Digital Forensics – Lab#14

Ahmad Abdullah i22-1609

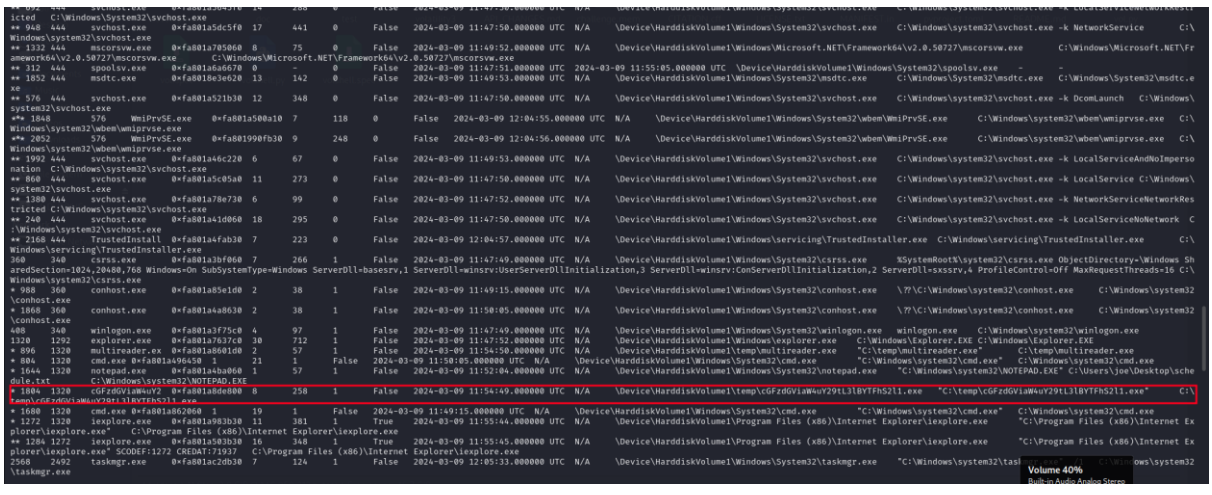
Task Description: You've been tasked with investigating a PC that belongs to a colleague. They've noticed unusual activity and suspect their computer may have been compromised by attackers. While you've confirmed the attackers were inside the system, they're curious about how the attackers managed to maintain access even after the computer was rebooted or security measures were applied.

Working:

There is no Profile usage in Volatility3 so, I directly went to the process list in the dump and found a process with a weird name. I did not think much of its name just knew that this is not a normal Windows process and needed to be analyzed.

