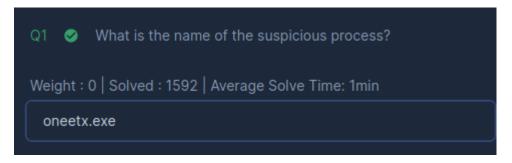
# Digital forensics assignment

Youssef sherif hassan

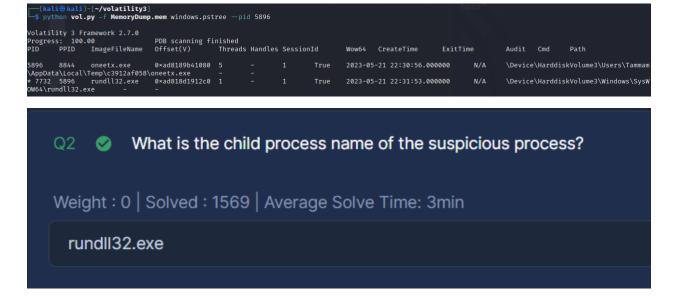
20221041587

Question one

Run python3 vol.py -f MemoryDump.mem windows.pstree to list all processes In the system



#### Question two



## **Question three**

```
-$ python vol.py -f MemoryDump.mem windows.malfind --pid 5896
Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished
PID Process Start VPN End VPN Tag Protec
                                                                     PrivateMemory File output
                                                                                                  Notes Hexdump Disasm
                 0×400000
                                  0×437fff VadS PAGE_EXECUTE_READWRITE 56
      oneetx.exe
                                                                                          Disabled
                                                                                                         MZ header
4d 5a 90 00 03 00 00 00 MZ.....
04 00 00 00 ff ff 00 00 .....
b8 00 00 00 00 00 00 00 ......
40 00 00 00 00 00 00 00 00 0.....
00 00 00 00 00 00 00 00 ......
00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 ......
00 00 00 00 00 01 00 00 ......
                                   4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 40 00 00 00 00 00 00
Q3
                 What is the memory protection applied to the suspicious process memory regi
```

