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 Ojehtrade & 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:

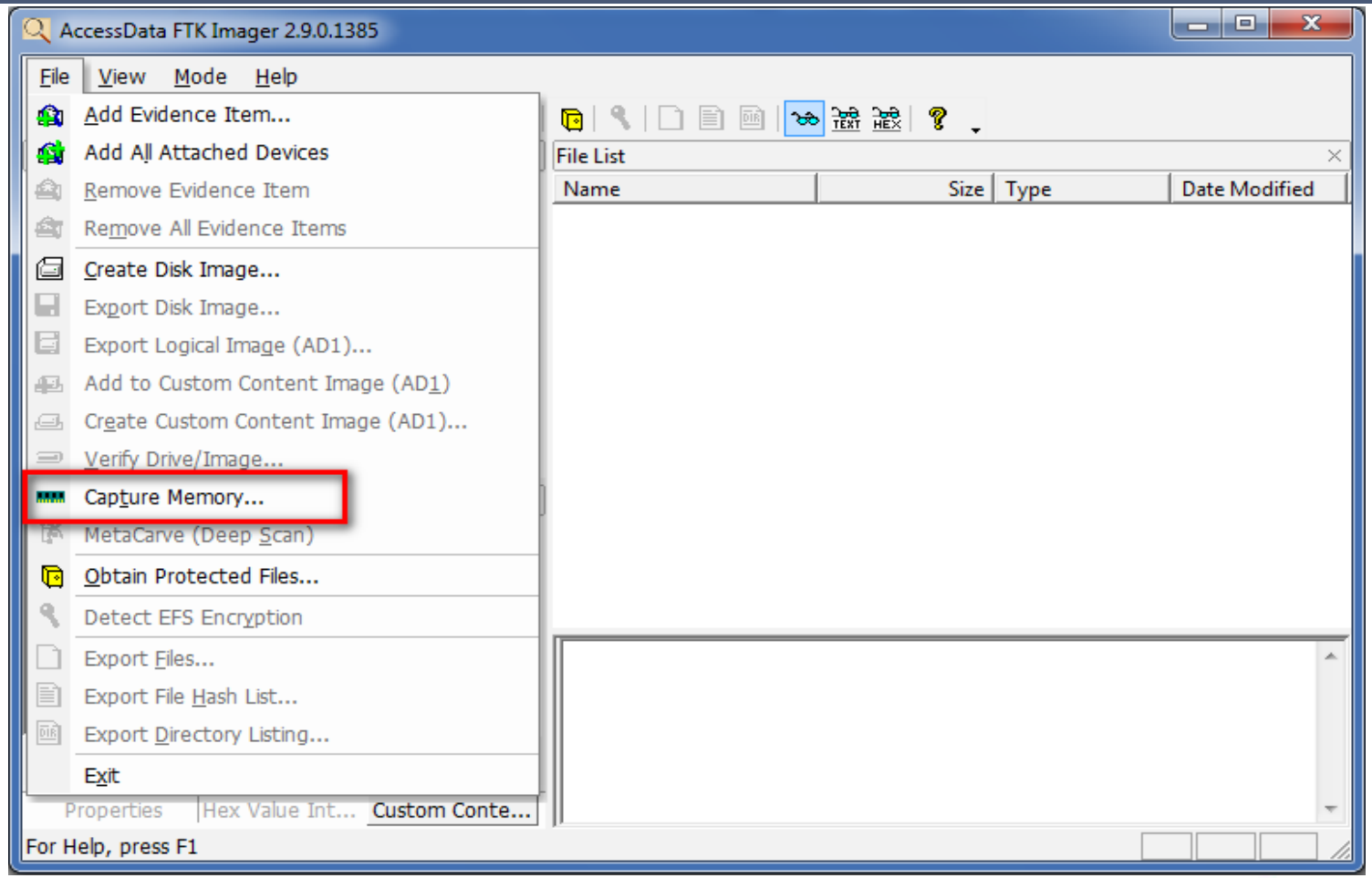
- You are a Security Analyst at Ojehtrade & Co, Inc., tasked to investigate the incident
- How would you go about performing this investigation if all you have is the Memory image?

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



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 Framework

- 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

Image Identification
- imageinfo
- datetime
- kdbgscan
- Kprcscan

Process Memory
- memmap
- memdump
- procmemdump
- procexedump
- vadwalk
- vadtree
- vadinfo
- vaddump

Processes and DLLs
- pslist
- pstree
- psscan2
- dlllist
- dlldump
- files
- regobjkeys
- getsids
- verinfo

Kernel Memory and Objects
- modules
- modscan2
- moddump
- ssdt
- driverscan
- filescan
- mutantscan
- thrdscan2

Volatility Modules (Contd.)

Networking

- connections
- connscan2
- sockets
- sockscan
- netscan

Registry

- hivescan
- hivelist
- printkey
- hivedump
- hashdump
- lsadump

Malware and Rootkits

- malfind
- svcscan
- ldrmodules
- impscan
- apihooks
- idt
- gdt
- orphanthreads
- callbacks
- driverirp
- psxview
- ssdt_ex
- ssdt_by_threads

Volatility Modules (Contd.)