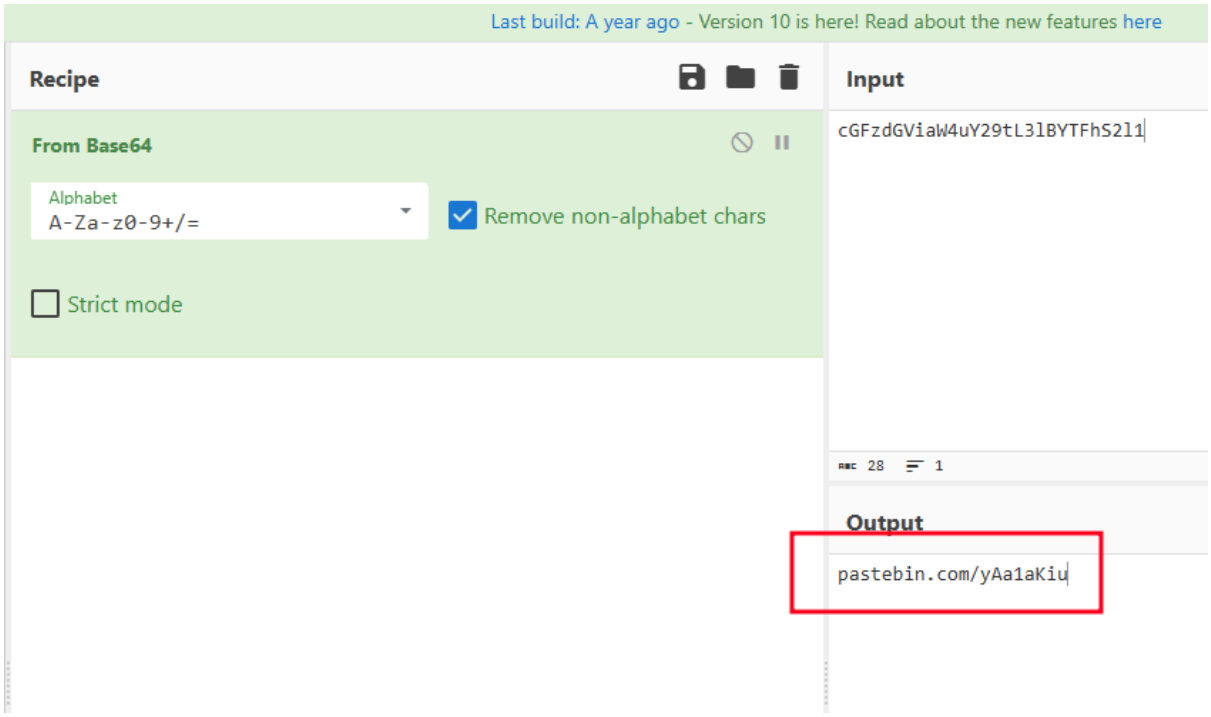
```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f challenge.mem windows.pslist
Volatility 3 Framework 2.11.0
Progress:  100.00       PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×fa8018d8db30  71      497     N/A     False   2024-03-09 11:47:48.000000 UTC  N/A     Disabled
224     4       smss.exe        0×fa8019c06310  2       29      N/A     False   2024-03-09 11:47:48.000000 UTC  N/A     Disabled
296     288     csrss.exe       0×fa801a39a750  9       341     0       False   2024-03-09 11:47:49.000000 UTC  N/A     Disabled
348     288     wininit.exe     0×fa801a3b8b30  4       77      0       False   2024-03-09 11:47:49.000000 UTC  N/A     Disabled
360     340     csrss.exe       0×fa801a3bf060  7       266     1       False   2024-03-09 11:47:49.000000 UTC  N/A     Disabled
408     340     winlogon.exe    0×fa801a3f75c0  4       97      1       False   2024-03-09 11:47:49.000000 UTC  N/A     Disabled
444     348     services.exe    0×fa801a3ff5f0  9       200     0       False   2024-03-09 11:47:49.000000 UTC  N/A     Disabled
460     348     lsass.exe       0×fa801a4083b0  8       569     0       False   2024-03-09 11:47:49.000000 UTC  N/A     Disabled
468     348     lsm.exe 0×fa801a40eb30  11      144     0       False   2024-03-09 11:47:49.000000 UTC  N/A     Disabled
576     444     svchost.exe     0×fa801a521b30  12      348     0       False   2024-03-09 11:47:50.000000 UTC  N/A     Disabled
640     444     svchost.exe     0×fa801a54bb30  9       243     0       False   2024-03-09 11:47:50.000000 UTC  N/A     Disabled
692     444     svchost.exe     0×fa801a5645f0  14      288     0       False   2024-03-09 11:47:50.000000 UTC  N/A     Disabled
812     444     svchost.exe     0×fa801a5a49e0  34      953     0       False   2024-03-09 11:47:50.000000 UTC  N/A     Disabled
860     444     svchost.exe     0×fa801a5c05a0  11      273     0       False   2024-03-09 11:47:50.000000 UTC  N/A     Disabled
908     444     svchost.exe     0×fa801a5ccb30  8       197     0       False   2024-03-09 11:47:50.000000 UTC  N/A     Disabled
948     444     svchost.exe     0×fa801a5dc5f0  17      441     0       False   2024-03-09 11:47:50.000000 UTC  N/A     Disabled
240     444     svchost.exe     0×fa801a41d060  18      295     0       False   2024-03-09 11:47:50.000000 UTC  N/A     Disabled
312     444     spoolsv.exe     0×fa801a6a6670  0       -       0       False   2024-03-09 11:47:51.000000 UTC  2024-03-09 11:55:05.000000 UTC  Disabled
1040    444     svchost.exe     0×fa801a6d0060  4       46      0       False   2024-03-09 11:47:51.000000 UTC  N/A     Disabled
1200    444     taskhost.exe    0×fa801a722b30  6       117     1       False   2024-03-09 11:47:51.000000 UTC  N/A     Disabled
