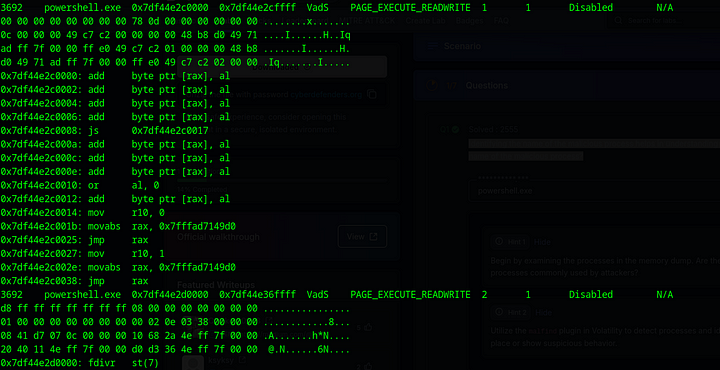
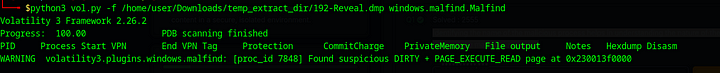
### **Reveal — CyberDefenders**

**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.

#### **Tasks**

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

python3 vol.py -f /path/to/192-reveal.dmp windows.malfind.Malfind

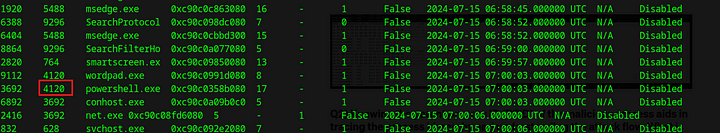
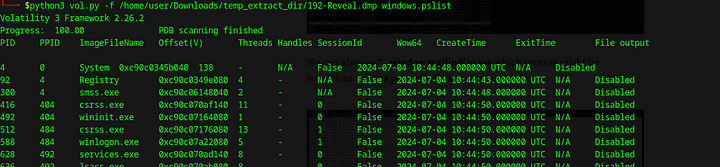


Although there were other processes identified by this, powershell.exe is particularly suspicious as it had **memory being executed and written to** within Pits process (with PAGE\_EXECUTE\_READWRITE ), especially at multiple addresses, signals that **something potentially malicious** is running in PowerShell's memory space.

Answer: PowerShell.exe

**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?**

python3 vol.py -f /path/to/192-reveal.dmp windows.pslist



**Answer:** 4120

**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?**

python3 vol.py -f /path/to/192-reveal.dmp windows.cmdline | grep 3692

The above command will output the command line arguments for the process with PID 3692. We can see the PID of the suspicious process in the above screenshot.



**Answer:** 3435.dll

**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?**

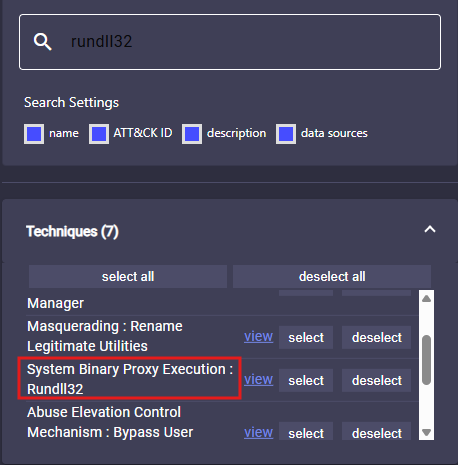
This can be found in the above screenshot.



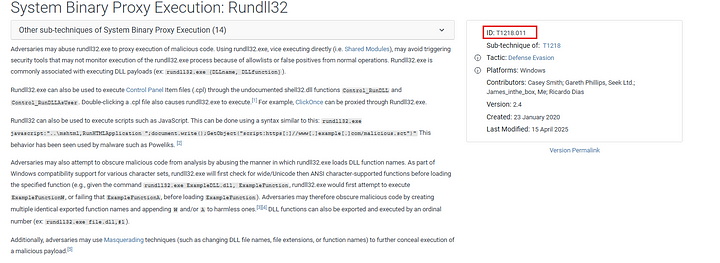
**Answer:** davwwwroot

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

We can use the ATT&CK [Navigator](https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0008%2FG0008-enterprise-layer.json) to check for any techniques that use rundll32.



We can see above, a matching technique to the process used by the attacker. Let us view this Technique.



**Answer:** T1218.011

**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?**

python3 vol.py -f /home/user/Downloads/temp\_extract\_dir/192-Reveal.dmp windows.getsids | grep powershell.exe

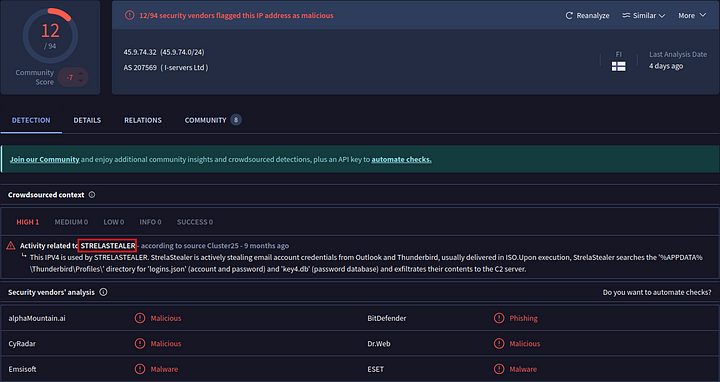
The above command retrieves **Security Identifiers (SIDs)** associated with powershell.exe, and the corresponding **usernames** or groups that are mapped to those SIDs



**Answer:** Elon

**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?**

In the question3 we found an IP address related to the C2 server. Let us check this IP address using VirusTotal.



**Answer:** STRELASTEALER

This is the end of this walkthrough.