Weight: 0 | Solved: 1502 | Average Solve Time: 8min

PAGE\_EXECUTE\_READWRITE

#### Question four

```
____(kali⊛ kali)-[~/volatility3]
_$ python vol.py -f MemoryDump.mem windows.pslist
Volatility 3 Framework 2.7.0
Progress: 100
PID PPID
            100.00
                                    PDB scanning finished
                 ImageFileName Offset(V)
                                                     Threads Handles SessionId
                                                                                          Wow64 CreateTime
                                                                                                                     ExitTime
                                                                                                                                       File output
                  System 0×ad8185883180 157
                                                                        False
                                                                                 2023-05-21 22:27:10.000000
                                   0×ad81858f2080 4
                                                                                          2023-05-21 22:26:54.000000
2023-05-21 22:27:10.000000
                                                                                                                              N/A
N/A
108
                  Registry
                                                                        N/A
                                                                                 False
                                                                                                                                       Disabled
                                    0×ad81860dc040 2
                                                                                 False
                                                                                                                                       Disabled
                  smss.exe
                                    0×ad81861cd080 12
                                                                                          2023-05-21 22:27:22.000000
                                                                                                                                       Disabled
                                   0×ad8186f1b140 14
                                                                                                                              N/A
528
        520
                  csrss.exe
                                                                                 False
                                                                                          2023-05-21 22:27:25.000000
                                                                                                                                       Disabled
                                    0×ad8186f2b080 1
                                                                                          2023-05-21 22:27:25.000000
552
                                                                                 False
                                                                                                                                       Disabled
         444
                  wininit.exe
                  wininit.exe
winlogon.exe
services.exe
588
                                    0×ad8186f450c0 5
                                                                                          2023-05-21 22:27:25.000000
         552
552
                                                                                          2023-05-21 22:27:29.000000
2023-05-21 22:27:29.000000
676
                                    0×ad8186f4d080 7
                                                                                 False
                                                                                                                              N/A
                                                                                                                                       Disabled
                                    0×ad8186fc6080 10
696
                  lsass.exe
                                                                                 False
                                                                                                                                       Disabled
                  824
                                                                                          2023-05-21 22:27:32.000000
                                                                                 False
                                                                                          2023-05-21 22:27:33.000000
                                                                                                                              N/A
                                                                                                                                       Disabled
         588
                  fontdrvhost.ex 0×ad818761f140 5
                                                                                          2023-05-21 22:27:33.000000
                                                                                                                              N/A
                                                                                                                                       Disabled
860
                                                                                 False
                                                                                          2023-05-21 22:27:36.000000
                                    0×ad81876802c0 12
                                                                                                                                       Disabled
                 dwm.exe 0×ad81876e4340 15 -
svchost.exe 0×ad8187721240 54
         588
                                                                        False
                                                                                 2023-05-21 22:27:38.000000
                                                                                                                              Disabled
                                                                                         2023-05-21 22:27:41.000000
2023-05-21 22:27:43.000000
                                                                                                                              N/A
N/A
448
         676
                                                                                 False
                                                                                                                                       Disabled
                                    0×ad8187758280 21
                  svchost.exe
                                                                                                                                       Disabled
                                    0×ad818774c080 19
                                                                                          2023-05-21 22:27:43.000000
                                                                                                                                       Disabled
                  svchost.exe
1196
         676
                  svchost.exe
                                    0×ad81877972c0 34
                                                                                 False
                                                                                          2023-05-21 22:27:46.000000
                                                                                                                              N/A
                                                                                                                                       Disabled
                  MemCompression 0×ad8187835080 62
                                                                                          2023-05-21 22:27:49.000000
                                                                                                                                       Disabled
1280
         676
                                    0×ad81878020c0
                                                                                          2023-05-21 22:27:49.000000
                                                                                 False
False
                                                                                          2023-05-21 22:27:52.000000
2023-05-21 22:27:52.000000
                                                                                                                              N/A
N/A
1448
         676
                  svchost.exe
                                    0×ad818796c2c0
                                                                                                                                       Disabled
                                    0×ad81879752c0 12
1496
         676
                                                                                                                                       Disabled
                  svchost.exe
                                    0×ad8187a112c0 6
                                                                                          2023-05-21 22:27:58.000000
2023-05-21 22:28:03.000000
2023-05-21 22:28:05.000000
                                                                                                                              N/A
N/A
                                   0×ad8187a2d2c0 10
                                                                                 False
                                                                                                                                       Disabled
1840
                                   0×ad8187acb200 10
                                                                                 False
                                                                                                                                       Disabled
         676
                  spoolsv.exe
                                                                                                                                       Disabled
                                                                                                                              N/A
N/A
                                    0×ad8187b65240
                                                                                          2023-05-21 22:28:11.000000
                                                                                                                                       Disabled
                                                                                          2023-05-21 22:28:19.000000
2023-05-21 22:28:19.000000
         676
                  svchost.exe
                                    0×ad8187b94080 10
                                                                                 False
                                                                                                                                       Disabled
                  vm3dservice.ex 0×ad81896ae240
                                                                                          2023-05-21 22:28:19.000000
                                                                                                                              N/A
N/A
                                                                                                                                       Disabled
                  VGAuthService. 0×ad81896b3300
                                                                                          2023-05-21 22:28:19.000000
                                                                                 False
                                                                                                                                       Disabled
```