1304    908     dwm.exe 0×fa801a75a060  4       66      1       False   2024-03-09 11:47:51.000000 UTC  N/A     Disabled
1320    1292    explorer.exe    0×fa801a7637c0  30      712     1       False   2024-03-09 11:47:52.000000 UTC  N/A     Disabled
1380    444     svchost.exe     0×fa801a78e730  6       99      0       False   2024-03-09 11:47:52.000000 UTC  N/A     Disabled
1956    444     sppsvc.exe      0×fa801a87f4f0  5       151     0       False   2024-03-09 11:47:59.000000 UTC  N/A     Disabled
1680    1320    cmd.exe 0×fa801a862060  1       19      1       False   2024-03-09 11:49:15.000000 UTC  N/A     Disabled
988     360     conhost.exe     0×fa801a85e1d0  2       38      1       False   2024-03-09 11:49:15.000000 UTC  N/A     Disabled
2040    444     mscorsvw.exe    0×fa801a85db30  8       84      0       True    2024-03-09 11:49:52.000000 UTC  N/A     Disabled
1332    444     mscorsvw.exe    0×fa801a705060  8       75      0       False   2024-03-09 11:49:52.000000 UTC  N/A     Disabled
1992    444     svchost.exe     0×fa801a46c220  6       67      0       False   2024-03-09 11:49:53.000000 UTC  N/A     Disabled
1852    444     msdtc.exe       0×fa8018e3e620  13      142     0       False   2024-03-09 11:49:53.000000 UTC  N/A     Disabled
804     1320    cmd.exe 0×fa801a496450  1       21      1       False   2024-03-09 11:50:05.000000 UTC  N/A     Disabled
1868    360     conhost.exe     0×fa801a4a8630  2       38      1       False   2024-03-09 11:50:05.000000 UTC  N/A     Disabled
1644    1320    notepad.exe     0×fa801a4ba060  1       57      1       False   2024-03-09 11:52:04.000000 UTC  N/A     Disabled
1804    1320    cGFzdGViaW4uY2  0×fa801a8de800  8       258     1       False   2024-03-09 11:54:49.000000 UTC  N/A     Disabled
896     1320    multireader.ex  0×fa801a8601d0  2       57      1       False   2024-03-09 11:54:50.000000 UTC  N/A     Disabled
1272    1320    iexplore.exe    0×fa801a983b30  11      381     1       True    2024-03-09 11:55:44.000000 UTC  N/A     Disabled
1284    1272    iexplore.exe    0×fa801a503b30  16      348     1       True    2024-03-09 11:55:45.000000 UTC  N/A     Disabled
1536    444     spoolsv.exe     0×fa801a93fb30  13      254     0       False   2024-03-09 11:56:05.000000 UTC  N/A     Disabled
1848    576     WmiPrvSE.exe    0×fa801a500a10  7       118     0       False   2024-03-09 12:04:55.000000 UTC  N/A     Disabled
2052    576     WmiPrvSE.exe    0×fa801990fb30  9       248     0       False   2024-03-09 12:04:56.000000 UTC  N/A     Disabled
2168    444     TrustedInstall  0×fa801a4fab30  7       223     0       False   2024-03-09 12:04:57.000000 UTC  N/A     Disabled
2568    2492    taskmgr.exe     0×fa801ac2db30  7       124     1       False   2024-03-09 12:05:33.000000 UTC  N/A     Disabled
```

