Live Incident Response
The Law Enforcement Perspective

Assistant Special Agent-in-Charge
Daniel Persson
OVERVIEW

- Background
- Law Enforcement (LE) Mindset
- Collection of Evidence
- Triage
- Final Thoughts
Background
Current Duties

- Assistant Special Agent-in-Charge OIG Technology Crimes Section (TCS)
  - Handle all LE related Tech Crimes for DOE
  - Digital media analysis
  - LE-centric intrusion cases
  - CP cases in DOE complex
  - LE POC for DOE in all joint investigations
    - FBI, AFOSI, ICE, etc
What I Don’t Do

- I am not a Lawyer
- I am not an Auditor
- I don’t create DOE policy
  - How can IG create and audit policy?
  - How can I define what DOE policy is?
- I don’t investigate APT – other people do
Current Problem: “How can we take the traditional LE mindset and apply it to today’s Incident Response environment?”
Law Enforcement (LE) Mindset
Catch the Bad Guys
Traditional Law Enforcement Mindset
- Seize physical evidence (drugs, body)
- Don’t alter the item
- Remove it from the scene
- Analyze it later
- Reference the original at all times
Computer Evidence is Different

- Physical computer vs. resident data
- Corrupting data part of collection
- Data lost during shut down
- Seizure re-victimizes Department
  - Hardware loses value
  - Reacquire hardware
  - Restore data from good backup
- Easy to collect too much
Evidence Collection
Forensic Computer Imaging
Digital Evidence Importance

- Holds evidence of a crime
  - Copies of fraudulent contracts
  - Emails showing Intellectual Property theft
  - Contacts in an online counterfeit ring

- Holds evidence about a crime
  - Timestamps on files used by attacker
  - TCP network connection to IP address
  - USB serial number entry in registry (USBSTOR)
What Can We Capture?

- **RAM**
  - RAM resident malware
  - Keys/passwords
  - Data fragments
  - Unpacked executables

- **Processes**
  - Source
  - Links
  - Scheduled
– Networking
  ● Active/listening/recent connections
  ● Routing tables
  ● Services listening on specific ports
– Logons
  ● Users remotely logged on
  ● Systems connected to shares
  ● Recent activity
- Services
  - What’s listening
  - What’s running
- DLL shared libraries
- File handles

**Whatever we don’t collect we lose**
- Far more challenging to recreate on dead box
- Some data can’t be recreated (e.g. RAM)
Methodology

- Have a plan!
– Learn tools
  ● Limitations
  ● Affect on system
– Test on non-production systems
  ● Various OS versions
  ● Different user levels
– Static binaries
  ● Helix CD/website
  ● Tested production binaries
– Set up proper collection process
  ● RAM should be 1st
  ● Use RFC 3227 Order of Volatility as guideline

– Repeatable (scripted) process
  ● Recreate steps at a later date
  ● Avoids missing steps
  ● Train new members quickly
  ● Rapid remote deployment
RAM Collection – Winen

- Created by Guidance Software
  - Large forensic firm
  - Numerous in-house developers
- Included on Helix CD
- Allows for case metadata
RAM Collection – MDD
- Created by ManTech International
- Included on Helix CD
- Some known issues
  - 2008 Server
  - Windows Vista/7
Live RAM Acquisition

Guidance Software
Version 6.12.0.44

Mantech MDD
Version 1.3

Matthew Suiche win32dd
Version 1.2.1.20090106

HELIX Forensic Command Shell

Ctrl-D for Directory or Ctrl-P for filename completion
The Shell Path has been modified to find trusted cron binaries first
Do not navigate away from the CD drive letter.

17:52:14.46 D:\IR\RAM-MDD> type mddusage.txt
mdd ManTech Physical Memory Dump Utility
Usage:
   mdd <--OUTPUTFILE> [-qew]
       -e OUTPUTFILE  output file for dump
       -q quiet; no output except on error
       -v verbose; output offsets of failed mappings
       -w redistribution conditions for GPL
       -w warranty information for GPL

17:52:31.61 D:\IR\RAM-MDD>
RAM Collection – FTK Imager 2.9

- Created by AccessData
  - Large forensic firm
  - Numerous in-house developers

- *Not included on Helix CD (2.5.3)*
  - Current version on Helix doesn’t support RAM
RAM Collection – Helix Pro

- Created by e-fense
  - Makers of Helix forensic CDs
  - Well known in IR community
- Flexible output
  - Attached drive
  - Networked to system running Helix Pro receiver
- Paid subscription required
Volatile Data Collection – Sysinternals

- Purchase by Microsoft
  - Created by Mark Russinovich
  - Long use in IR community

- Numerous capabilities
  - Command line tools
  - GUI tools
Volatile Data Collection – ICRR

- Included on Helix CD
- Scripted data collection
  - Output to a netcat listener
  - Large text file
- Numerous interactive messages
  - Need to monitor while running
  - Sysinternals EULAs on screen
Volatile Data Collection – Helix Pro