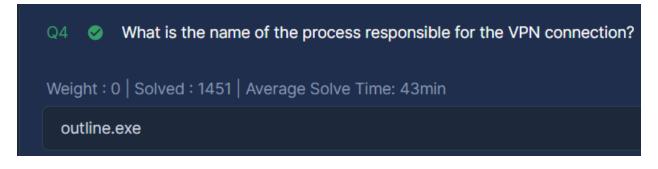
Using netscan

```
on vol.py
                   f MemoryDump.mem windows.netscan
olatility 3 Framework 2.7.0
rogress: 100.00
ffset Proto LocalAddr
                                 PDB scanning finished
                                 LocalPort
                                                  ForeignAddr
                                                                    ForeignPort
                                                                                     State PID
                                                                                                      Owner Created
×ad81861e2310
                TCPv4 0.0.0.0 49668
                                         0.0.0.0 0
                                                           LISTENING
                                                                                                       2023-05-21 22:28:09.000000
                TCPv6
                                 49668
                                                           LISTENING
                                                                             1840
                                                                                                       2023-05-21 22:28:09.000000
ad81861e2310
                        0.0.0.0 5040
                                         0.0.0.0 0
                                                                                                      2023-05-21 22:30:31.000000
×ad81861e2470
                TCPv4
                                                           LISTENING
                                                                                     svchost.exe
                        0.0.0.0 135
                                                           LISTENING
                TCPv4
                                                                                                       2023-05-21 22:27:36.000000
×ad81861e2730
                                          0.0.0.0 0
                                                                                     svchost.exe
                                          0.0.0.0 0
                                                           LISTENING
                                                                                                       2023-05-21 22:27:36.000000
ad81861e2b50
                TCPv4
×ad81861e2b50
                TCPv6
                                49665
                                                           LISTENING
                                                                                                       2023-05-21 22:27:36.000000
                        0.0.0.0 49665
                                         0.0.0.0 0
                                                           LISTENING
                                                                                                      2023-05-21 22:27:36.000000
2023-05-21 22:27:36.000000
×ad81861e2e10
                TCPv4
                                                                                     wininit.exe
                TCPv4
                        0.0.0.0 49664
                                                                                     lsass.exe
×ad81861e3230
                                          0.0.0.0 0
×ad81861e3390
                TCPv4
                                          0.0.0.0 0
                                                           LISTENING
                                                                                     svchost.exe
                                                                                                       2023-05-21 22:27:36.000000
xad81861e3390
                TCPv6
                                                           LISTENING
                                                                                     svchost.exe
                                                                                                      2023-05-21 22:27:36.000000
                                                                                     lsass.exe
                        0.0.0.0 49664
                                         0.0.0.0 0
                                                                                                      2023-05-21 22:27:36.000000
×ad81861e34f0
                TCPv4
                                                           LISTENING
                                                                            696
                TCPv6
                                                           LISTENING
                                                                                                       2023-05-21 22:27:36.000000
×ad81861e34f0
×ad81861e37b0
                TCPv4
                        0.0.0.0 49666
                                         0.0.0.0 0
                                                           LISTENING
                                                                                     svchost.exe
                                                                                                       2023-05-21 22:27:49.000000
                                                                                                      2023-05-21 22:27:49.000000
2023-05-21 22:27:58.000000
×ad81861e37b0
                TCPv6
                               49666
                                                           LISTENING
                                                                            1012
                                                                                     sychost.exe
                        0.0.0.0 49667
                                         0.0.0.0 0
                                                           LISTENING
                TCPv4
×ad81861e3910
                                                                                     svchost.exe
                TCPv6
                                                           LISTENING
                                                                                     svchost.exe
                                                                                                       2023-05-21 22:27:58.000000
                        0.0.0.0 49668
×ad81861e3a70
                TCPv4
                                         0.0.0.0 0
                                                           LISTENING
                                                                            1840
                                                                                     spoolsv.exe
                                                                                                       2023-05-21 22:28:09.000000
                        0.0.0.0 49666
                                                           LISTENING
                                                                                                       2023-05-21 22:27:49.000000
×ad81861e3bd0
                TCPv4
                                         0.0.0.0 0
                                                                            1012
                                                                                     svchost.exe
×ad81861e3e90
                TCPv4
                        0.0.0.0 49667
                                                           LISTENING
                                                                                     svchost.exe
                                                                                                       2023-05-21 22:27:58.000000
                                                                                     System 2023-05-21 22:29:04.000000
System 2023-05-21 22:29:04.000000
ad818662ecb0
                TCPv4
                        0.0.0.0 445
×ad818662ecb0
                TCPv6
                                                           LISTENING
×ad818662f390
                        0.0.0.0 7680
                                          0.0.0.0 0
                                                                                                      2023-05-21 22:58:09.000000
                TCPv4
                                                           LISTENING
                                                                                     svchost.exe
                                                                                                       2023-05-21 22:58:09.000000
                TCPv6
                                                           LISTENING
                                                                                     System 2023-05-21 22:27:56.000000
System 2023-05-21 22:27:56.000000
×ad81878518f0
               UDPv4
                        192.168.190.141 137 192.168.190.141 139
×ad8187852250
                UDPv4
×ad818902a5d0
                TCPv4
                                                  0.0.0.0 0
                                                                   LISTENING
                                                                                              System 2023-05-21 22:27:56.000000
ad818971f870
                UDPv4
                                                                             SkypeApp.exe
                                                                                              2023-05-21 22:58:07.000000
                                56250
                                                                            SkypeApp.exe
CLOSED 448
×ad818971f870
                UDPv6
                                                                    6644
                                                                                              2023-05-21 22:58:07.000000
                        10.0.85.2
                                          55439
                                                  20.22.207.36
                                                                                                              2023-05-21 23:00:40.000000
×ad81897eb010
                TCPv4
                                                                                             svchost.exe
ad81898a6d10
                         127.0.0.1
                                                                                                     2023-05-21 22:28:54.000000
ad81898bc7f0
                UDPv4
                        0.0.0.0 5355
                                                                                              2023-05-21 22:57:37.000000
×ad81898bc7f0 UDPv6
                                 5355
                                                                             svchost.exe
                                                                                             2023-05-21 22:57:37.000000
```