Next, I used pstree plugin to find the executable's directory and other information that wasn't listed in pslist and found that it was in the temp folder.

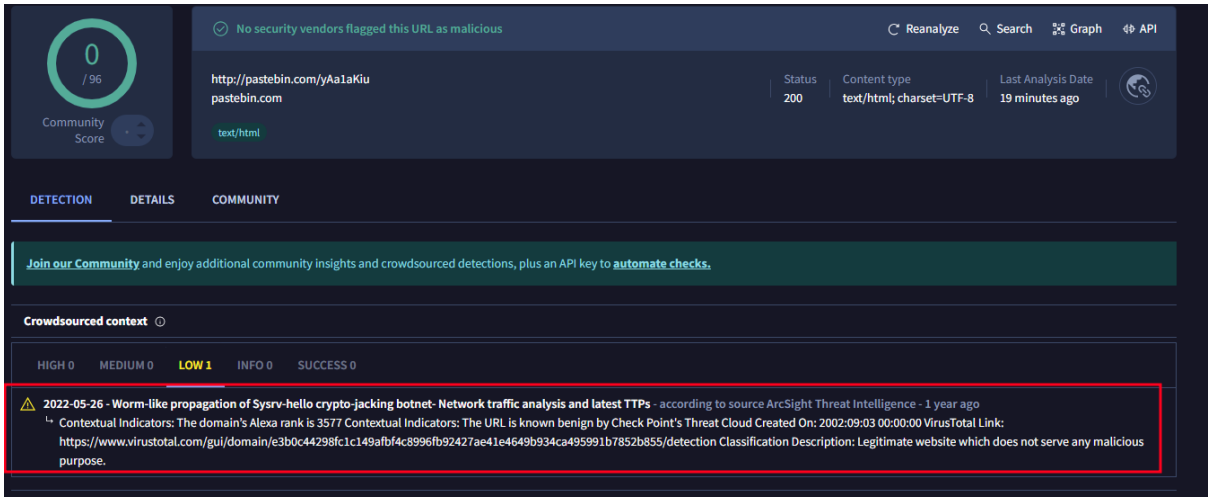


After the pstree , I suddenly noticed that the name of the executable looked encoded **cGFzdGViaW4uY29tL3lBYTFhS2l1.**

So I pasted the name of the file in cyberChef and yes the name was actually a URL. *pastebin.com/yAa1aKiu*

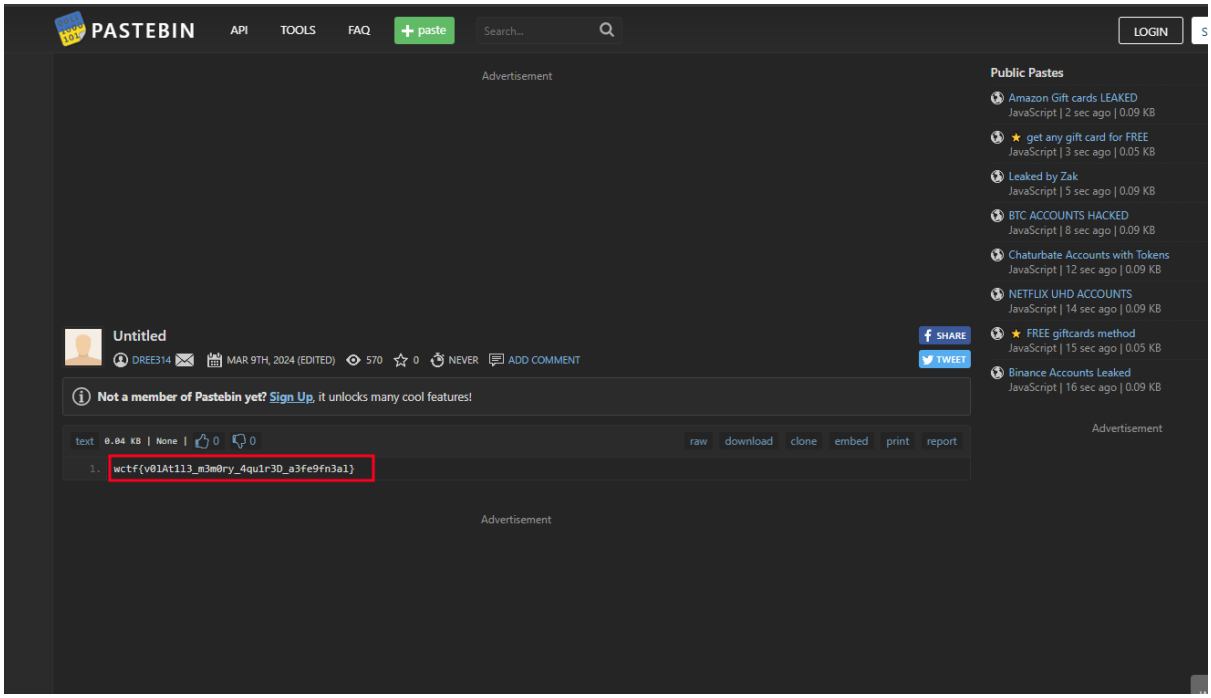


VirusTotal gave no information about this being suspicious, rather it said that many people use the website so it is opposite of suspicious.



I kept looking around about what this website is used for and found out that this website is used to share text based file and information among people over the internet. So, to me it looked like the attacker might be pasted information about the victim here and

reading from the other end.
I visited the url and found a flag wctf{vØlAt113_m3mØry_4qu1r3D_a3fe9fn3a1}
but this did not tell how the attackers kept persistence.



Network scan did not reveal much other than the file tried to connect to the the ip which seemed like printer's ip.

