

Incident Scenario

Our user "Hattori" has reported strange behavior on his computer and realized that some PDF files have been encrypted, including a critical document to the company named important_document.pdf. He decided to report it; since it was suspected that some credentials might have been stolen, the DFIR team has been involved and has captured some evidence. Join the team to investigate and learn how to get information from a memory dump in a practical scenario.

1.- Sistema operativo del volcado de memoria

```
$ vol -f memdump.mem windows.info
```

```
Is64Bit True
IsPAE False
layer name 0 WindowsIntel32e
memory layer 1 FileLayer
KdVersionBlock 0xf8066222a400
Major/Minor 15.19041
MachineType 34404
KeNumberProcessors 2
SystemTime 2024-02-24 22:52:52
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine 34404
PE TimeDateStamp Sat Jan 13 03:45:32 2085
analyst@ip-10-10-16-17:~$
```

2.- Procesos sospechosos en el sistema

```
$ vol -f memdump.mem windows.pstree
```

* 636	500	services.exe	0xe50ed73d3080	6	-	0	False	2024-02-24 22:47:35.000000	N/A
** 896	636	svchost.exe	0xe50ed7d112c0	9	-	0	False	2024-02-24 22:47:36.000000	N/A
** 1924	636	svchost.exe	0xe50ed73ab2c0	5	-	0	False	2024-02-24 22:47:36.000000	N/A
** 3464	636	svchost.exe	0xe50ed88e3080	7	-	1	False	2024-02-24 22:47:39.000000	N/A
** 7312	636	SecurityHealth	0xe50ed9af1280	10	-	0	False	2024-02-24 22:47:56.000000	N/A
** 2964	636	dllhost.exe	0xe50ed858d280	14	-	0	False	2024-02-24 22:47:37.000000	N/A
** 3348	636	svchost.exe	0xe50ed8b722c0	6	-	0	False	2024-02-24 22:47:39.000000	N/A
** 7060	636	WUDFHost.exe	0xe50ed9ad41c0	9	-	0	False	2024-02-24 22:47:53.000000	N/A
** 792	636	svchost.exe	0xe50ed7c85240	13	-	0	False	2024-02-24 22:47:35.000000	N/A

```
$ vol -f memdump.mem windows.pstree | grep critical -B 2
```

**** 8748	8756	conhost.exe	0xe50edac73340	3	-	1	False	2024-02-24 22:48:03.000000	N/A
*** 7960	3196	cmd.exe	0xe50edacdd080	1	-	1	False	2024-02-24 22:50:40.000000	N/A
**** 3384	7960	conhost.exe	0xe50edab37080	4	-	1	False	2024-02-24 22:50:40.000000	N/A
**** 1648	7960	critical updat	0xe50ed94c1080	5	-	1	False	2024-02-24 22:51:50.000000	N/A
***** 1612	1648	updater.exe	0xe50edab53080	6	-	1	False	2024-02-24 22:51:50.000000	N/A
*** 6460	3196	FTK Imager.exe	0xe50edad09080	19	-	1	False	2024-02-24 22:52:18.000000	N/A

3.- Procesos de red activos en el sistema conectado al puerto 80`$ vol -f memdump.mem windows.netscan`

```
analyst@ip-10-10-16-17:~$ vol -f memdump.mem windows.netscan | grep ESTABLISHED
0xe50ed9087b40.0TCPv4 192.168.182.139n49817fi 192.168.182.128 80 ESTABLISHED 8380 msedge.exe 2024-02-24 22:52:53.000
000
0xe50ed9275a20 TCPv4 192.168.182.139 3389 192.168.182.150 49253 ESTABLISHED 744 svchost.exe 2024-02-24 22:47:52.000
000
0xe50ed9427a20 TCPv4 192.168.182.139 49694 20.7.1.246 443 ESTABLISHED 368 svchost.exe 2024-02-24 22:47:54.000
000
analyst@ip-10-10-16-17:~$
```

4.- Ficheros que se han accedido o ejecutado en el sistema`$ vol -f memdump.mem windows.filescan > filescan.txt`

```
analyst@ip-10-10-16-17:~$ cat filescan.txt | grep updater
0xe50ed736e8a0 \Users\user01\Documents\updater.exe 216
0xe50ed846fc60 \Program Files (x86)\Microsoft\EdgeUpdate\1.3.185.17\msedgeupdateres en.dll 216
0xe50ed8482d10 \Program Files (x86)\Microsoft\EdgeUpdate\1.3.185.17\msedgeupdateres en.dll 216
analyst@ip-10-10-16-17:~$
```

5.- Ficheros que se han accedido o ejecutado en el sistema`vol -f memdump.mem windows.mftscan.MFTScan > mftscan.txt`

```
analyst@ip-10-10-16-17:~$ vol -f memdump.mem windows.mftscan.MFTScan > mftscan.txt
analyst@ip-10-10-16-17:~$ cat mftscan.txt | grep updater
* 0xd389c63ce528 FILE 111417 2 File Archive FILE NAME 2024-02-24 22:51:50.000000 2024-02-24 22:51:50.000000
000 2024-02-24 22:51:50.000000 2024-02-24 22:51:50.000000 updater[1].exe
analyst@ip-10-10-16-17:~$
```

6.- Volcado del proceso pid 1612 updater.exe`$ vol -f memdump.mem -o . windows.memmap --dump --pid 1612`

7.- Buscamos strings en el proceso pid 1612

\$ strings pid.1612.dmp | less

```
j^{k
IxYl
TVdl
j^{k
`X-k
Px@l
OMIL
&F`
,Fn
*Ft
20R`
PROCESSOR IDENTIFIER=AMD64 Family 25 Model 97 Stepping 2, AuthenticAMD
hZG
tN}frL
tN}frL
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
h8H$
DriverData=C:\Windows\System32\Drivers\DriverData
8[G
USERDOMAIN ROAMINGPROFILE=DESKTOP-3NMNM0H
C:\Users\user01\Documents\updater.exe
WB0
SB<
B8
```

Veamos peticiones http con resultado OK

\$ strings pid.1612.dmp | grep 'HTTP\1\0 200 OK' -C 5

```
@s1/0/ dk http://critical-update.com http://critical-update.com http://key.critical-update.com/encKEY.txt
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.10.4
Date: Sat, 24 Feb 2024 22:52:40 GMT
Content-type: text/plain
Content-Length: 9
Last-Modified: Fri, 23 Feb 2024 22:56:51 GMT
--
http
critical-update.com
http
critical-update.com
http://key.critical-update.com/encKEY.txt
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.10.4
Date: Sat, 24 Feb 2024 22:52:40 GMT
Content-type: text/plain
Content-Length: 9
Last-Modified: Fri, 23 Feb 2024 22:56:51 GMT
```

Recursos:

<https://tryhackme.com/r/room/critical>

Volatility 3