Fileless Malware
09/10/2020
Agenda

• Executive Summary
• What is Fileless Malware
• What makes it different than other malware
• Tools, Techniques, and Procedures
• Case Studies
• Defending Against Fileless Malware
• Summary

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Executive Summary

• Fileless malware: Anatomy and Differences
  • “a type of malicious software that uses legitimate programs to infect a computer. It does not rely on files and leaves no footprint, making it challenging to detect and remove” (McAfee, 2020)

• Operates mainly in memory
  • Entry point for other malware

• Heavy use of
  • Social Engineering
  • PowerShell

Photo credit Christiaan Colen
Anatomy of a Malware attack

- Cybercriminal sends a phishing email to potential victims.
- Victims download a compressed file by clicking a link embedded in the email.
- Victims execute the .CPL file.
- Cybercriminal captures victims' account information.
- .CPL file infects victims' computer with a CPL malware or drops a new malware variant.
- Malware monitors victim access to bank sites, redirects victims to malicious sites, or hijacks victims' banking sessions.
Why is Fileless Malware Different?

- User clicks on link in spam email
- Website loads flash and triggers exploit
- Shellcode launches Powershell (PS) with cmd line to download and execute payload in memory only
- Download and in-memory execution and reflectively load code. Payload can perform exfiltration, damage, etc.
- Auto-start registry created to invoke PS with cmd line
Types of Fileless Malware

- **Type I**: No file activity performed.
- **Type II**: No files written on disk, but some files used indirectly.
- **Type III**: Files required to achieve fileless persistence.

Taxonomy of fileless threats:

- Documents
- Exe
- Java
- Flash
- LNK, Scheduled Task, Executable
- Service
- Registry, WMI Repo
- Shell
- MBR VBR
- BIOS UEFI
- PCI
- Network card, Hard disk
- Circuitry backdoors, IME
- BadUSB
- Motherboard firmware
- Hypervisor

Microsoft 2020
Living off the Land

- Using trusted off-the-shelf equipment
- Blends in with daily work of a system administrator
- Using preinstalled systems tools
- No need to create or deploy own binary files on disk
Living Off the Land Attack Chain

Typical living off the land attack chain

1. **INCURSION**
   - This could be achieved by exploiting a remote code execution (RCE) vulnerability to run shell code directly in memory. More commonly it is an email with a malicious script inside a document or hidden in another host file such as a LNK file. The threat may implement multiple stages with downloader or self-decrypting parts, each of which might follow living off the land techniques again. Another method is misusing system tools by simply logging in with a stolen or guessed password.

2. **PERSISTENCE**
   - Once the computer is compromised, stage two may or may not be fileless in regards to the persistence method. The threat may also not to be persistent at all, depending on what the end goal is for the attacker.

3. **PAYLOAD**
   - The payload of the threat often makes use of dual-use tools.

<table>
<thead>
<tr>
<th>Exploit in memory</th>
<th>Dual-use tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g. SMB EternalBlue</td>
<td>e.g. netsh PsExec.exe</td>
</tr>
<tr>
<td>Email with Non-PE file</td>
<td>Memory only payload</td>
</tr>
<tr>
<td>e.g. Document macro</td>
<td>e.g. Mirai DDoS</td>
</tr>
<tr>
<td>Remote script dropper e.g. LNK with Powershell from cloud storage</td>
<td>Non-PE file payload</td>
</tr>
<tr>
<td></td>
<td>e.g. PowerShell script</td>
</tr>
<tr>
<td>Weak or stolen credentials</td>
<td>Regular non-fileless payload</td>
</tr>
<tr>
<td>e.g. RDP password guess</td>
<td></td>
</tr>
</tbody>
</table>

Non-persistent
- Memory only malware
  - e.g. SQL slammer

Persistent
- Fileless persistence Loadpoint
  - e.g. JScript in registry

Regular non-fileless method

Wueest 2017
# Fileless Attack Methods

## Memory only threats
- These infections are not persistent. Restart will disinfect system
- Shellcode loads payload into memory without writing it to disk

## Fileless persistence
- Windows Registry – Most popular fileless load point method is storing a script in the Windows registry
- Windows Management Instrumentation – Can stop process and execute scripts
- Group Policy Objects – Can be used to add a backdoor
- Scheduled Tasks – May be used to bypass User Account Controls

## Dual-use tools
- Clean applications can be dual purposed by attacker
- Most system tools can be used in an unintended way

## Non-Portable Executable (non-PE) file attacks
- Office documents with macros and scripts
- Involves a script and a legitimate tool
- Host system tool is a powerful scripting framework (PowerShell, WScript, CScript)
PowerShell

• Powerful interactive command-line interface and scripting environment in the Windows OS used to automate tasks
• May be used to download and run executables from the internet which can be executed in memory without touching disk
• PowerShell commands/scripts can be executed without directly invoking powershell.exe

Why Use PowerShell for Fileless Malware Attacks

• PowerShell is installed by default on Windows
• Sysadmins frequently use and trust PowerShell.
• PowerShell scripts are easy to obfuscate and can be difficult to detect in legacy security tools
• Has remote access capabilities by default, so can be used remotely by attackers
Fileless Attack Vectors