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f challenge.mem windows.netscan
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x7e2719a0      TCPv4   0.0.0.0 49157   0.0.0.0 0       LISTENING       460     lsass.exe       -
0x7e2bb570      TCPv4   0.0.0.0 49157   0.0.0.0 0       LISTENING       460     lsass.exe       -
0x7e2bb570      TCPv6   ::      49157   ::      0       LISTENING       460     lsass.exe       -
0x7e2e2010      TCPv4   -       49175   23.206.214.219  80      CLOSED  1284    iexplore.exe    -
0x7e2f6510      TCPv4   192.168.3.140   49171   192.168.3.133   4444    ESTABLISHED     312     spoolsv.exe     N/A
0x7e303010      TCPv4   -       49174   23.206.214.219  80      CLOSED  1284    iexplore.exe    -
0x7e3408e0      UDPv4   0.0.0.0 5355    *       0               948     svchost.exe     2024-03-09 12:02:51.000000 UTC
0x7e41a870      UDPv4   0.0.0.0 0       *       0               948     svchost.exe     2024-03-09 11:47:50.000000 UTC
0x7e41a870      UDPv6   ::      0       *       0               948     svchost.exe     2024-03-09 11:47:50.000000 UTC
0x7e45f0d0      TCPv4   0.0.0.0 47001   0.0.0.0 0       LISTENING       4       System  -
0x7e45f0d0      TCPv6   ::      47001   ::      0       LISTENING       4       System  -
0x7e4ca010      UDPv4   0.0.0.0 0       *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e4f1180      UDPv4   0.0.0.0 4500    *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e4f1420      UDPv4   0.0.0.0 500     *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e4f5010      UDPv4   0.0.0.0 500     *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e4f5010      UDPv6   ::      500     *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e4f5950      UDPv4   0.0.0.0 4500    *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e4f5950      UDPv6   ::      4500    *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e50dae0      UDPv4   0.0.0.0 0       *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e50dae0      UDPv6   ::      0       *       0               812     svchost.exe     2024-03-09 11:47:51.000000 UTC
0x7e56b4e0      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       444     services.exe    -
0x7e56b4e0      TCPv6   ::      49155   ::      0       LISTENING       444     services.exe    -
0x7e574010      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       444     services.exe    -
0x7e5bc470      UDPv4   127.0.0.1       52953   *       0               1284    iexplore.exe    2024-03-09 12:01:27.000000 UTC
0x7e5cd190      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       1380    svchost.exe     -
0x7e5ce180      UDPv4   0.0.0.0 0       *       0               1380    svchost.exe     2024-03-09 11:47:52.000000 UTC
0x7e5ce7a0      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       1380    svchost.exe     -
0x7e5ce7a0      TCPv6   ::      49156   ::      0       LISTENING       1380    svchost.exe     -
0x7e5cfbb0      UDPv4   0.0.0.0 0       *       0               1380    svchost.exe     2024-03-09 11:47:52.000000 UTC
0x7e5cfbb0      UDPv6   ::      0       *       0               1380    svchost.exe     2024-03-09 11:47:52.000000 UTC
0x7e5ea550      TCPv4   192.168.3.140   49173   192.168.3.133   60457   CLOSED  1804    cGFzdGViaW4uY2  -
0x7e638230      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       348     wininit.exe     -
0x7e640010      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       640     svchost.exe     -
0x7e640010      TCPv6   ::      135     ::      0       LISTENING       640     svchost.exe     -
0x7e735bc0      TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0x7e735bc0      TCPv6   ::      445     ::      0       LISTENING       4       System  -
0x7e753a90      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       348     wininit.exe     -
0x7e753a90      TCPv6   ::      49152   ::      0       LISTENING       348     wininit.exe     -
0x7e75a410      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       640     svchost.exe     -
0x7e79aaa0      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       692     svchost.exe     -
0x7e79f8e0      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       692     svchost.exe     -
0x7e79f8e0      TCPv6   ::      49153   ::      0       LISTENING       692     svchost.exe     -
0x7e7bf9c0      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       812     svchost.exe     -
0x7e7f8900      UDPv4   192.168.3.140   137     *       0               4       System  2024-03-09 11:47:50.000000 UTC
```

There were other files in the temp folder as well so i extracted the file and analysed them.

Multireader.exe had nothing suspicious about it. The file just automated Google search for the selected text every 150ms.

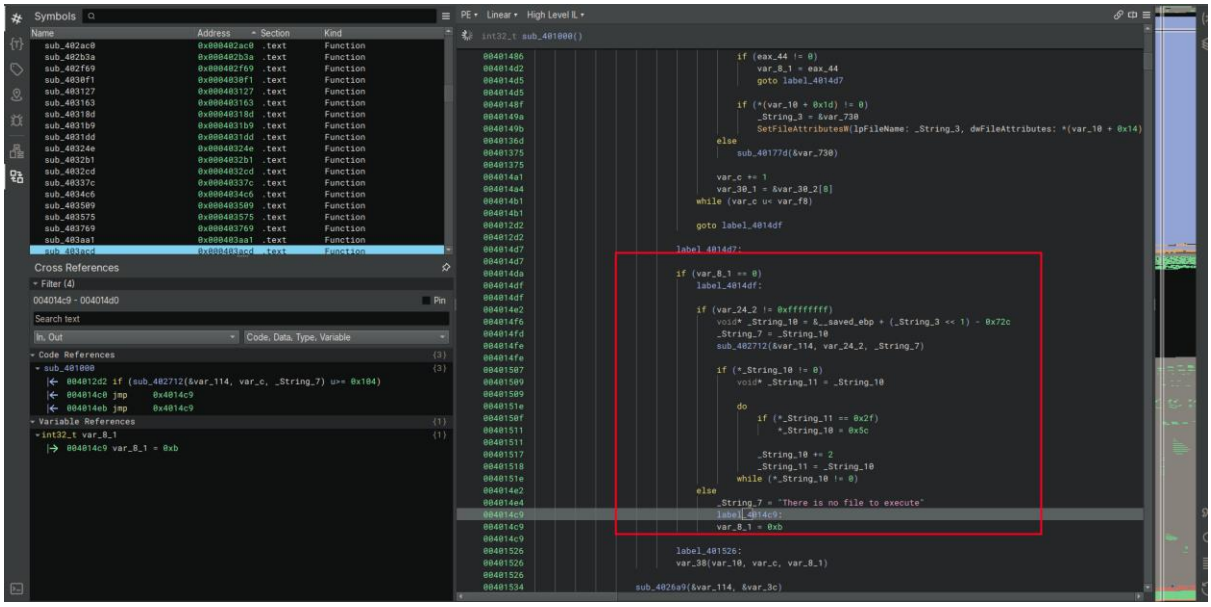
```
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Cache    FileObject      FileName        Result

