SANS

EUROPEAN

Digital Forensics AND Incident Response

SUMMIT

PRAGUE, CZECH REPUBLIC

6-7 October 2013

PROGRAM GUIDE

Agenda

All Summit Sessions will be held in Moldavite (unless noted).

*All approved presentations will be available online following the Summit at **https://files.sans.org/summits/euforensics13**.*
An e-mail will be sent out within 5 business days once the presentations are posted.

Sunday, 6 October

8:00 - 9:00 am

Registration & Coffee

9:00 - 10:00 am

Massive Incident Investigations

How do you approach an investigation when dozens or hundreds of systems in your network are suspected to be compromised? What if the attackers have been living in your systems for months? What if they have been using sophisticated malware? What do you look for? What tools and techniques can be used to escale up to that level? What should the strategy be? What if the attackers are ninja-level and they are still in your network? How can you fight them? And finally... how can you successfully recover from such a massive breach?

In this talk, Jess Garcia will show how he and his DFIR Team have succeeded in fighting these types of incidents during the last few years. He will address these topics and many more, showing how to procedurally and technologically approach these massive incidents and their corresponding investigations, and illustrating hands-on what tools and techniques prove to be especially useful in these cases.

***Jess Garcia**, Summit Chair, SANS Institute*

10:00 - 10:20 am

Networking Break

10:20 - 11:15 am

Blue Teams, PICERL, and You

Many SANS classes introduce the student to PICERL - Preparation, Identification, Containment, Eradication, Recovery and Lessons learned. Once introduced, the class will generally dive into one element enabling students to develop a deep understanding of C, E, or R. The larger picture, the context they operate within, might not be fully explored.

This presentation ties together all the elements into a complete narrative, walking the attendees through the entire incident response process. Attendees will develop a greater appreciation of their role, the role of others in their IR team, and their relationship with the larger organization. While we each may think our role is confined to one of those phases, or maybe two, we should be involved in all phases to a greater or lesser degree. And in doing so we expand our own capabilities and contribute to the development of a stronger and more flexible team.

*Speaker: **David Kovar**, Manager, Ernst & Young*

11:15 am - Noon

SSD Storage & Forensics Analysis

Compared to traditional hard disk drives (HDD), solid state drives (SSD) are faster, smaller, more robust and do not have any moving parts. Their market share has been growing and they are expected to prevail on the market in the future.

The goal of the presentation is to outline the differences between traditional HDD and SSD regarding data storage and access to deleted data. Technology, structure and principles of used NAND flash memories, internal optimization mechanisms and parameters of the particular tested drive are described in detail.

The presentation describes mechanisms such as de-duplication, compression, garbage collector, FTL and over-provisioning used in the SSD. Their impact on data stored is supported by the results of experiments.

The presentation summarises the present knowledge about the internal functions of SSDs and its controller; data storage method and the implications of using SSD for forensic analysis and e-discovery.

*Speakers: **Mr. Ing. Aleš Padrta, Ph.D.**, CESNET, Czech Education and Scientific Network*
***Mr. Bc. Karel Nykles**, CESNET, Czech Education and Scientific Network*

Noon - 1:30 pm

Lunch

Location: Onyx

1:30 - 2:15 pm

EVTXtract: Recovering EVTX Records from Unallocated Space

This presentation will introduce a novel technique for recovering event log records from unallocated space on Windows Vista, 7 and 8 systems. On a Windows XP system with cleared event logs, its not uncommon to recover 50,000 events – some of which may contain critical evidence or help scope an investigation. EVTXtract identifies this evidence on newer Microsoft operating systems. We'll begin with a refresher on the format of EVTX log files and demonstrate some of the concerns in reviewing modern event log record structures. Then, we'll introduce a step-by-step technique for identifying potential records in unallocated space, extracting their data, and reconstructing the original entries. Of course, a concise case study will help show exactly what this means to an investigator. And, to make this accessible to all, we'll finally release EVTXtract – an original suite of tools that make it simple to recover evidence of evildoers. Attendees will leave prepared and excited to tackle future investigations with knowledge of this robust technique.

Speaker: ***Willi Ballenthin****, Consultant, Mandiant*

2:15 - 3:00 pm

New School Forensics: Latest Tools and Techniques in Memory Analysis

Whether you are just getting started with memory forensics, or you have been at it since the early days, the last year produced a wealth of new memory analysis capabilities. Notably, nearly all of the progress has been accomplished in free and open source tools. Learn about the latest and greatest additions to the memory forensics arsenal:

- In-memory registry forensics
- Building and analyzing memory object timelines
- Mac and Linux memory analysis
- The advantages of "live" memory analysis

Speaker: ***Chad Tilbury****, Certified Instructor, SANS Institute*

3:00 - 3:30 pm

Networking Break

3:30 - 4:30 pm

DFIR SANS360

In one hour, 10 Digital Forensics and Incident Response experts will discuss the coolest forensic technique, plugin tool, command line, or script they used in the last year that really changed the outcome of a case they were working. If you have never been to a lightning talk, it is an eye opening experience. Each speaker has 360 seconds (6 minutes) to deliver his or her message. This format allows SANS to present 10 experts within one hour, instead of the standard one-presenter-per-hour. The compressed format gives attendees a clear and condensed message, eliminating the fluff. If the topic isn't engaging, a new topic is just 6 minutes away.