, look for connections involving VPN server IPs/domains (e.g., 20.22.207.36, 38.121.43.65, 204.79.197.203, etc.) on relevant ports.

0×ad818662f390	TCPv4	0.0.0.0 7680	0.0.0.0	0	LISTENIN	G	5476	svchost.	.exe	2023-05-	-21 22:58:	:09.000000
0×ad818662f390	TCPv6	:: 7680		0	LISTENIN	G	5476	svchost.	.exe	2023-05-	-21 22:58	:09.000000
0×ad81878518f0	UDPv4	192.168.190.141	138		0			System	2023-05-	21 22:27	7:56.00000	00
0×ad8187852250	UDPv4	192.168.190.141	137		0			System	2023-05-	21 22:27	7:56.00000	00
0×ad818902a5d0	TCPv4	192.168.190.141	139	0.0.0.0	0	LISTENI	NG		System	2023-05-	-21 22:27	:56.000000
0×ad818971f870	UDPv4	0.0.0.0 56250		0		6644	SkypeApp	o.exe	2023-05-	21 22:58	3:07.00000	00
0×ad818971f870	UDPv6	:: 56250		0		6644	SkypeAp		2023-05-	21 22:58	3:07.00000	00
0×ad81897eb010	TCPv4	10.0.85.2	55439	20.22.2		443	21 11	448	sychost.			21 23:00:40.000000
0×ad81898a6d10	UDPv4	127.0.0.1	57787	*	0		448	sychost.			-21 22:28	:54.000000
0×ad81898bc7f0	UDPv4	0.0.0.0 5355	*	0		1448	sychost	exe			7:37.00000	
0×ad81898bc7f0	UDPv6	:: 5355	*	0		1448	svchost				7:37.00000	
0×ad8189a291b0	TCPv4	0.0.0.0 55972	0.0.0.0	0	LISTENIN		5964	svchost.				57.000000
0×ad8189a291b0	TCPv6	:: 55972		0	LISTENIN		5964	svchost				57.000000
0×ad8189a29470	TCPv4	0.0.0.0 55972	0.0.0.0		LISTENIN		5964	svchost				57.000000
0×ad8189a2a7b0	TCPv4	0.0.0.0 49669	0.0.0.0		LISTENIN		676	services				:08.000000
0×ad8189a2a7b0	TCPV4	0.0.0.0 49669	0.0.0.0		LISTENIN		676	services				:08.000000
nasstva tyr												
0×ad8189a2a910	TCPv6	:: 49669	::	0	LISTENIN		676	services				:08.000000
0×ad8189a30a20	TCPv4	192.168.190.141		38.121.		443	CLOSED	4628	tun2sock			21 22:00:25.000000
0×ad8189a844e0	UDPv4	10.0.85.2	58844		0		5328	msedge.				:53.000000
0×ad8189cea350	UDPv4	0.0.0.0 5050		0		1196	svchost		2023-05-	21 22:30	0:27.00000	00
0×ad818c17ada0	UDPv4	0.0.0.0 52051	*	0		4628	tun2socl	cs.exe	2023-05-	21 22:24	4:14.00000	00

