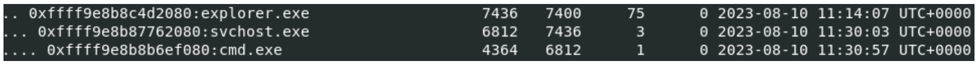
RogueOne Challenge

Sherlock Scenario

Your SIEM system generated multiple alerts in less than a minute, indicating potential C2 communication from Simon Stark's workstation. Despite Simon not noticing anything unusual, the IT team had him share screenshots of his task manager to check for any unusual processes. No suspicious processes were found, yet alerts about C2 communications persisted. The SOC manager then directed the immediate containment of the workstation and a memory dump for analysis. As a memory forensics expert, you are tasked with assisting the SOC team at Forela to investigate and resolve this urgent incident.

Task 1
Please identify the malicious process and confirm process id of malicious process.

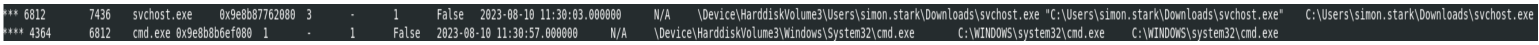
python2 vol.py -f '/home/remnux/20230810.mem' --profile=Win10x64_19041 pstree



```
.. 0xffff9e8b8c4d2080:explorer.exe                    7436   7400     75      0 2023-08-10 11:14:07 UTC+0000
... 0xffff9e8b87762080:svchost.exe                    6812   7436      3      0 2023-08-10 11:30:03 UTC+0000
.... 0xffff9e8b8b6ef080:cmd.exe                       4364   6812      1      0 2023-08-10 11:30:57 UTC+0000
```

We can see the that the svchost.exe has a different PID from the others svchost.exe

If we use volatility 3, we can also see that the svchost.exe is coming from the path C:\Users\simon.stark\Downloads\svchost.exe

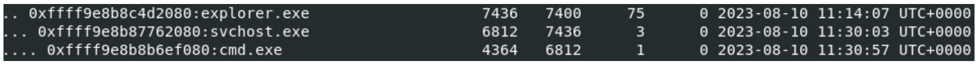


```
*** 6812       7436    svchost.exe     0x9e8b87762080  3       -       1       False   2023-08-10 11:30:03.000000      N/A     \Device\HarddiskVolume3\Users\simon.stark\Downloads\svchost.exe "C:\Users\simon.stark\Downloads\svchost.exe"    C:\Users\simon.stark\Downloads\svchost.exe
**** 4364      6812    cmd.exe 0x9e8b8b6ef080  1       -       1       False   2023-08-10 11:30:57.000000      N/A     \Device\HarddiskVolume3\Windows\System32\cmd.exe        C:\WINDOWS\system32\cmd.exe     C:\WINDOWS\system32\cmd.exe
```

Answer: 6812

Task 2
The SOC team believe the malicious process may spawned another process which enabled threat actor to execute commands. What is the process ID of that child process?

We can see the svchost is spawning cmd.exe



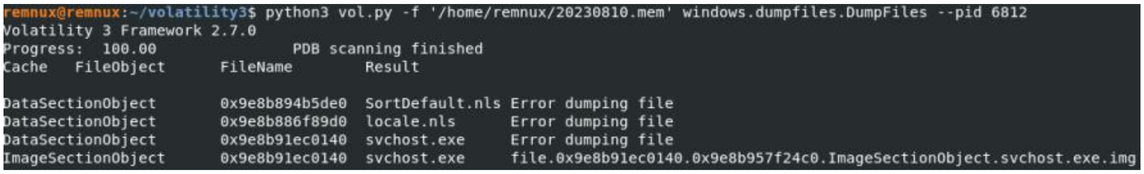
```
.. 0xffff9e8b8c4d2080:explorer.exe                    7436   7400     75      0 2023-08-10 11:14:07 UTC+0000
... 0xffff9e8b87762080:svchost.exe                    6812   7436      3      0 2023-08-10 11:30:03 UTC+0000
.... 0xffff9e8b8b6ef080:cmd.exe                       4364   6812      1      0 2023-08-10 11:30:57 UTC+0000
```

Answer: 4364

Task 3
The reverse engineering team need the malicious file sample to analyze. Your SOC manager instructed you to find the hash of the file and then forward the sample to reverse engineering team. Whats the md5 hash of the malicious file?

