PS C:\> Start-Process PowerShell | Get-ForensicArtifact
@jaredcatkinson

• Jared Atkinson
  • Defensive Services Technical Lead for Adaptive Threat Division
    • Leads the service line responsible for proactive detection and response to advanced threats in Fortune 100 commercial environments
  • Former
  • 2015 Black Hat Minesweeper Champion
  • Moderator of the PowerShell.com “Security Forum”
  • Open Source Developer
    • PowerForensics
    • Uroot IDS
    • WMIEventing
  • Researcher of forensic artifact file formats
PowerForensics

• PowerShell Module for Live Forensic Investigation
• Binary Module (Compiled C# DLL)
• Minimizes Use of Windows APIs
• Currently Parses:
  • NTFS Data Structures
  • Windows Specific Data Structures
    • Windows Registry
    • Windows Event Log
    • Scheduled Jobs
    • Prefetch Files
Design Requirements

• **Forensically sound**
  • Parse raw disk structures
  • Don’t alter NTFS timestamps
• Can execute on a live (running) host
• Operationally fast
  • Collect forensic data in seconds or minutes
• Modular capabilities
  • Cmdlets perform discrete tasks and can be tied together for more complicated tasks
• Capable of working remotely
  • At the proof of concept stage
Reading a Disk/Volume’s Contents

• CreateFile API
  • Used to create a read handle to Physical Disk or Logical Volume

• FileStream Read Method
  • Used to read from the handle
NTFS

Volume Boot Record

File Header

- Jump Instruction: jmp 0x000000054
- OEM ID: NTFS

Fields

- Bytes per sector
- OEM ID
- Number of heads
- MFT first cluster
- MFT mirr first cluster
- Clusters per MFT record
- Clusters per index block
- Volume serial
- Checksum

Values

- 0x200
- 0x08
- 0x00
- 0xF6
- 0x3F
- 0xFF
- 0x8000
- 0x6368FF
- 0xC0000
- 0x02
- 0xF6
- 0x01
- E313CD4233CD4CA
- 0x00000000

Boot Record Block

- Error Message: A disk read error occurred. BOOYMGR is compressed. Press Ctrl+Alt+Del to restart
- Marker: 0x55AA
Hello World
Demo: Web Server Investigation

This demo is based on the @security4arabs Digital Forensics challenge by @binaryz0ne. To download a copy of the challenge please visit http://goo.gl/CVoEpo.
Situation

• Client does not provide much information:
  • Believes their Web Server has been compromised
  • Provides a forensic image to investigate

• Investigator must:
  • Find a temporal starting point
  • Determine if the web server has in fact been compromised
  • If compromised, provide leads for Incident Responders
Demo Video

https://youtu.be/Vh_UFnCgVkw
Initial Findings

• Time: 9/3/2015 6:49:23 AM
• Some sort of brute forcing (sqlmap?)
• Possible Attacker IP Address
  • 192.168.56.102
• Webshell Created
  • webshells.zip
  • c99.php
  • webshell.php
  • phpshell2.php
This demo is based on Ryan Benson’s (@_RyanBenson) blog post (http://www.obsidianforensics.com/blog/finding-the-first-thread-with-visualization) where he describes leveraging Gource (http://gource.io/) to visualize a forensic timeline.
Timeline Visualization Demo

https://youtu.be/v5mYegFG1DA
The Future of PowerForensics

• Multiple File System Support
  • Extended File System (Ext2/3/4)
  • Hierarchical File System (HFS/HFS+)
  • File Allocation Table (FAT12/16/32)

• Additional Artifacts
  • SQLite
  • ESE Database

• WinPE + PowerForensics

• Remote Capabilities
  • PowerForensics Portable

• Community Involvement!