLC where he has a passion for control system packet analysis, digital forensics, and threat intelligence research. He is a passionate educator having taught for various organisations including Utica College where he is currently an Adjunct Lecturer in the M.S. Cybersecurity programme. He is the SANS ICS 515 - Active ccourse author and co-author for SANS FOR 578 - Cyber Threat Intelligence. Robert is often confused with the other Rob Lee at SANS who is a SANS Fellow and runs the Forensics track. It is in fact a different Rob Lee who just so happened to have also been in the Air Force and attended the same undergraduate university as Robert - that Rob Lee is more talented although it has cost him his hair.

Robert obtained his start in cyber security in the U.S. Air Force where he currently serves as an active-duty Cyber Warfare Operations Officer. He has been a member of multiple computer network operation teams including his establishing and leading of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission in the intelligence community. He has published numerous articles and journals for various publications including SC Magazine, Air and Space Power Journal, Control Global, and Control Engineering and is a frequent speaker at conferences having previously presented at events such as SANS, IFRI, BSides, and TROOPERS. Robert received his B.S. from the United States Air Force Academy, his M.S. in Cybersecurity - Digital Forensics from Utica College, and is currently pursuing his PhD at Kings College London with research into cyber conflict and the cyber security of control systems. He is also the author of the book "SCADA and Me."

Kevin McGlone

Digital Evidence Specialist, Cernam

Kevin McGlone is a Digital Evidence Specialist in Cernam's Dublin office. Kevin has worked with Cernam since 2011 and has played a key role in several complex investigations which required in-depth analysis of sophisticated cloud systems. His work with Cernam has included several large-scale e-discovery projects where he was responsible for evidence identification and collection from both on-premises Exchange and Exchange Online (Office 365). More recently he has played a key role in developing advanced evidence collection tools for Office 365 which required a detailed knowledge of Exchange Online data structures and the value of evidence stored in Exchange mailboxes. He holds an honours degree in Computer Forensics & Security from Waterford Institute of Technology.

Cindy Murphy

Detective, City of Madison, WI Police Department

Detective Cindy Murphy works for the City of Madison, WI Police Department and has been a Law Enforcement Officer since 1985. She is a certified forensic examiner and has been involved in computer forensics since 1999. She earned her Master's degree in Forensic Computing and Cyber Crime Investigation through University College, Dublin in 2011. She has directly participated in the examination of many hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations including homicides, missing persons, computer intrusions, sexual assaults, child pornography, financial crimes, and various other crimes. She has testified as a computer forensics expert in state and federal court on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She is also a part time digital forensics instructor at Madison College, and a part time Advanced Mobile Device Forensics instructor for the SANS Institute.

Owen O'Connor, VP of Digital Evidence, Cernam
Owen O'Connor is VP of Digital Evidence at Cernam, a cloud-focused digital evidence firm based in Dublin and San Francisco, and has over 17 years of experience in digital evidence and corporate information security. Prior to founding Cernam he served as Director of IT Security with Elan Pharmaceuticals where he developed and managed an in-house digital evidence capability, covering electronic discovery, internal investigations and response to government investigations. He has led numerous e-discovery projects and investigations, including multiple cases where his analysis led directly to the favourable resolution of high-value lawsuits or to successful criminal prosecutions. He holds a Master's in Forensic Computing from Cranfield University (Royal Military College of Science), has been an invited speaker at several of the largest digital evidence conferences, and has provided specialist training for law enforcement and government agencies.

Francesco Picasso

CTO, Reality Net

Francesco Picasso is CTO at Reality Net – System Solutions, an Italian consulting company involved in InfoSec and Digital Forensics. He provides Digital Forensics and Incident Response services to customers. He is a Computer Science Engineer and Ph.D. focused on research and innovation. GCFA and GCIH certified.

Alissa Torres

Certified Instructor, SANS Institute

Alissa Torres is a certified SANS instructor, specialising in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on a internal security team as a digital forensic investigator. She has extensive experience in information security, spanning government, academic, and corporate environments and holds a Bachelors degree from University of Virginia and a Masters from University of Maryland in Information Technology. Alissa has taught as an instructor at the Defence Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community. She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+.

Daniel White

Security Engineer, Google

Daniel White is a security engineer at Google, focused on forensics, incident response, tool development, and whatever else comes up.

SANS EMEA

✉ training@sans.org ☎ +44 (0)20 3384 3470 www.sans.org/event/ dfir-prague-2015 @SANSEMEA