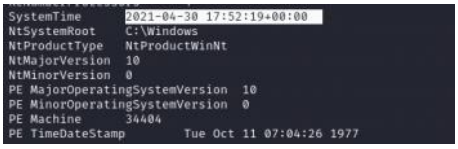
# Brave Lab (Cyber Defenders) - Walkthrough

Sunday, September 15, 2024 8:20 PM

Story:
A memory image was taken from a seized Windows machine. As a security blue team analyst, analyze the image and answer the provided questions.

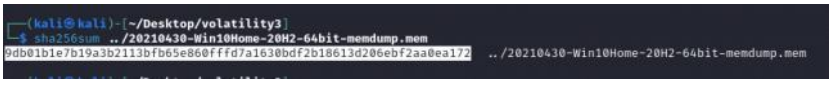
**Q1: What time was the RAM image acquired according to the suspect system? (YYYY-MM-DD HH:MM:SS)**

- I used Volatility3's windows.info.Info plugin to determine that the memory image was captured on 2021-04-30 at 17:52:19.




**Q2: What is the SHA256 hash value of the RAM image?**

- I used 'sha256sum' command to find the sha256 of the image.

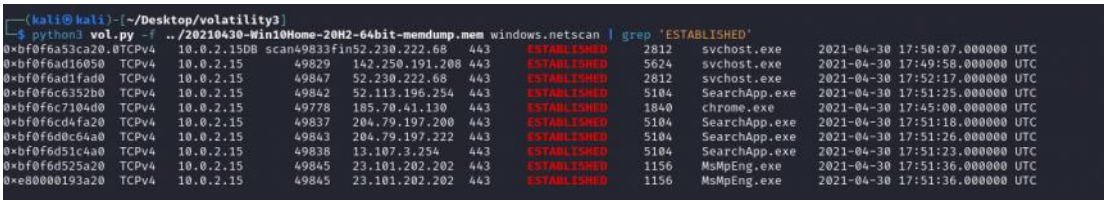



**Q3: What is the process ID of "brave.exe"?**

- I used 'Pstree' plugin to find the PID of 'Brave.exe'


**Q4: How many established network connections were there at the time of acquisition? (number)**

- I used 'netscan' plugin and filtered by 'Grep' utility 'Established'.




**Q5: What FQDN does Chrome have an established network connection with?**

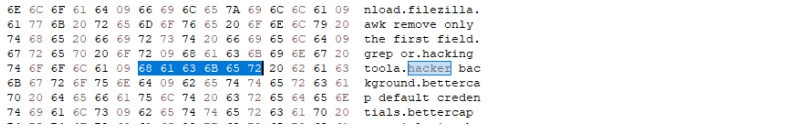
- I used the IP connected via Chrome and looked it up on AbuseIPDB, which led me to the registered domain 'protonmail.ch'.

**Q6: What is the MD5 hash value of process executable for PID 6988?**

- I executed the following command:
  python3 vol.py -f ../20210430-Win10Home-20H2-64bit-memdump.mem windows.pslist --pid=6988 --dump
  to dump the process. After dumping the process, I used the md5sum command to find the MD5 hash.

Q7: **What is the word starting at offset 0x45BE876 with a length of 6 bytes?**

- To address this question, I used 'HxD', I loaded the memory dump to the HxD and used the 'Go To' operation and put the offest (45BE876) and found the 6 bytes word is hacker




**Q8: What is the creation date and time of the parent process of "powershell.exe"? (YYYY-MM-DD HH:MM:SS)**

- You are able to use 'Pstree' plugin to see when the 'Explorer.exe' created (2021-04-30 17:39:48)

**Q9: What is the full path and name of the last file opened in notepad?**

- You are able to see the file path and the filename via 'Pstree' plugin

```
C:\Windows\System32\SecurityHealthSystray.exe
2520    2152    notepad.exe     0xbf0f6d8450c0  1       -       1       False   2021-04-30 17:44:28.000000 UTC  N/A     \Device\Harddis
C:\Users\JOHNDO~1\AppData\Local\Temp\7zO4FB31F24\accountNum C:\Windows\system32\NOTEPAD.EXE
```

**Q10: How long did the suspect use Brave browser? (hh:mm:ss)**

- To address this question, I used 'windows.registry.userassist.UserAssist' plugin to find how much time the user used Brave browser.