DataSectionObject       0×7e5e4600      multireader.exe file.0×7e5e4600.0×fa801a4b5310.DataSectionObject.multireader.exe.dat
ImageSectionObject      0×7e5e4600      multireader.exe file.0×7e5e4600.0×fa801a5c9b60.ImageSectionObject.multireader.exe.img
```

Next, I extracted the weird name file and this file was used to show which key was pressed on top of the screen.

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f challenge.mem windows.dumpfiles --physaddr 0×7e2ff070
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Cache    FileObject      FileName        Result

DataSectionObject       0×7e2ff070      cGFzdGViaW4uY29tL3lBYTFhS2l1.exe     file.0×7e2ff070.0×fa8018e51900.DataSectionObject.cGFzdGViaW4uY29tL3lBYTFhS2l1.exe.dat
ImageSectionObject      0×7e2ff070      cGFzdGViaW4uY29tL3lBYTFhS2l1.exe     file.0×7e2ff070.0×fa801a4c09b0.ImageSectionObject.cGFzdGViaW4uY29tL3lBYTFhS2l1.exe.img
```

I found a third file in the same folder. Briefly, this executable tries to create a temp folder and execute some files. I uploaded it to virustotal and gave pretty interesting results..

```
┌──(kali㉿kali)-[~/Downloads/volatility3]
└─$ python3 vol.py -f challenge.mem windows.filescan | grep "temp"
^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A0×7de17f20in\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\SystemCertificates\My
0×7e293dd0      \temp
0×7e2ff070      \temp\cGFzdGViaW4uY29tL3lBYTFhS2l1.exe
0×7e481070      \temp
0×7e4ab070      \temp
0×7e5e4600      \temp\multireader.exe
0×7e5f4f20      \temp
0×7e712e60      \temp\AutoHotkey_1.1.37.01.exe
```



VirusTotal showed that 5 vendors flagged this Malicious and this file might try to connect to C2. Since I'm no binary Ninja I will not be able to uncover how this file executes other files. But in my opinion

1. This is the main file that executes a weird name file by only taking its name and sending information to the Pastebin declared in its code.

2. Other 2 files are just there to waste our time.