- Simple GUI interface
- Flexible output
  - Attached drive
  - Networked to system running Helix Pro receiver
- Paid subscription required
Volatile Data Collection – e-fense

- Live Response/Aperio
  - USB drive based
  - Automated collection and storage
– Live Response/Aperio
  ● Automated collection = “Agent Proof”
  ● Centralized analysis console
Triage
Collection was Initial Challenge
New Challenge – Rapid Analysis
- Quickly aggregate and compare data
- Still labor intensive
- Aspects of interest
  - What ports connected
  - IP addresses utilized
  - Processes (names, sources, utilization)
  - Find a commonality
Enterprise Level Platforms

- Have hook into systems
- Common output/reporting
- No need for physical access to computer
- Pre-deployed agent
- Require network access to system
- Ensure agent is working and communicating
Non-Enterprise Level
- Much more challenging
- Need collection/analysis tools
- Requires physical access to systems
Triage Tools- Live Response/Aperio

- Centralized collection
- Easy to run multiple cases concurrently
- Comparison between systems cumbersome
- Extensive reports
### Processes

<table>
<thead>
<tr>
<th>PID</th>
<th>Process</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>System</td>
<td>System Idle Process</td>
</tr>
<tr>
<td>4</td>
<td>System</td>
<td>System</td>
</tr>
<tr>
<td>1316</td>
<td>smss.exe</td>
<td>%SystemRoot%System32\smss.exe</td>
</tr>
<tr>
<td>1372</td>
<td>csrss.exe</td>
<td>%SystemRoot%System32\csrss.exe</td>
</tr>
<tr>
<td>1404</td>
<td>winlogon.exe</td>
<td>%SystemRoot%System32\winlogon.exe</td>
</tr>
<tr>
<td>1460</td>
<td>services.exe</td>
<td>%SystemRoot%System32\services.exe</td>
</tr>
</tbody>
</table>

### Processes

<table>
<thead>
<tr>
<th>Base</th>
<th>Version</th>
<th>Path</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1000000</td>
<td>5.1.2600.5755</td>
<td>%SystemRoot%System32\winlogon.exe</td>
<td>5288</td>
</tr>
<tr>
<td>0x7C900000</td>
<td>5.1.2600.5781</td>
<td>%SystemRoot%System32\ntdll.dll</td>
<td>7290</td>
</tr>
<tr>
<td>0x7C800000</td>
<td>5.1.2600.5781</td>
<td>%SystemRoot%System32\kernel32.dll</td>
<td>1000</td>
</tr>
<tr>
<td>0x77D00000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\advapi32.dll</td>
<td>6344</td>
</tr>
<tr>
<td>0x77E00000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\rpcrt4.dll</td>
<td>5984</td>
</tr>
<tr>
<td>0x77E00000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\secur32.dll</td>
<td>6960</td>
</tr>
<tr>
<td>0x77C00000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\authz.dll</td>
<td>7377</td>
</tr>
<tr>
<td>0x77C10000</td>
<td>7.0.2600.5512</td>
<td>%SystemRoot%System32\msvcr1.dll</td>
<td>3600</td>
</tr>
<tr>
<td>0x77A00000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\crypt32.dll</td>
<td>6100</td>
</tr>
<tr>
<td>0x77B00000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\msasn1.dll</td>
<td>7377</td>
</tr>
<tr>
<td>0x77E00000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\mssec.dll</td>
<td>5930</td>
</tr>
<tr>
<td>0x77F00000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\gdi32.dll</td>
<td>2999</td>
</tr>
<tr>
<td>0x75940000</td>
<td>5.1.2600.5512</td>
<td>%SystemRoot%System32\ntdll.dll</td>
<td>3270</td>
</tr>
</tbody>
</table>
Triage Tools - Mandiant First Response

- Centralized collection
  - Pre-deployed agents
  - Individual system collection

- Easy comparison between systems
  - Compare specific aspects
    - Processes
    - Ports
  - Ability to add analysis notes to file
Final Thoughts
Identify Commonalities between Attacks
- Tie attacks together
- Determine Modus Operandi
- Create profile

Trace Attacks to Common Sources
- IPs
- Servers
- Controllers
Gather Info at Service Provider Level

- 2703(f) Preservation Letters
  - Provides time to get Court Order
  - Notifies service provider of intent
- 2703(d) Disclosure
  - Provides customer communications
  - Provides customer records
Use Info Gathered

- Profile of attack and user data
  - Determine attribution
  - Attempt to serve warrant on individual(s)
  - Present case for prosecution - Federal Court System
- Share information with LE partners
  - Gather history on person or group
  - Provide common threat picture
Work with Cyber Security
- CS knows systems, networks, processes best
- Don’t want to be stumbling block in process
- Augment process by running parallel with copy of evidence
  - Provide attribution when possible
  - Provide deterrent
  - De-conflict with
    - FBI, USSS, DOD, ICE
    - CI and Intel elements
Questions?