Real-World Computer Forensics Challenges Facing Cyber Investigators

Inno Eroraha, CISSP-ISSAP, CISM, CISA, CHFI, PI
Founder & Chief Strategist
NetSecurity Corporation

Computer Forensics Show 2010 Conference
New York, NY

netSecurity Forensic Labs

netSecurity®

Abstract Condensed

Technology continues to emerge at a fast pace while forensics and security technologies lag behind. Recently released products such as Apple iPad, HP Slate, and MSI Tegra 2 are technologies that cyber criminals are either likely to use to launch a cyber attack or become the target of such an attack. Moreover, there are few tested and standardized forensic tools with which to conduct a forensics investigation on these devices and other emerging electronic gadgets. Cyber criminals are constantly inventing ways to circumvent security and forensics techniques, whether targeting outdated, current, or emerging technologies. The increasing sophistication of cyber attackers poses significant challenges to the cyber investigator. Criminals now devise anti-forensics techniques that can require endless investigation into the attack! To "think like the hacker" may not be sufficient to uncover their approaches. Training and education that places too much emphasis on vendor specific tools or that seek to merely provide certification often diminishes critical thinking skills and creative problem solving techniques. Lacking adequate knowledge in malicious software collection and analysis may result in an incomplete investigation that could exonerate a suspect in a case. Likewise, failing to collect volatile data during the initial cyber crime scene response may prevent successful prosecution of the attacker. Based upon field experience and interviews conducted with seasoned experts, this presentation summarizes some of the challenges faced by cyber investigators and recommendations for overcoming these and other challenges.

Forensics Challenges

- Windows OS “Handicap” Factor
- Training/Education
- Emerging Technologies
- Emerging Cyber Threats
- Sophisticated Rootkits (Malware)
- Advanced Persistent Threats (APT)
- Privacy/Encryption Software
- Live Volatile Data
- Memory Forensics
- Remote Forensics
- Malware Analysis
- Network Forensics
- Massive Data Collection and Analysis
- Legal System

Are Investigators Getting Crippled by Windows?

Do Investigators have the skills to investigate non-Windows OS?

Is Windows OS a Handicap?

- In addition to Windows, operating systems such as Mac OS and Linux/Unix are widely used today
- Unfortunately, most Forensics tools and training primarily focus on Windows platform
- Heavy Windows focus makes investigators weaker in investigating “live” non-Windows systems
- Network infrastructure devices are often ignored

Forensics Training and Education

- Are we getting the right training and education in the right specialty areas?
- Are we just going for training to learn one vendor's product or tool?
- Are we just going for certifications?
- Are we just going with-the-flow?

Training/Education Challenges

- Most training is predominately certification- and vendor-focused rather than learning to solve real-world problems with broad tools
- Fundamental knowledge is inadequate in broader skill areas, including:
  - Operating Systems (Unix/Linux, Mac OS, Mainframe, Windows)
  - Networking
  - Software Development (Scripting!)
  - System Administration
  - System/Network Security
  - System Exploitation and Countermeasures
  - Incident Response
  - Intrusion Detection
  - Log Analysis
  - Reverse Engineering

Forensics vs. Medicine

- Both fields have Specialties:

Forensics Specialties	Medical Specialties
Windows Forensics	General Practice
Incident Response	General Surgery
Reverse Engineering	Neurosurgery
Malware Analysis	Ophthalmology
Internet Forensics	Orthodontics
Non-Windows Forensics	Native Doctor
Ethical Hacking	Chiropractor

- Forensics practitioners can easily focus in more specialties, especially due to the severe shortage of experts

Emerging Technologies are Good...

...Do they make Life Easier for Investigators?

Technology Advancement

- Cloud Computing
- Virtualization
- Emerging Devices

Are forensics tools keeping up?

Cloud Computing

- Computing model where shared hardware, software, applications are provided to consumer on-demand
- Service is paid for when used – “utility” concept
- Avoidance for initial capital expenditure by the consumer
- Examples: Hosted Email, Hosted Payroll

Cloud Computing – Challenges

- Logging may be minimized due to storage space
- Logging and data for multiple customers may be co-located
- Data may be spread across an ever-changing set of hosts and data centers
- Record of user activity, temporary files, and other useful artifacts may get lost when the user exits
- Data traditionally stored in RAM, may no longer be accessible in the cloud
- Length of time to request and receive this data from cloud vendor is prohibitive
- Jurisdiction of other countries may prevent/limit retrieval of stored data due to privacy laws
- Bankruptcy of vendor may render data inaccessible or unavailable
- Chain of Custody issues may arise
- Residual information stored in a third-party server may be difficult to obtain, without a subpoena

Sources:

1. http://www.zdnet.co.uk/blogs/cloud-computing-and-the-impact-on-digital-forensic-investigations-10012285/cloud-computing-and-the-impact-on-digital-forensic-
2. http://www.articlesnatch.com/Article/Cloud-Computing-And-Computer-Forensics/663389investigations-10012286/
3. http://www.forensicmag.com/articles.asp?pid=303

Emerging Devices

- First-to-market is forcing exponential advancement in emerging computing devices
- Examples include:
  - Apple iPad
  - HP Slate
  - Amazon Kindle
  - MSI Tegra 2
- Hackers are interested in using these devices as the source or target of attack
  - Attackers are quickly finding vulnerabilities and devising exploits once a new device hit the street

Emerging Devices – Challenges

- Inadequate forensics technologies to excavate digital evidence
- Forensic tools cover a small fraction of the PDA/Mobile devices in circulation
- Knowledge may be inadequate in understanding source of forensics artifacts
- Securely erasing data could be problematic

Is a Cure-all Solution Possible?