Speakers:

- ***Expert Witness Testimony: 7 Tips for Forensicators from Forensicators*** - *Christian Prickaerts, SANS Institute*
- ***iPhone Backup Analyzer and Whatsapp Xtract: Open Source Tools for Mobile Forensics*** – *Mattia Eppifani, Digital Forensics Specialist, REALITY NET Snc*
- ***5 Ninja Tricks to Detect Bad Guys in Your Systems & Networks*** - *Jess Garcia, SANS Institute*
- ***Applications' Credentials Harvesting from Android Memory*** - *Pasquale Stirparo, Digital Forensics & Mobile Security Researcher, Joint Research Centre – European Commission*
- ***Forensic Capabilities and ICS Networks*** – *Robert M. Lee, Founder & Director, hackINT*
- ***Your Workflow is Not My Workflow!: A Short Rant About "Tool-Imposed Workflow"*** – *Joachim Metz*
- ***ProcDOT – Visual Malware Analysis*** – *Christian Wojner, Austrian CERT*
- ***Mobile Device Data Recovery via Chip-Off Extraction*** – *Arturo Rodriguez, Guardia Civil (Spanish LE)*
- ***AGGRESSIVE Incident Response*** – *Rob Lee, SANS Institute*

Please remember to complete your speaker evaluation form.
You may leave the completed survey at your seat or turn it in to the SANS registration desk.

Monday, 7 October

8:00 - 9:00 am

Registration & Coffee

9:00 am - 10:00 am

A Week in the Life of DFIR

Follow along the fast paced world of Incident Response as one intrepid responder goes through a typical week of chasing down malware infections, domain hijackings, and possible data breaches.

DFIR is the intersection of all Security topics, not just dead disk forensics. We aren't jacks of all trades, we are the masters of all trades. See how different tools work together to produce the big picture of what's happening on your network with some "ripped from the headlines" examples.

Speaker: ***Elizabeth Schweinsberg,*** *Incident Responder, Google, Inc.*

10:00 - 10:20 am

Networking Break

10:20 - 11:15 am

Exchange in the Cloud: Investigative and Forensic Aspects of MS Office 365

Moving corporate email from self-hosted Exchange servers to Microsoft's Office 365 service has many benefits: reduced costs, reduced infrastructure, potentially even better availability and improved end-user service. For digital evidence professionals, switching to Office 365 represents a radical change and poses many practical challenges: how do we gain access to user mailboxes, how do we collect email evidence, how do we investigate mailbox access? Investigators who regularly work with on-premises Exchange servers may find the transition to Office 365 jarring, for example the lack of a mailbox export feature and the fact that many useful logs are unavailable – e.g., Exchange tracking logs, Windows security logs and Outlook Web Access logs.

This talk will look at the investigative and forensic aspects of Office 365, specifically the "Exchange Online" component which replaces a traditional corporate email environment. The talk will introduce the Office 365 permissions model, look at key administrative processes for investigations and review methods of collecting evidence from Office 365. We will also consider the logs and audit data available within Office 365, as well as discussing investigative approaches for email misuse, unauthorised mailbox access, questioned email analysis and other common email investigations. Finally we will briefly look at other components of Office 365, in particular Lync Online and SharePoint Online, and review some features of the wider Office 365 platform which have investigative implications.

Speaker: ***Owen O'Connor****, Managing Director, Cernam Online Evidence*

11:15 am - Noon

Detecting Malicious PDF Documents Using Machine Learning

Portable Document Format (PDF) documents are widely used due to their well-defined format that is supported by many applications, services, operating platforms and computing devices. PDF documents are also target for abuse in hostile activities as the potential impact could be far spread. Those malicious PDF documents contain content, such as PDF instructions, that can render undesired actions as for example leaking personal information, or escalating the permissions of a user so that an attacker can take over control of the device. Other malicious content in PDF files is embedded Java script that is going to be executed while the PDF is rendered for display or printing.

Machine learning and pattern recognition methods can be used to learn flexible models from exemplars of malicious PDF instructions or javascript. Once the models are created they are used to classify "normal" and "abnormal" aka malicious PDF. In our study several features of PDF documents are analyzed in order to retrieve those significant for the detection of malicious PDF. Additional experiments were performed to determine the best combination of features, machine-learning classifier, and its parameterization to maximize efficiency and effectiveness in the detection. Finally, a real world study was performed by implementing the algorithm in a communication network belonging to the Norwegian Defence analyzing up to 100,000 different PDF documents automatically.

