Memory Forensics: Collecting & Analyzing Malware Artifacts from RAM

ISSA DC Chapter

March 15, 2011

Presented by:
Inno Eroraha, CISSP, CISM, CHFI, PI
NetSecurity Corporation
21351 Gentry Drive, Suite 230
Dulles, VA  20166
Agenda

- Why Memory Forensics?
- Type of Memory
- Collection Approaches
  - Remote
  - Local
- Collection Techniques and Tools
- Analysis Techniques and Tools
- Conclusion
Memory Forensics Questions...

- What processes were running on the suspect system at the time memory image was taken?
- What (hidden or closed) processes existed?
- Are there any (hidden or closed) network connections?
- Are there any (hidden or closed) sockets?
- What is the purpose and intent of the suspected file?
- Are there any suspicious DLL modules?
- Are there any suspicious URLs or IP addresses associated with a process?
- Are there any suspicious open files associated with a process?
- Are there any closed or hidden files associated with any process?
Memory Forensics Questions...
(Contd.)

- Are there any suspicious strings associated with a particular process?
- Are there any suspicious files present? Can you extract them?
- Can you extract malicious processes from the memory and analyze it?
- Can you identify the attackers and their IP addresses?
- Did the attacker create a user account on the system?
- Did the malware modify or add any registry entry?
- Does the malware use any type of hooks to hide itself?
- Did the malware inject itself to any running processes?
- What is the relationship between different processes?
- What is the intent and purpose of this malware?
Real-World Scenario

The Problem:
- Ted, a Marketing Director, at OjeheTrade & Co Inc., received a Hallmark E-Greeting Card from a colleague, Maria.
- When Ted opened the E-Greeting Card, it opened a graphic image of animals.
- When Ted saw Maria later in the day, he thanked her for the E-Greeting Card.
- Maria told Ted that she did not send him any E-greeting card!
- Ted called Mike, the Network Security Lead, and told him what happened.
- Mike asked one of his Security Analysts to make a Memory Image of Ted’s computer.

Your Task:
- You are a Security Analyst at OjeheTrade & Co, Inc., tasked to investigate the incident.
- How would you go about performing this investigation if all you have is the Memory image?

Memory Forensics: Collecting and Analyzing Malware Artifacts from RAM
MEMORY ACQUISITION
RAM Acquisition Tools

- **Winen** (Guidance Software)
- **FastDump Pro** (HB Gary) - Limited Free version available
- **FTK Imager** - Free
- **DD**  Free but limited - May not work on later versions of Windows
- **WinHex** - Has some limitations
- **Nigilant32**  - Free but for 32-bit systems only
- **Memoryze** (Mandiant) - Free
RAM Acquisition with FTK Imager

Memory Forensics: Collecting and Analyzing Malware Artifacts from RAM
RAM Acquisition with DD

- MDD_1.3.exe by ManTech
- DD in Unix
MEMORY ANALYSIS
RAM Analysis Tools

- Some commercial forensics tools have built-in capabilities
- Volatility Framework
- Mandiant Memoryze
- HB Gary Responder
Volatility supports the following extraction capabilities for memory images:

- Image date and time
- Running processes
- Open network sockets
- Open network connections
- DLLs loaded for each process
- Open files for each process
- Open registry keys for each process
- Memory maps for each process
- Extract executable samples
- Scanning examples: processes, threads, sockets, connections, modules
## Volatility Modules

<table>
<thead>
<tr>
<th>Image Identification</th>
<th>Processes and DLLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageinfo</td>
<td>pplist</td>
</tr>
<tr>
<td>datetime</td>
<td>pstree</td>
</tr>
<tr>
<td>kdbgscan</td>
<td>psscan2</td>
</tr>
<tr>
<td>Kprcscan</td>
<td>dlllist</td>
</tr>
<tr>
<td></td>
<td>dlldump</td>
</tr>
<tr>
<td></td>
<td>files</td>
</tr>
<tr>
<td></td>
<td>regobjkeys</td>
</tr>
<tr>
<td></td>
<td>getsids</td>
</tr>
<tr>
<td></td>
<td>verinfo</td>
</tr>
<tr>
<td>Process Memory</td>
<td></td>
</tr>
<tr>
<td>memmap</td>
<td></td>
</tr>
<tr>
<td>memdump</td>
<td></td>
</tr>
<tr>
<td>procmemdump</td>
<td></td>
</tr>
<tr>
<td>procdump</td>
<td></td>
</tr>
<tr>
<td>vadwalk</td>
<td></td>
</tr>
<tr>
<td>vadtrees</td>
<td></td>
</tr>
<tr>
<td>vadinfo</td>
<td></td>
</tr>
<tr>
<td>vaddump</td>
<td></td>
</tr>
<tr>
<td>Kernel Memory and Objects</td>
<td></td>
</tr>
<tr>
<td>modules</td>
<td></td>
</tr>
<tr>
<td>modscan2</td>
<td></td>
</tr>
<tr>
<td>moddump</td>
<td></td>
</tr>
<tr>
<td>ssdt</td>
<td></td>
</tr>
<tr>
<td>driverscan</td>
<td></td>
</tr>
<tr>
<td>filesystem</td>
<td></td>
</tr>
<tr>
<td>mutantscan</td>
<td></td>
</tr>
<tr>
<td>thrdscan2</td>
<td></td>
</tr>
</tbody>
</table>
### Volatility Modules (Contd.)