Let's examine a potential solution to forensics of emerging devices…

A Proposed Solution (v0.1) for Emerging Device Forensics

- Manufacturers provide a “User Activity Recorder” capability similar to a “Flight Recorder”
- Record all user activities in this container
- Provide a common interface for easier access by investigators or users
- Provide a capability to forensically erase user data (i.e. the recorder)

Emerging Cyber Threats

- Evolving threats are on the increase
- Goal is to steal data, create backdoors, collect keystrokes, and other confidential information on the target
- Well-Known Threats
  - Annoying
  - Script kiddies
  - Easily detected and mitigated
- Anti-Forensics Threats
  - Determined to make forensics difficult
  - Examples include using Encryption, Packing, Steganography, etc.
- Sophisticated Rootkits (“Bootkits”)
- Advanced Persistent Threats
  - Very serious attacks , well funded, coordinated
  - Profit-driven

Sophisticated Rootkits

- Hypervisor Level Rootkits are Virtual Machine Based
  - Modify a machine's boot sequence and loading as a hypervisor
  - Original OS become a VM!
  - Examples: Blue Pill (by Joanna Rutkowska) and SubVirt (by Microsoft and University of MI)
- Bootkits (Boot Level Rootkits) are boot loader rootkits that attack full disk encryption
  - Replace a legitimate boot loader with that of the adversary
  - May require physical access to system
  - "Evil Maid Attack" (requires physical access)
  - Stoned Bootkit (May not require physical access. Attacks all Windows versions from 2000 up to 7)

Sophisticated Rootkits (Contd.)

- "Cold Boot Attack" attacks Encryption Keys of Disk Encryption
  - Successful attacks have been mounted against popular disk encryption systems — FileVault, BitLocker, dm-crypt, and TrueCrypt
  - Physical Access whether in Sleep Mode, On, or Completely Off
  - Exploit the content of RAM – **-50 degrees Celsius (-58 degrees Fahrenheit)** (through Canned Air Duster Spray) and Liquid Nitrogen (-196 deg Cel != -321 deg F)

- Sources:
  1. http://en.wikipedia.org/wiki/Rootkit
  2. http://theinvisiblethings.blogspot.com/2009/10/evil-maid-goes-after-truecrypt.html
  3. http://citp.princeton.edu/pub/coldboot.pdf
  4. http://www.stoned-vienna.com/

Are Rootkits Evil to Investigators?

Rootkits may be leveraged to gain access into the data of non-cooperating suspect

Advanced Persistent Threats (APT)

- Threats posed by attackers that are organized-crime, state-, or nation-sponsored
- Skilled software programmers are recruited to develop malware
- Targets Government entities, defense, corporations, political groups, and “high-valued” organizations
- Low key and stealth attacks, developed to bypass security measures and forensics techniques
- Employs web and email as attack vectors to target their victims – through social networks, malicious websites, or **Spear-Fishing** (carefully crafted and spoof emails)

Advanced Persistent Threats (Contd.)

- Takes great skills in proactive incident response, security, forensics, and malware analysis to identify – Attacks are very difficult to detect
- Detection relies upon knowledge of host- and network-based compromise indicators
- Rushing to quick fixes (i.e. removing “affected” system) could provoke the adversary and result in reoccurrence

- Widely Publicized Example: Project Aurora (Google, etc.)

What are We Learning from APT?

- Understand the scope and extent of damage before implementing mitigation approaches
- Protect critical assets proactively, even within an internal network
- Implement carefully planned remediation strategies to prevent attacks
- Sharpen your defensive arsenal proactively**

**See Techno Security 2010 Conference Keynote Presentation by Inno Eroraha

Challenges in Key Forensic Areas

- Privacy/Encryption
- Live Volatile Data
- Memory Forensics
- Remote Forensics
- Malware Analysis
- Network Forensics
- Massive Data Collection and Analysis

Privacy/Encryption Utilities

- Privacy Software such as Anonymizers make investigation of online difficult
- Sandboxing tools may eradicate crucial evidence
- Whole/Full disk encryption
- Decryption of encrypted containers and data can result in never-ending investigation – Rootkits may help!

