Digital Forensics Investigation

Nicolas Villatte
RISK Labs EMEA Manager
Digital Forensics

A part of the overall incident handling process
## Governance and Standards

### Legal & Regulatory Requirements

**US Federal:**
- HITECH – Health Information Technology for Economic and Clinical Health Act (2009)

**European Community:**
- EU Directive 2009/140/EC Article 13a

### Good Practices & Standards

**Guidance:**
- NIST Special Publication 800-61 R2 – Computer Security Incident Handling Guide
- ENISA Technical Guideline on Incident Reporting
- SANS Institute (various)

**Accepted Standards:**
- ISO 27001/27002 – International Organization for Standardization
- PCI-DSS – Payment Card Industry

### Evidence Handling Compliance

- FRCP – Federal Rules of Civil Procedure
- FRE – Federal Rules of Evidence
- ACPO – Good Practice Guide for Digital Evidence
Incident Response Stakeholders (1/2)

- Information Security Organizations
- Business Organizations
- Information Technology (IT) Organizations
- Legal
- Human Resources
- Corporate Communications / Public Relations

*It ultimately depends on the situation...*
Incident Response Stakeholders (2/2)

Incident Response Process

Source: NIST SP 800-61, R2, Computer Security Incident Handling Guide
Digital Forensics Process

Source: NIST SP SP800-86, Guide to Integrating Forensic Techniques into Incident Response
Incident Response

Preparation Phase
Incident Response Preparation (1/2)

- Governance, Risk & Compliance
  - Data Classification
  - Risk and Business Impact Analysis
  - Policies and Standards
  - Security Infrastructure
  - Prevention
  - Monitoring
  - **Logging**
Incident Response Preparation (2/2)

- Incident Response Plan Development & Testing (Mock Incidents)
- Incident Classification
- Incident Escalation Process
  - Stakeholders Identification
  - Roles & Responsibilities (RACI)
  - Incident Response Team – Organizational Structure
- Training
- Documentation and Communication Steps
- Incident Resolution Workflows and Methodology (pre-made decisions e.g. pull the plug, contact Law Enforcement Agency …)
- Post-mortem
Digital Forensics Case Management

- It is not just an Incident Response Task Tracking / Ticketing System!!
- Everything related to case management and linked together
  - Contacts and contracts database
    - Customers
    - Budget allowance
    - Suppliers
    - Third-party
    - Resources
  - Documents repository
  - Resources management:
    - Tasks assignment and follow-up to completion
    - Time allowance
    - Communication workflows
  - Asset Management / Evidence Handling
Here comes the incident

Digital Forensics Investigation will start if the incident has been validated...
Initial Triage

- Events Vs Incident validation
  - Incident classification
  - Incident categories
  - Attack vector
  - Target
- Incident prioritization
- Documentation (Forensics Vs IR)
  - Actions taken
  - Evidence collected
  - Logbook
- Notification(s) and Escalation(s)
  - Actionable Information
  - Organizational
  - Special reporting requirements
    - LE / PCI / PII
Engagement Scoping (1/2)

• What happened
  • Identify Target(s)
  • Identify Attack Vector(s)
  • Identify Timings
  • Determine likely scenario(s)
• Visualize / Gather information about in-scope environment
  • Network Maps and Data Flows
  • Policies and Standards
  • Systems in scope and possible sources of evidence
Engagement Scoping (2/2)

- Prioritize Actions
  - Evidence Collection
  - Additional Analysis and Examination
  - Containment, Eradication and Recovery
- Mind the legal aspects:
  - Expectation of privacy
  - Authority to seize company property
Evidence Handling
Forensically Sound Collection

- Make sure backup rotation is halted for in-scope data and preserve all possible evidence
- Establish a repeatable process
- Minimize interaction with the system and preserve the scene
  - Pull the network cable Vs shut the system down
  - If it is off, don’t turn it on
  - Don’t patch / run antivirus before
  - Use your prepared / known collection toolkit
- Collect by observing the order of data volatility
- Follow evidence handling procedures
Find the Evidence

Where to find data?