<table>
<thead>
<tr>
<th>Networking</th>
<th>Malware and Rootkits</th>
</tr>
</thead>
<tbody>
<tr>
<td>connections</td>
<td>malfind</td>
</tr>
<tr>
<td>connscan2</td>
<td>svcscan</td>
</tr>
<tr>
<td>sockets</td>
<td>ldrmodules</td>
</tr>
<tr>
<td>sockscan</td>
<td>impscan</td>
</tr>
<tr>
<td>netscan</td>
<td>apihooks</td>
</tr>
<tr>
<td></td>
<td>idt</td>
</tr>
<tr>
<td></td>
<td>gdt</td>
</tr>
<tr>
<td>Registry</td>
<td>orphanthreads</td>
</tr>
<tr>
<td>hivescan</td>
<td>callbacks</td>
</tr>
<tr>
<td>hivelist</td>
<td>driverirp</td>
</tr>
<tr>
<td>printkey</td>
<td>psxview</td>
</tr>
<tr>
<td>hivedump</td>
<td>ssdt_ex</td>
</tr>
<tr>
<td>hashdump</td>
<td>ssdt_by_threads</td>
</tr>
<tr>
<td>lsadump</td>
<td></td>
</tr>
</tbody>
</table>
## Volatility Modules (Contd.)

<table>
<thead>
<tr>
<th>Crash Dumps, Hibernation, and Conversion</th>
<th>Miscellaneous</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashinfo</td>
<td>strings</td>
</tr>
<tr>
<td>hibdump</td>
<td>volshell</td>
</tr>
<tr>
<td>hibinfo</td>
<td>bioskbdd</td>
</tr>
<tr>
<td>imagecopy</td>
<td>inspectcache</td>
</tr>
</tbody>
</table>

**Source:**
http://www.forensicswiki.org/wiki/List_of_Volatility_Plugins
http://code.google.com/p/volatility/wiki/CommandReference
Volatility Usage

```
usage: volatility cmd [cmd_opts]

Run command cmd with options cmd_opts
For help on a specific command, run 'volatility cmd --help'

Supported Internet Commands:
connections  Print list of open connections
connscan    Scan for connection objects
connscan2   Scan for connection objects (New)
dotstat     Get date/time information for image
dlllist     Print list of loaded dll's for each process
dmp2raw     Convert a crash dump to a raw dump
dmpchk      Dump crash dump information
dumpfiles   Print list of open files for each process
hibernfo    Convert hibernation file to linear raw image
ident       Identify image properties
mmap        Dump the addressable memory for a process
mmap      Print the memory map
modscan     Scan for modules
modscan2    Scan for module objects (New)
modules     Print list of loaded modules
procdump    Dump a process to an executable sample
pslist      Print list of running processes
psscan      Scan for EPROCESS objects
psscan2     Scan for process objects (New)
raw2dmp     Convert a raw dump to a crash dump
regkeys     Print list of open regkeys for each process
sockets     Print list of open sockets
socketscan  Scan for socket objects
socketscan2 Scan for socket objects (New)
strings     Match physical offsets to virtual addresses (may
take a while, VERY verbose)
threadscan  Scan for ETW objects
threadscan2 Scan for thread objects (New)
vad2dmp     Dump the Vad sections to files
vadinfo     Dump the Vad info
vadwalk     Walk the vad tree

Supported Plugin Commands:
cryptoscan  Find TrueCrypt passphrases
malfind2    Detect hidden and injected code
mmapmap     Print the memory map
orphan_threads Find kernel threads that don't map back to loaded
modules     
pslist       Print list running processes
pslist2      Print list running processes
pslist3      Print list running processes
pslist4      Print list running processes
pslist5      Print list running processes

Example: volatility pslist -f /path/to/my/file
```
Working with RAM Images

- Image Identification
  - `volatility ident -f HOHTLE4.vmem`

- Identify Suspicious Processes
  - `volatility pslist -f HOHTLE4.vmem`
  - `volatility psscan2 -f HOHTLE4.vmem` (EXITED!)