Speakers: ***Jarle Kittilsen,*** *MSc, Network Security Analyst, Norwegian Cyber Force*
Katrin Franke, PhD*, Professor of Computer Science, Norwegian Information Security Laboratory*

Noon - 1:30 pm

Lunch

Location: Onyx

1:30 - 2:15 pm

Cloud Storage Forensics: Analysis of Dropbox, Google Drive and iCloud

The use of Digital Forensics Cloud Storage systems (like Dropbox, SkyDrive, GoogleDrive, iCloud, etc.) has grown over the last few years. In many cases, the digital investigator needs to analyze data regarding the use of this tool, and the analyses are conducted both online and on seized digital devices.This talk will introduce the most important Digital Forensics Cloud Storage System, explain the forensics artifacts left in computers and mobile devices by the usage of these tools, explore and use some tools and techniques to analyze the kind of information and describe the information available online for that service.Then a case study will be presented on a Windows virtual machine running some Cloud Storage services and an iPhone backup with some cloud storage apps.

Speaker: ***Mattia Epifani****, Digital Forensics Specialist, REALITY NET Snc*

2:15 - 3:00 pm

Hypervisor Memory Forensics

Nowadays virtualization is everywhere, both as part of the cloud and in normal desktop installations. Unfortunately, there are no techniques or tools to perform a complete memory investigations of these virtual environments. In this presentation we will explain Actaeon. Actaeon is a tool to perform memory forensics of virtualization environments. Starting from a physical memory dump, Actaeon can achieve the following goals: locate any Hypervisor (virtual machine monitor) that uses the Intel VT-x technology, detect and analyze nested virtualization and show the relationships among different hypervisors running on the same machine, and provide a transparent mechanism to recognize and support the address space of the virtual machines. Actaeon adopts a hypervisor-agnostic approach, thus it can detect any hypervisor (benign or malicious) that uses this technology. The attendees will learn the basics of virtualizazion memory forensics. In particular we will describe how to locate an hypervisor in a physical memory dump, how to understand its main features, and finally how to transparently introspect the Windows Guests using Volatility.

Speaker: ***Mariano Graziano*** *and* ***Davide Balzarotti****, Eurecom*

3:00 - 3:20 pm

Networking Break

3:20 - 4:15 pm

Catching "Bayas" on the Wire: Practical Kung-Fu to Detect Malware Traffic

Bayas (Swahili word for "badness," aka. malware of any kind, shape or form) continue to grow in number as script kiddies, hacktivists, organized crime and nation-state actors use them to deface websites, steal money, engage in cyber-warfare or "simply" to disrupt large businesses or nation-critical infrastructure.

However, malicious software doesn't exist in a vacuum; any piece of malware is designed to call-back home sooner or later: to download additional malware, to report back to a C&C server or to exfiltrate data. How can Incident Responders detect hidden malware on the network using open-source tools and what patterns do they need to look for? In my talk, I will share lessons learned from practical traffic analysis in the field (i.e. predominate communication protocols, current trends, etc.) and present some effective techniques used to filter suspicious connections and investigate network data for traces of malware using tools like Wireshark, Suricata and Bro.

Speaker: ***Ismael Valenzuela****, Principal Architect - Foundstone Services EMEA, McAfee Strategic Security/Foundstone Services*

4:15 - 5:00 pm

More Digital Threats or a Better DFIR Community?

Over the past decade there has been an exponential increase in the amount of network exploitation and digital threats that have been observed both in the DFIR community as well as the news media. International attention has been given to these threats in the form of national cybersecurity documents, political campaigning, establishment of computer network operation programs, and the often misused and abused term "cyber." The last decade has also seen an increase in both the availability and quality of education and training for analysts which has led to a digital forensics community that is more prepared to face challenges now than ever before.

The purpose of this talk is to explore the simple question: "Are the digital threats we face exponentially increasing in number or are we now simply better at discovering these threats thanks to a more mature and well-educated DFIR community?" This question will be explored through discussions with the audience and a variety of case studies on threats as well as education, tools, and developments in the community.

Speaker: ***Robert M. Lee****, Founder & Director, hackINT*

Thank you for attending the SANS European Digital Forensics & Incident Response Summit.

Please remember to complete your evaluation forms.
You may leave the completed surveys at your seat or turn them in to the SANS registration desk.

UPCOMING SUMMITS & TRAINING COURSES

2013

Securing the Internet of Things Summit
San Francisco, CA | October 22

Healthcare Cyber Security Summit
San Francisco, CA | October 23-24

Pen Test Hackfest Summit & Training
Washington, DC | November 7-14

Asia Pacific ICS Security Summit & Training
Singapore | December 2-8

2014

AppSec Summit & Training
Austin, TX | February 3-8

Industrial Control Systems Security Summit & Training
Orlando, FL | March 12-18

Digital Forensics & Incident Response Summit & Training
Austin, TX | June 3-10

For more information on speaking at an upcoming summit or sponsorship opportunities, e-mail SANS at **summit@sans.org**. Visit **www.sans.org/summit** for detailed summit agendas as they become available.