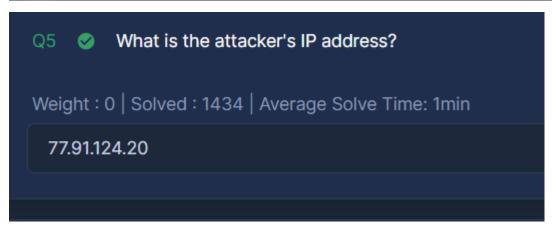
Process is tun2socks.exe and the parent which is the answer is **outline.exe** 



## **Question five**

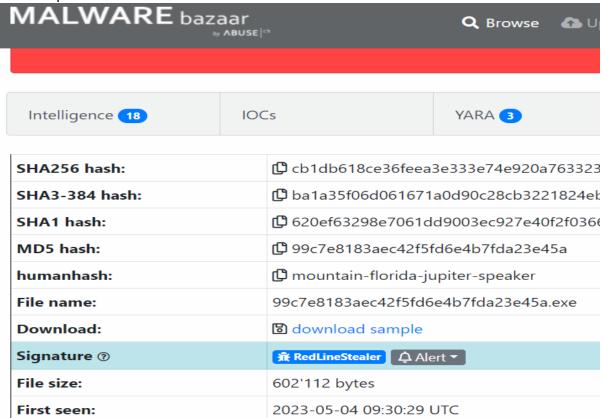
## Using also netscan command

×ad818da21bd0	UDPv4	0.0.0.0 0	*	0	5964	svchost.exe	2023-05-21 22:27:57.000000
×ad818dbc1a60	TCPv4	192.168.190.141	49713	104.119.188.96	443	CLOSE_WAIT	1916 SearchApp.exe 2023-05-21 22:33:11.000000
×ad818dd05370	UDPv4	0.0.0.0 5353		0	5328	msedge.exe	2023-05-21 23:01:32.000000
×ad818dd07440	UDPv4	0.0.0.0 5353		0	5328	msedge.exe	2023-05-21 23:01:32.000000
×ad818dd07440	UDPv6	:: 5353		0	5328	msedge.exe	2023-05-21 23:01:32.000000
×ad818de4aa20	TCPv4	10.0.85.2	55462	77.91.124.20	80	CLOSED 5896	oneetx.exe 2023-05-21 23:01:22.000000



#### Question six

Browse the ip in malware bazaar website



Q6 Sased on the previous artifacts. What is the name of the malware family?

Weight: 0 | Solved: 1356 | Average Solve Time: 25min

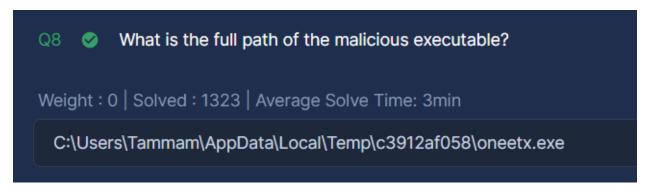
redline stealer

#### Question seven

Same page look for the php file



## Question eight



Using filescan command

Python vol.py -f MemoryDump.mem windows.filescanFileScan

0	×ad818d436310	\Windows\System32\winevt\Logs\Microsoft-Windows-Fault-Tolerant-Heap%40perational.evtx	216
0	×ad818d436630	\CMApi 216	
0	×ad818d436950	\Program Files\VMware\VMware Tools\plugins\vmusr\desktopEvents.dll 216	
0	×ad818d436c70	\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe 216	- 10
0	×ad818d436e00	\Windows\System32\en-GB\edgehtml.dll.mui 216	
0	×ad818d437120	\Windows\System32\en-US\KernelBase.dll.mui 216	- 1//