Incident Response with Memory Forensics

Steven Manning
Lead Security Analyst
Texas A&M IT Security
Workshop Overview (1/2)

• Introduction/Goals
• What is memory forensics?
• Why and when to use
• Enhancing incident response with memory forensics
• Windows Fundamentals
• Memory Fundamentals
• Break
Workshop Overview (2/2)

• Windows memory acquisition
  • Redline/Memoryze Demo
  • Comae Dumpit.exe Demo
• Windows memory analysis
  • Redline demos
  • Volatility demos
• Memory analysis for enterprise
• Questions/Discussion
Introduction

• Graduated from Texas A&M in 2015
• A+, N+, GIAC Certified Incident Handler (GCIH)
• Applications Development for Texas A&M IT for 5 years
• Lead Security Analyst for Texas A&M IT Security
Today's Goals

• By the end of the morning:
  • Be able to reliably capture a raw memory image from a modern Windows machine
  • Be able to utilize Mandiant Redline and Volatility to identify certain types of malicious behavior in a raw memory image of a Windows system.
Memory Forensics: What is it?

• The collection and analysis of the volatile memory of a system
• Useful in investigating advanced computer attacks which utilize varieties of techniques to avoid detection by traditional methods
Memory Forensics: What is it?

- CPU Registers
- CPU Cache
- Physical Memory
- Solid State Drives
- Mechanical Hard Drives

Speed/Cost:

Volatile:
Memory Forensics: What is it?

• Acquisition
  • Capturing the memory image
• Contextualization
• Analyzation
  • Analyze capture for events
  • Collect evidence
Why Use Memory Forensics?

• Discern recent activity
• Reliable way to get accurate system information
  • Open Sockets
  • Open Files
  • Processes
  • Threads
• Detect Malware
Why Use Memory Forensics?

• Modern malware is good at evading endpoint detection
  • Polymorphic/Metamorphic Malware
  • Encoding
  • Obfuscation
  • Packing
• Rootkits
• Memory Only Malware
Enhancing Incident Response

• Stages of Incident Response
  • Preparation
  • Identification
  • Containment
  • Eradication
  • Recovery
  • Lessons Learned
Windows Fundamentals
Machine Fundamentals

The Art of Memory Forensics - Figure 1-1
Memory Fundamentals

• Address Space
  • Linear/Virtual vs Physical
• Segmentation
• Paging
• Address Translation
Memory Fundamentals

![Diagram of Memory Fundamentals](image)

- **Control Register**
- **Page Directory Pointer Index**
  - PDPE
  - Page Directory Pointer Entries
- **Page Directory**
  - PDE
  - 512 Page Directory Entries
- **Page Table**
  - PTE
  - 512 Page Table Entries
- **Byte Index** (12 bits)
- **Virtual Address**
  - PDPI (2 bits)
  - Page Directory Index (9 bits)
  - Page Table Index (9 bits)
- **4 KB Page**
  - Desired Byte
Memory Acquisition: Overview

• User mode component
• Kernel mode component
  • Driver provides interface to kernel APIs which are able to read raw memory
  • \Device\PhysicalMemory
Memory Acquisition: Evasion

• Block Acquisition
  • Kill the memory acquisition tool
  • Block driver installation

• Block Analysis
  • Modify artifacts to trigger abort factors in analysis software

• Rootkit
  • Custom page fault handler
  • Faking read and writes
Memory Acquisition: Image Formats

• AFF
  • Extensible
  • Open Format
  • Forensic Metadata

• AFF4
  • Expanded on AFF
  • Provides multiple data views
  • Selective imaging
  • Logical file volumes
  • Hash-based imaging
Memory Acquisition: Image Formats

• RAW
  • Bit-for-bit copy of RAW data
    • Disk or Memory
  • Originally used by DD
  • Very common and widely used/accepted
    • (.dd, .dmg, .img)
Windows Memory Acquisition: Live Capture

• FireEye Redline
  • Formally Mandiant Redline
  • Acts as an interface for Memoryze output
• Collection and Investigation
• Easy to use
• Windows/Mac
• Windows 2000 SP4 to Windows 8 Service Pack 0
Windows Memory Acquisition: Live Capture

- Comae dumpit.exe
  - Formally provided by Moonsols
  - Captures RAW memory image of target machine.
  - Normally used with removable storage.
  - Extremely easy to use
  - XP to Windows 10
Windows Memory Acquisition: Live Capture

• Other Tools
  • HBGary
  • FTK Imager
  • WinPmem
  • Win32dd, Win64dd
Windows Memory Acquisition: hyberfil.sys

- `%SystemDrive%/hiberfile.sys`
  - Contains compressed RAM image
- Comae Hibr2bin.exe
  - Extract RAW memory
Windows Memory Acquisition: Virtual Machines

- VMware
  - Can be extracted from .VMSN or .VMSS files
    - RAW format
    - VMWare’s vmss2core utility
  - .VMEM == RAW

- Microsoft Hyber-V
  - .bin == RAW

- Virtualbox
  - .sav file only contains active memory pages
Break

• Snacks!
Memory Acquisition Demo

- FireEye Redline
Memory Acquisition Demo

- Comae Dumpit.exe
Malware Techniques: DLL Injection

- Normal DLL Interaction with Kernel Space
Malware Techniques: DLL Injection

- DLL injected with malicious code
Malware Techniques: DLL Injection

• Common
• OpenProcess() -> VirtualAllocEx() -> WriteProcessMemory() -> Execute
• Process Hollowing
  • Start process
  • Replace process internals with malicious code
Malware Techniques: DLL Injection

• Detection
  • Review pages which are marked as Page_Execute_Readwrite with no memory-mapped file
  • If process image does not have associated file on disk. Process is likely hollowed
Malware Techniques: DLL Injection

• Demo: Detecting Zeus/Zbot DLL Injection using Redline
Malware Techniques: DLL Injection

- Demo: Detecting Zeus/Zbot DLL Injection Volatility
Malware Techniques: Process Hiding
Malware Techniques: Process Hiding

Notepad.exe
Flink
Blink

svchost.exe
Flink
Blink

Evil.exe
Flink
Blink
Malware Techniques: Process Hiding

• Demo: Detecting Eprocess structure manipulation using Volatility
Malware Analysis for Enterprise

- Redline and Volatility are both very extensible
- Volatility supports Linux, Windows, and Mac OSx images
- Can be reactive or proactive
Malware Analysis for Enterprise

- Google’s Rekall forensic memory analysis framework
- Agents can be deployed across and environment and memory captures can be retrieved over a network.
Discussion/Questions