- Identify active, hidden or closed connections
  - `volatility connections -f HOHTLE4.vmem`
  - `volatility connscan2 -f HOHTLE4.vmem` (hidden)
Working with Images (Cont.)

- Identify active, hidden or closed
  - volatility sockets -f HOHTLE4.vmem
  - volatility sockscan2 -f HOHTLE4.vmem (hidden)

- Identify suspicious dlls and any open, hidden or closed files
  - volatility dlllist -f HOHTLE4.vmem
  - volatility files -f HOHTLE4.vmem > files.txt
  - volatility fileobjscan -f HOHTLE4.vmem > fileobjscan.txt (hidden)
Identify suspicious strings for each suspect process

- `volatility memdmp -f HOHTLE4.vmem -p <PID> > PID.dmp`
- `strings PID.dmp > PID_ASCII.txt`

Extract Executable (EXE)

- `volatility procdump -f HOHTLE4.vmem -p <PID>`

Verify Online at VirusTotal, VirusScan, etc.
<table>
<thead>
<tr>
<th>Vendor</th>
<th>Version</th>
<th>Date</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortinet</td>
<td>4.1.143.0</td>
<td>2010.07.29</td>
<td>W32/MyDocm.fam8mm</td>
</tr>
<tr>
<td>GData</td>
<td>21</td>
<td>2010.07.29</td>
<td>Win32.Worm McMaggot.A</td>
</tr>
<tr>
<td>Ikarus</td>
<td>T3.1.1.84.0</td>
<td>2010.07.29</td>
<td>Trojan.Win32.Genome</td>
</tr>
<tr>
<td>Jiangmin</td>
<td>13.0.900</td>
<td>2010.07.29</td>
<td>-</td>
</tr>
<tr>
<td>Kaspersky</td>
<td>7.0.0.125</td>
<td>2010.07.29</td>
<td>Trojan.Win32.Genome.hjtyt</td>
</tr>
<tr>
<td>McAfee</td>
<td>5.400.0.1158</td>
<td>2010.07.29</td>
<td>Generic.dx</td>
</tr>
<tr>
<td>Microsoft</td>
<td>1.6004</td>
<td>2010.07.29</td>
<td>Worm:Win32/Prolaco</td>
</tr>
<tr>
<td>NOD32</td>
<td>5322</td>
<td>2010.07.29</td>
<td>Win32/Mydoom.NAI</td>
</tr>
<tr>
<td>Norman</td>
<td>6.05.11</td>
<td>2010.07.29</td>
<td>W32/Mydoom.ER</td>
</tr>
<tr>
<td>nProtect</td>
<td>2010-07-29.01</td>
<td>2010.07.29</td>
<td>Win32.Worm McMaggot.A</td>
</tr>
<tr>
<td>Panda</td>
<td>10.0.2.7</td>
<td>2010.07.28</td>
<td>W32/Mydoom.HY.worm</td>
</tr>
<tr>
<td>PCTools</td>
<td>7.0.3.5</td>
<td>2010.07.29</td>
<td>Spyware.007Spy</td>
</tr>
<tr>
<td>Frewx</td>
<td>3.0</td>
<td>2010.07.29</td>
<td>-</td>
</tr>
<tr>
<td>Rising</td>
<td>22.58.03.04</td>
<td>2010.07.29</td>
<td>-</td>
</tr>
<tr>
<td>Sophos</td>
<td>4.55.0</td>
<td>2010.07.29</td>
<td>Mal/Generic-A</td>
</tr>
<tr>
<td>Sunbelt</td>
<td>6658</td>
<td>2010.07.29</td>
<td>Trojan.Win32.Generic!BT</td>
</tr>
<tr>
<td>SUPERAntiSpyware</td>
<td>4.40.0.1006</td>
<td>2010.07.29</td>
<td>-</td>
</tr>
<tr>
<td>Symantec</td>
<td>20101.1.1.7</td>
<td>2010.07.29</td>
<td>Spyware.007Spy</td>
</tr>
</tbody>
</table>
Data Carving Using Foremost

- **Foremost**
  - `foremost -c foremost.conf -t exe -i <PID>.dmp -o output3`
Scan for Registry Artifacts

- volatility hivescan -f HOHTLE4.vmem
- volatility hivelist -f HOHTLE4.vmem -o 0x212cb60
Analyzing Extracted Executables

- Using the resulting EXE from “procdump,” analyze the EXE further
- Scan using Anti-Virus
- Run in a Virtual Machine
  - Analyze using Static means
  - Analyze using Dynamic means
  - Perform Code Analysis
QUESTIONS & ANSWERS