We need to dump the file to check the MD5

python3 vol.py -f '/home/remnux/20230810.mem' windows.dumpfiles.DumpFiles --pid 6812



```
remnux@remnux:~/volatility3$ python3 vol.py -f '/home/remnux/20230810.mem' windows.dumpfiles.DumpFiles --pid 6812
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0x9e8b894b5de0  SortDefault.nls Error dumping file
DataSectionObject       0x9e8b886f89d0  locale.nls      Error dumping file
DataSectionObject       0x9e8b91ec0140  svchost.exe     Error dumping file
ImageSectionObject      0x9e8b91ec0140  svchost.exe     file.0x9e8b91ec0140.0x9e8b957f24c0.ImageSectionObject.svchost.exe.img
```

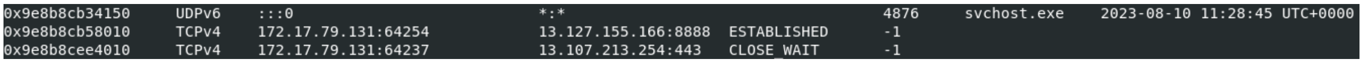
Lets use md5sum to see the hash

md5sum '/home/remnux/volatility3/file.0x9e8b91ec0140.0x9e8b957f24c0.ImageSectionObject.svchost.exe.img'

Answer: 5bd547c6f5bfc4858fe62c8867acfbb5

Task 4:
In order to find the scope of the incident, the SOC manager has deployed a threat hunting team to sweep across the environment for any indicator of compromise. It would be a great help to the team if you are able to confirm the C2 IP address and ports so our team can utilise these in their sweep.

We will use netscan plugin python2 vol.py -f '/home/remnux/20230810.mem' --profile=Win10x64_19041 netscan

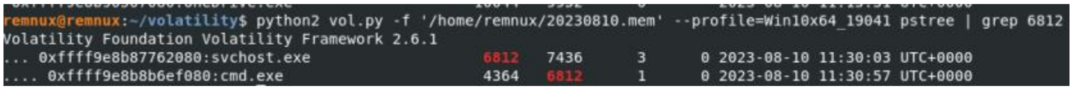


```
0x9e8b8cb34150     UDPv6    :::0                          *:*                                  4876     svchost.exe    2023-08-10 11:28:45 UTC+0000
0x9e8b8cb58010     TCPv4    172.17.79.131:64254           13.127.155.166:8888  ESTABLISHED      -1
0x9e8b8cee4010     TCPv4    172.17.79.131:64237           13.107.213.254:443   CLOSE_WAIT       -1
```

Answer: 13.127.155.166:8888

Task 5:
We need a timeline to help us scope out the incident and help the wider DFIR team to perform root cause analysis. Can you confirm time the process was executed and C2 channel was established?

Lets use pstree again with grep of the PID python2 vol.py -f '/home/remnux/20230810.mem' --profile=Win10x64_19041 pstree | grep 6812

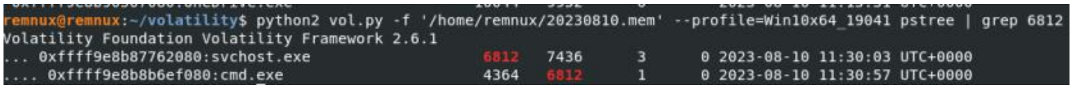


```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/20230810.mem' --profile=Win10x64_19041 pstree | grep 6812
Volatility Foundation Volatility Framework 2.6.1
... 0xffff9e8b87762080:svchost.exe                    6812   7436      3      0 2023-08-10 11:30:03 UTC+0000
.... 0xffff9e8b8b6ef080:cmd.exe                       4364   6812      1      0 2023-08-10 11:30:57 UTC+0000
```

Answer: 10/08/2023 11:30:03

Task 6:
What is the memory offset of the malicious process?

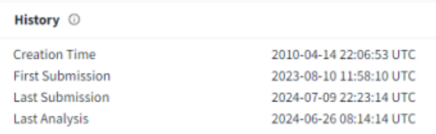
Same as the question above



```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/20230810.mem' --profile=Win10x64_19041 pstree | grep 6812
Volatility Foundation Volatility Framework 2.6.1
... 0xffff9e8b87762080:svchost.exe                  6812   7436      3      0 2023-08-10 11:30:03 UTC+0000
.... 0xffff9e8b8b6ef080:cmd.exe                     4364   6812      1      0 2023-08-10 11:30:57 UTC+0000
```

Answer: 0x9e8b87762080

Task 7:
You successfully analyzed a memory dump and received praise from your manager. The following day, your manager requests an update on the malicious file. You check VirusTotal and find that the file has already been uploaded, likely by the reverse engineering team. Your task is to determine when thesample was first submitted to VirusTotal



History ⓘ

Creation Time	2010-04-14 22:06:53 UTC
First Submission	2023-08-10 11:58:10 UTC
Last Submission	2024-07-09 22:23:14 UTC
Last Analysis	2024-06-26 08:14:14 UTC

Answer: 10/08/2023 11:58:10