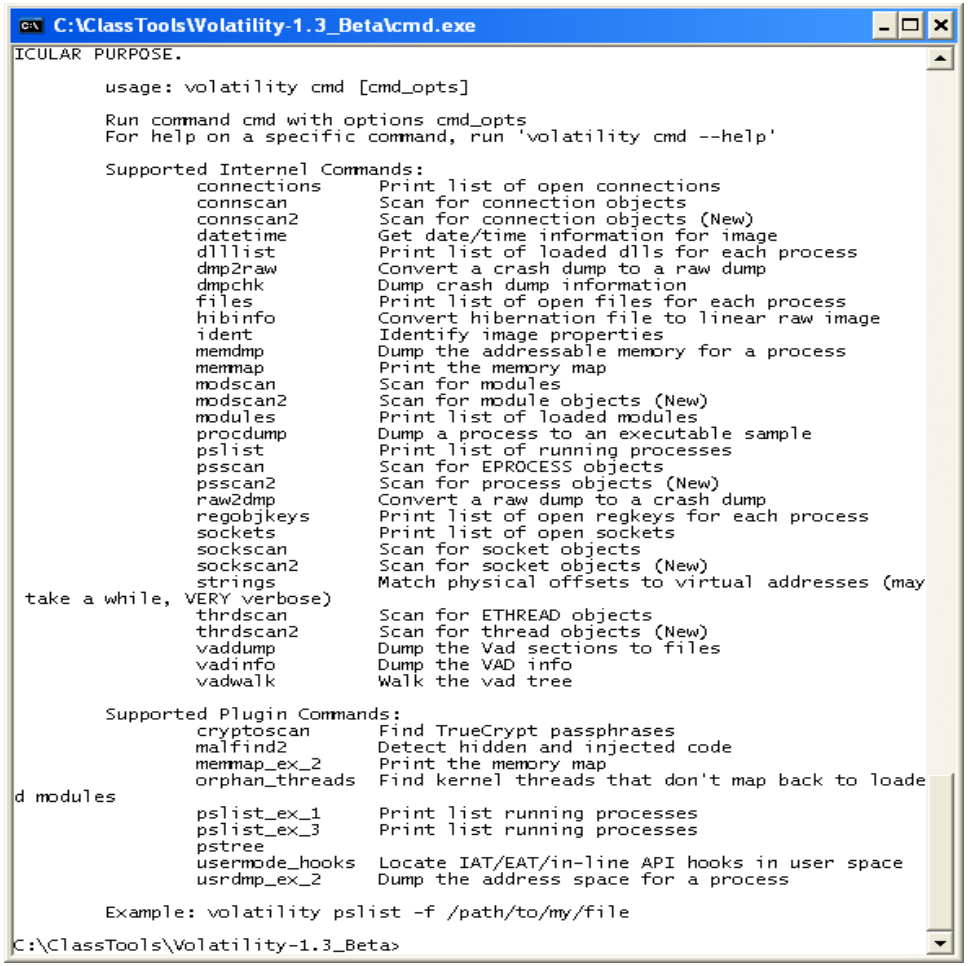
Crash Dumps, Hibernation, and Conversion	Miscellaneous
crashinfo	strings
hibdump	volshell
hibinfo	bioskbd
imagecopy	inspectcache
	patcher
	testsuite

Source:

http://www.forensicswiki.org/wiki/List_of_Volatility_Plugins

http://code.google.com/p/volatility/wiki/CommandReference

Volatility Usage



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)

Working with Images (Cont.)

- 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.

Working with Images (Cont.)

Fortinet	4.1.143.0	2010.07.29	W32/MyDoom.fam@mm
GData	21	2010.07.29	Win32.Worm.McMaggot.A
Ikarus	T3.1.1.84.0	2010.07.29	Trojan.Win32.Genome
Jiangmin	13.0.900	2010.07.29	-
Kaspersky	7.0.0.125	2010.07.29	Trojan.Win32.Genome.btyt
McAfee	5.400.0.1158	2010.07.29	Generic.dx
McAfee-GW-Edition	2010.1	2010.07.29	Heuristic.BehavesLike.Win32.Suspicious.H
Microsoft	1.6004	2010.07.29	Worm:Win32/Prolaco
NOD32	5322	2010.07.29	Win32/Mydoom.NAI
Norman	6.05.11	2010.07.29	W32/Mydoom.ER
nProtect	2010-07-29.01	2010.07.29	Win32.Worm.McMaggot.A
Panda	10.0.2.7	2010.07.28	W32/Mydoom.HY.worm
PCTools	7.0.3.5	2010.07.29	Spyware.007Spy
Prevx	3.0	2010.07.29	-
Rising	22.58.03.04	2010.07.29	-
Sophos	4.55.0	2010.07.29	Mal/Generic-A
Sunbelt	6658	2010.07.29	Trojan.Win32.Generic!BT
SUPERAntiSpyware	4.40.0.1006	2010.07.29	-
Symantec	20101.1.1.7	2010.07.29	Spyware.007Spy

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