Generic Flow Diagram of Fileless Malware Infection

1. Spam Campaign
2. Dropper
3. Malicious Websites
4. Run Registry with JavaScript
5. Thumb Cache Registry Entry

Create:
- Powershell

Execute:
- Executes the Encrypted Script
- Malicious Payload
- Malicious Code Executes Within the Legitimate Process Memory

McAfee 2017
Windows Management Instrumentation (WMI)

- Provides management of all Windows devices on a network
- Can be used to configure security settings like system properties, scheduling processes, user groups, or disabling error logs

Why Use WMI in a Fileless Malware Attack

- Installed by default on Windows OS
- WMI is frequently used and trusted by sysadmins
- WMI is given more credibility because every permanent WMI event subscription runs as SYSTEM
- Almost every OS action can trigger a WMI event, making it incredibly easy to use in combination with operating system actions
Fileless Attack Vectors

Metasploit Meterpreter

- Metasploit is a penetration testing framework used by attackers to connect to PowerShell on the victim's side
- Meterpreter is an attack payload within Metasploit

Why use Metasploit Meterpreter in a Malware Attack

- Meterpreter resides entirely in memory and writes nothing to disk
- No new process are created when Meterpreter injects itself into the compromised process and can migrate to other processes easily
- Uses encrypted communications by establishing a TLS/1.0 link
- Provides limited forensic evidence and impact on the victim machine
Fileless Attack Vectors

.NET Framework
- Framework to develop applications

Visual Basic for Applications
- VBA scripts are macros embedded in Word/Excel to automate tasks

WinDivert
- Network packet capture and manipulation utility

Node JS
- JavaScript Framework to execute JavaScript code
## Case Studies

<table>
<thead>
<tr>
<th>Threat using Fileless Methods</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Netwalker**  
MITRE, 2020                                  | • Ransomware attack that uses fileless methods to gain access to systems  
• Exploited VPN vulnerabilities  
• Taken advantage of the COVID-19 pandemic  
• Collected over $25 million since March 2020 |
| **Nodorsok/Divergent**                         | • Named Nodorsok by Microsoft and Divergent by Cisco Talos  
• Malware that employs advanced fileless techniques  
• Turns PCs into Proxies  
• Used for adware/click fraud  
• Reported last fall to have turned thousands of PCs into Zombie Proxies with malicious intent. |
| **Not Petya**  
MITRE (2), 2020, McAfee (2), 2017             | • Not Petya emerged in June 2017  
• Has infected organizations in several sectors, including finance, transportation, energy, commercial facilities, and healthcare causing $10 billion in damages worldwide  
• Infects computers Master Boot Records  
• Encrypts files without any way to decrypt wiping files from the infected machines |
Case Studies: Netwalker TTPs

1. Detect if running X64 or X86
2. Use Windows API functions or psexec.exe to deploy ransomware
3. Embed ransomware DLL
4. Delete shadow volumes to prevent recovery
5. Reflectively inject the DLL into explorer.exe
Case Studies: Nordosok/Divergent TTPs

User loads an HTA download → HTA Embedded Javascript downloads a 2nd component → 2nd stage launches PowerShell

PowerShell script downloads and runs additional encrypted payload → Payload contains a Node JS module, converting host into a proxy
Case Studies: Not Petya TTPs

Access gained via ExternalBlue Exploit → Credentials stolen using Mimikatz → Stolen credentials
+ WMIC or psexec.exe = Access to nearby systems

MBR files encrypted
Ransom demand issued → System wiped
Defending Against Fileless Malware

- Practice strong cyber hygiene and defense in depth
- Train users to identify and guard against Social Engineering
- Instituting Least Privilege and Zero Trust Privilege
- Secure PowerShell use by taking advantage of its logging capability to monitor suspicious behavior.
- Use PowerShell commands such as Constrained Language Mode to secure systems from malicious code.
- Properly configure system components, apply updates and disable unused and outdated systems to block possible entry points.
- Never download and execute files from unfamiliar sources
- Use network detection and responses security solutions that utilize behavior monitoring
Defending Against Fileless Malware

**Signature Based Detection**

*Advantages*
- Immediate use
- Needs less monitoring
- Fast and effective for known malware

*Disadvantages*
- Uses malware file characteristics (e.g.)
  - Byte size
  - Hashes
- Unable to detect zero-day attacks or attacks that obfuscate signatures

**Behavioral Based Detection**

*Advantages*
- Can detect changes in activity does not need files
- Can take advantage of machine learning

*Disadvantages*
- High false positive rate
- Time needed to establish baseline
- Excessive monitoring
Summary

- Fileless Malware: Anatomy and Differences
- Attack Vectors: Social Engineering, PowerShell, Zero Day Vulnerabilities
- Mitigations include:
  - Improving cyber hygiene
  - Information security training for all important stakeholders
  - Updating systems (patching & securing configurations)
  - Disabling unused potential entry points
Reference Materials


References


- Microsoft. (n.d.). Licenses. Retrieved from Creative Commons: https://creativecommons.org/licenses/by-nc/3.0/
References


Questions

Upcoming Briefs

• 9/17 – Malsapam
• 9/24 – Netwalker Ransomware
• 10/15 - Side Channel Attacks
• 10/22 – Disinformation in the Healthcare Sector

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.
HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Visit us at: www.HHS.Gov/HC3
Contact

www.HHS.GOV/HC3  (202) 691-2110  HC3@HHS.GOV