EVERYWHERE
Evidence Handling (1/5)

- Definition: Relevance & Admissibility
- Evidence Identification
Evidence Handling (2/5)

- Evidence Label
- Evidence Working Copy
Evidence Handling (3/5)

- Data Protection & Evidence Storage
- Physical Security and Damage Control
- Encryption
Evidence Handling (4/5)

- Integrity
- Write-Blocker
- Evidence bags
- Hashing
Evidence Handling (5/5)

- Evidence Documentation
- Chain of Custody
- Logbook

### Digital Evidence Chain of Custody Form

<table>
<thead>
<tr>
<th>Description of Item:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item 1: Western Digital 2.5&quot; External USB Hard Drive; Model WD3200ME; S/N: AB123456; containing the following forensic images:</td>
</tr>
<tr>
<td>Hard_drive E01</td>
</tr>
<tr>
<td>Hard_drive E02</td>
</tr>
<tr>
<td>Hard_drive E03</td>
</tr>
<tr>
<td>Hard_drive E04</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case No: ABC-0001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page: 1 of 1</td>
</tr>
</tbody>
</table>

**Released By:**

**Name / Title:** John Doe / Incident Response Manager

**Received By:**

**Name / Title:** Jack Sparrow / Forensic Investigator

**Signature:**

John Doe

**Signature:**

Jack Sparrow

**Date / Time:** 1/22/09 1:55 PM

**Reason:** Transfer of custody to conduct forensic analysis
Challenges

• Full disk encryption
• Proprietary RAID configurations
• Proprietary appliance systems
• Cloud service providers aspects
  • Accessibility of customer server
  • Guest system access
  • Co-location and shared services
  • International and cross-border aspects
• The more the device is mobile, the more personal it becomes
• Cat & mouse game with the attacker
  • The mouse is watching you!
• Anti-forensics
  • Timestamps modification
  • Stealth – hidden/overlooked locations, files…
• Encryption / Steganography
Examination & Analysis
Examination & Analysis (1/2)

- Memory analysis
- File system analysis
  - User created files
    - Documents
    - Web surfing / Chatting
    - E-mails
  - System created files
    - Log files
    - Temporary files
    - Windows registry
- Other locations
  - Metadata
  - Unallocated space
  - Slack space
- Network analysis
- Mobile devices analysis
- Malware analysis
  - Behavioral analysis
  - Reverse engineering
Examination & Analysis (2/2)

- Keyword searches
- File signature analysis
- Hash analysis
- File recovery
- Web browser artifacts
- LNK files
- Recycle Bin / INFO2 record
- Prefetch files
- Windows registry
  - Autorun locations
  - MRU lists
  - Mounted devices
  - Typed URLs
- Timeline analysis
Threat Intelligence Sharing

- Verizon DBIR App for
- CERTs collaboration
  - Honeybot
  - MISP
  - Passive DNS
  - Passive SSL
- PCI SSCouncil for payment card fraud investigations
- Eventual transition to Law Enforcement
  - Via investigation report
Threat intelligence: IoC feeds overlap

Overall IOC are 97% unique on analyzed sample over 6 months period.
## Threat intelligence: Frequency of IoC types shared

