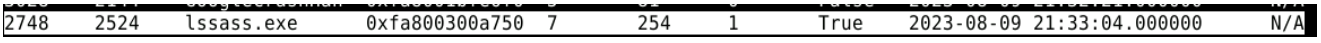
Amadey_allunell---CyberDefenders

Q1: In the memory dump analysis, determining the root of the malicious activity is essential for comprehending the extent of the intrusion. What is the name of the parent process that triggered this malicious behavior?

```
lssass.exe
```

Resolution:

```
./vol.py -f /home/ubuntu/Desktop/'Start here'/Artifacts/'Windows 7 x64-Snapshot4.vmem' windows.pstree
```



2748	2524	lssass.exe	0xfa800300a750	7	254	1	True	2023-08-09 21:33:04.000000	N/A

Q2: Once the rogue process is identified, its exact location on the device can reveal more about its nature and source. Where is this process housed on the workstation?

```
C:\Users\0XSH3R~1\AppData\Local\Temp\925e7e99c5\lssass.exe
```

Resolution:

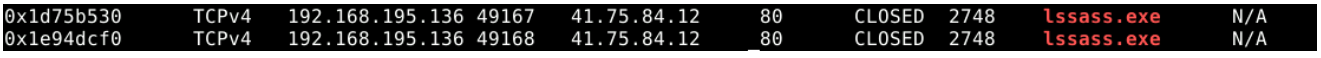
```
./vol.py -f /home/ubuntu/Desktop/'Start here'/Artifacts/'Windows 7 x64-Snapshot4.vmem' cmdline | grep lssass.exe
```

Q3: Persistent external communications suggest the malware's attempts to reach out C2C server. Can you identify the Command and Control (C2C) server IP that the process interacts with?

```
41.75.84.12
```

Resolution:

```
./vol.py -f /home/ubuntu/Desktop/'Start here'/Artifacts/'Windows 7 x64-Snapshot4.vmem' netscan | grep lssass.exe
```



Q4: Following the malware link with the C2C, the malware is likely fetching additional tools or modules. How many distinct files is it trying to bring onto the compromised workstation?

```
2
```

Resolution:

```
./vol.py -f /home/ubuntu/Desktop/'Start here'/Artifacts/'Windows 7 x64-Snapshot4.vmem' windows.memmap.Memmap --pid 2748 --dump
```

```
strings pid.2748.dmp | grep 'GET /'
```

```
GET /rock/Plugins/cred64.dll HTTP/1.1
GET /rock/Plugins/clip64.dll HTTP/1.1
```

Q5: Identifying the storage points of these additional components is critical for containment and cleanup. What is the full path of the file downloaded and used by the malware in its malicious activity?

```
C:\Users\0xSh3rl0ck\AppData\Roaming\116711e5a2ab05\clip64.dll
```

Resolution:

```
./vol.py -f /home/ubuntu/Desktop/'Start here'/Artifacts/'Windows 7 x64-Snapshot4.vmem' cmdline | grep dll
```

```
868gressdllhost.exe     C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
3064    rundll32.exe    "C:\Windows\System32\rundll32.exe" C:\Users\0xSh3rl0ck\AppData\Roaming\116711e5a2ab05\clip64.dll, Main
```

Q6: Once retrieved, the malware aims to activate its additional components. Which child process is initiated by the malware to execute these files?

```
rundll32.exe
```

Resolution:

```
./vol.py -f /home/ubuntu/Desktop/'Start here'/Artifacts/'Windows 7 x64-Snapshot4.vmem' windows.pstree
```

Q7:Understanding the full range of Amadey's persistence mechanisms can help in an effective mitigation. Apart from the locations already spotlighted, where else might the malware be ensuring its consistent presence?

```
C:\Windows\System32\Tasks\lssass.exe
```

Resolution:

```
./vol.py -f /home/ubuntu/Desktop/'Start here'/Artifacts/'Windows 7 x64-Snapshot4.vmem' filescan | grep lssass.ex
```