Cyber Defenders: Brave

The following writeup is for <u>Brave</u> on CyberDefenders, it involves investigating a memory dump using Volatility3 and HxD.

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

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

To determine when the RAM image was taken, we can use the windows.info.Info plugin like as follows:

python vol.py -f 20210430-Win10Home-20H2-64bit-memdump.mem windows.info.Info

The image was taken at: 2021-04-30 17:52:19

What is the SHA256 hash value of the RAM image?

You can use the Get-FileHash PowerShell cmdlet to generate the SHA256 hash of the image:

Get-FileHash -algorithm SHA256 .\20210430-Win10Home-20H2-64bit-memdump.mem

```
Algorithm Hash
-----
SHA256 9DB01B1E7B19A3B2113BFB65E860FFFD7A1630BDF2B18613D206EBF2AA0EA172
```

What is the process ID of "brave.exe"?

You can use the pslist (or pstree) plugin to determine the process ID of brave.exe:

```
python .\vol.py -f .\20210430-Win10Home-20H2-64bit-memdump.mem windows.pslist
4856 1872 brave.exe
```

The PID is 4856.

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

To identify network connections present at the time of extraction on the host machine, we can use the netscan plugin (you can also use the netstat plugin):

```
python .\vol.py -f .\20210430-Win10Home-20H2-64bit-memdump.mem windows.netscan
```

(a better way to do this would be to filter for only established connections, but I just decided to count them manually). There are 10 established network connections.

What FQDN does Chrome have an established network connection with?

In the output of the netscan plugin, we can see the established connection chrome has with 185.70.41.130:

```
185.70.41.130 443 ESTABLISHED 1840 chrome.exe
```

You can then use a DNS lookup tool or the Resolve-DnsName cmdlet to determine the FQDN:

Resolve-DnsName 185.70.41.130

Name	Туре	TTL	Section	NameHost
130.41.70.185.in-addr.arpa	PTR	1164	Answer	185-70-41-130.protonmail.ch

Therefore, the answer is protonmail.ch.

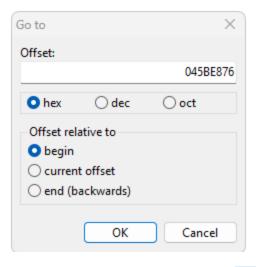
What is the MD5 hash value of process executable for PID 6988?

We can use the windows.pslist.Pslist plugin to dump the executable associated with PID 6988:



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

I opened up the memory dump in HxD, navigated to Search > Go To, entered the offset and voila:



0045BE870 74 6F 6F 6C 61 09 68 61 63 6B 65 72 20 62 61 63 toola. hacker bac

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

We can use the pstree plugin to find the parent process of powershell.exe and see its creation time:



Therefore, the answer is 2021-04-30 17:39:48.

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



C:\Users\JOHNDO~1\AppData\Local\Temp\7zO4FB31F24\accountNum

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

You can see how long the user was using Brave for by looking at the Time Focus column of the Brave application:

Name	ID	Count	Focus Count	Time Focused
RDc	я 🛮 С	RBC	R ■ C	нвс
%ProgramFiles%\\ <mark>Brave</mark> Software\\Temp\\GUM20E0.tmp\\BraveUpdate.exe		0	0	0:00:03.531000
%ProgramFiles%\\BraveSoftware\\Update\\BraveUpdate.exe		0	1	0:00:24.797000
Brave	N/A	9	22	4:01:54.328000
C:\\Users\\Public\\Desktop\\ <mark>Brave</mark> .lnk	N/A	8	0	0:00:00.508000

The answer is 04:01:54.