<table>
<thead>
<tr>
<th>COMMUNITY</th>
<th>IP ADDRESSES</th>
<th>E-MAIL ADDRESSES</th>
<th>FILES</th>
<th>HOSTS</th>
<th>URLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Community</td>
<td>35.9%</td>
<td>1.0%</td>
<td>23.3%</td>
<td>33.0%</td>
<td>6.8%</td>
</tr>
<tr>
<td>Event-Based Community #1</td>
<td>77.4%</td>
<td>0.1%</td>
<td>2.5%</td>
<td>19.5%</td>
<td>0.5%</td>
</tr>
<tr>
<td>Industry Community #1</td>
<td>16.5%</td>
<td>32.3%</td>
<td>6.3%</td>
<td>43.0%</td>
<td>1.9%</td>
</tr>
<tr>
<td>Industry Community #2</td>
<td>47.1%</td>
<td>4.4%</td>
<td>10.3%</td>
<td>29.4%</td>
<td>8.8%</td>
</tr>
<tr>
<td>Industry Community #3</td>
<td>8.3%</td>
<td>0.3%</td>
<td>1.2%</td>
<td>87.5%</td>
<td>2.7%</td>
</tr>
<tr>
<td>Industry Community #4</td>
<td>25.2%</td>
<td>2.4%</td>
<td>9.0%</td>
<td>58.6%</td>
<td>4.8%</td>
</tr>
<tr>
<td>Industry Community #5</td>
<td>50.9%</td>
<td>0.7%</td>
<td>1.3%</td>
<td>22.8%</td>
<td>24.4%</td>
</tr>
<tr>
<td>Industry Community #6</td>
<td>66.4%</td>
<td>0.6%</td>
<td>14.0%</td>
<td>13.8%</td>
<td>5.2%</td>
</tr>
<tr>
<td>Industry Community #7</td>
<td>59.1%</td>
<td>0.5%</td>
<td>1.4%</td>
<td>23.5%</td>
<td>15.5%</td>
</tr>
<tr>
<td>Industry Community #8</td>
<td>39.6%</td>
<td>3.0%</td>
<td>7.7%</td>
<td>36.9%</td>
<td>12.8%</td>
</tr>
<tr>
<td>Industry Community #9</td>
<td>51.5%</td>
<td>2.6%</td>
<td>12.6%</td>
<td>23.8%</td>
<td>9.5%</td>
</tr>
<tr>
<td>Regional Threat Community #1</td>
<td>49.2%</td>
<td>0.3%</td>
<td>4.5%</td>
<td>42.6%</td>
<td>3.4%</td>
</tr>
<tr>
<td>Regional Threat Community #2</td>
<td>50.0%</td>
<td>1.1%</td>
<td>4.5%</td>
<td>30.8%</td>
<td>13.6%</td>
</tr>
<tr>
<td>Subscriber Community</td>
<td>45.4%</td>
<td>1.2%</td>
<td>18.4%</td>
<td>24.4%</td>
<td>10.6%</td>
</tr>
<tr>
<td>Threat-Based Community #1</td>
<td>50.3%</td>
<td>1.1%</td>
<td>11.0%</td>
<td>24.3%</td>
<td>13.3%</td>
</tr>
</tbody>
</table>
Threat intelligence: IoC: Count of days observed

We need to close the gap between sharing speed and attack speed.
Reporting (1/2)
Reporting (2/2)

- Report title, author’s name, company name, versioning information
- Distribution list
- Executive summary
- Case Description
- Scope of the investigation / assignment
- List of evidence items
- Investigative actions and results
- Recommendations
- Glossary (Appendix)
- Detailed additional relevant information (Appendix)
- Transition to Law Enforcement
Case study

An industrial espionage attempt story
Case study – The context
Case study – investigation results

INVESTIGATION REVEALED

— Lack of employee security awareness program;
— Lack of strong authentication for remote users to access OWA;
— Malware undetected by antivirus;
— Lack of consistent log files retention;
— Lack of monitoring;
— No incident response plan in place (response was not bad, but could have been better);
— No network security monitoring
— No proxy server preventing control of domain name based flows
— No pro-active vulnerability assessment in place
— No Mobile device security policy in place (e.g. devices were not easily available for investigation)
— Policies preventing the execution of e-mail attachments in sensitive environment;
— Upon detection of the incident, quick appropriate primary response – disconnecting the potentially infected computer from the network
LESSONS LEARNED

— Educate users to detect spearphishing, MITM attempts and bad SSL certificates;
— Implement stronger remote access controls (Two-factor/OTP)
— Deploy proxy servers to control flows in and out of the infrastructure on a domain name basis;
— Make sure network security monitoring is in place;
— Make sure there is an incident response plan in place that addresses log files retention;
— Apply system hardening guidelines and develop security policies including for mobile devices;
— Proactively scan your own infrastructure for vulnerabilities and patch vulnerable applications periodically;
Thank You