Live Volatile Data

- Forensic artifacts in a state of flux that can be lost when power (or network connections, in some cases) has been removed from a computing device
- Critical in forensics investigation to provide a more complete picture

Reasons to Collect Volatile Data

- May help determine criminal activity that can get lost if the system is powered off
- May contain passwords used for encryption
- May show indication of anti-forensic use
- May show memory resident malware which could go unnoticed by an examiner
- Can help avoid backlog of cases – performing live data collection avoids waiting for months for a full-blown investigation
- Critical systems cannot be shut down and require 24x7 operation to satisfy SLA or other business requirements
- Shutting down a system may create legal liability for examiners due to damage to equipment or unintentional loss of data – servers that have been running for years may not come back up after a shutdown!
- Courts request that evidence gathering be conducted using the least intrusive methods available

Order of Volatility

- Registers, cache, and peripheral memory
- Main/Physical memory
- Virtual memory (Page, Hibernation, and Swap files)
- Network State/Connections
- Running processes
- Disk
- Floppies, backup media, etc.
- Archival media, including: CD-ROMs, USB drives, etc.

Live Volatile Data – Challenges

- Ensuring integrity (using Hash) of collected information may not be easily performed
- Adhering to order of volatility
- Tested tools to support various operating system environments
- Lack of incident response capabilities or forensics readiness plan
- Untrained live data collectors
- Untested or lack of established processes and procedures
- Risk of abnormal termination of suspect machine (when memory is captured)!
- Malicious software, rootkits, or booby traps may alter outcome of information collected
- Kernel-level rootkits and malware can alter user-level tools
- Command time-stamping – helps to answer the questions: which commands were run, at what time, and with what output
- Not taking verbose notes

Memory Forensics

- Critical reservoir of information
- Volatile Data in RAM can include:
  - Data files
  - Password hashes or in plain text
  - Recent commands
  - Residual data in slack and free space
  - Running processes
  - Unencrypted/Unpacked data
  - Internet Protocol (IP) addresses
  - Instant Messages (IMs)
  - Malicious Software (“malware”)
  - Anti-forensics tools
  - Other evidentiary artifacts

Memory Forensics – Challenges

- Some memory collection may not include Hibernation File or Page (Swap) File
- Most existing tools target Windows OS RAM
- Analysis requires expertise
- Executable file (EXE or DLL) extracted from memory must be reconstructed to return it to the portable executable (PE) format
- The hash of the memory file and reconstructed file will not match
- Until recently, Memory Forensics has been slow to mature
  - Free tools:
    - Are limited to specific OS versions
    - Command-line only interfaces
    - Minimal parsing and extraction capabilities

- Sources:
  - http://www.hbgary.com/wp-content/themes/blackhat/images/the-value-of-physical-memory-for-incident-response.pdf

Remote Forensics – Challenges

- Must be deployed in advance, prior to a compromise on all potential targets, to obtain pre- and post- attack events
- Some legacy OSs may not be supported by commercial tools (Example: Linux 2.3.x, Windows 95, Windows NT, etc.)
- Speed of acquisition may pose a challenge
  - A 20 GB hard drive over a T-1 Line (1.54MB/sec) could take (20,000MB/1.54/3600 secs =) Four (4) Hours, if all goes well!
- Commercial tools may be cost-prohibitive – all organizational assets may not be covered, and ones covered may never experience an incident!

Malware Analysis

- Malware must be well tamed!
- Some malware may exhibit different behavior if they are being investigated
- Custom-Packing and Encryption makes investigations challenging
- VM environment may not always be the best environment to study them
  - Malware are capable of “jumping out” of the VM onto Host OS
  - A full-blown simulated network may be needed
- Research “lab” systems must be cleaned for the next analysis!

Network Forensics

- Relies upon existing infrastructure to support network traffic capture
- Expertise in networking port spanning or port mirroring is required to make collection possible
- Sometimes overlooked perhaps due to lack of expertise in collecting data from network devices – FWs, routers, IDS, etc.

Application Log Capturing

- Most applications lack the ability to detect and notify staff of potentially malicious activity – deferring these tasks to the firewall/IDS!
- Applications capture minimal log information for fear of performance penalty
- Even high transaction database may choose not to capture any event to prevent server performance “degradation!”
- Adequate Logs are not captured from network devices

Log Events Correlation

- Dissimilar log types (W3C, Syslog, DB, Firewall, and Windows log, etc.) must be aggregated, normalized, correlated and analyzed
- Analysis of dissimilar log events requires a tool customized to examine various log types, with real-time capability

Massive Data Collection and Analysis

- Can be very expensive and take days to collect
- Size of a storage device may require logical data collection, which may not contain critical evidence
- Centralized logging in real-time provides the ability to search massive logs

Challenges Posed by the Legal System

- 4th Amendment
  - Using a warrant to legally seize and search a computer
  - Types of files that are allowed to be searched may be limited
- State Laws are now requiring PI license to conduct computer forensics
  - Virginia, Texas, Michigan, South Carolina, etc.
- Corporate policies and procedures regarding investigations

Summary

- Get well-rounded training in other forensics specialties and OS platforms
- Be aware of hackers techniques and devise appropriate countermeasures
- Adapt our mindsets about hackers:
  - If you think like an attacker, you would say:
    - The hacker is going to portscan or exploit a known vulnerability before penetrating
  - ...But the attackers know we are thinking like them, so:
    - The hacker may not portscan or exploit a known vulnerability before penetrating
- Know the laws and your limitations

Direct Comments/Questions to:

Inno@NetSecurity.com