


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

Q1  What is the name of the suspicious process?


Weight : 0 | Solved : 1592 | Average Solve Time: 1min

oneetx.exe

Question two

```
(kali@kali)-[~/volatility3]
$ python vol.py -f MemoryDump.mem windows.pstree --pid 5896

Volatility 3 Framework 2.7.0
Progress: 100.00
PDB scanning finished
Offset(V)
Threads Handles SessionId Wow64 CreateTime ExitTime Audit Cmd Path
PID PPID ImageFileName
5896 8844 oneetx.exe 0xad8189b41080 5 - 1 True 2023-05-21 22:30:56.000000 N/A \Device\HarddiskVolume3\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe
* 7732 5896 rundll32.exe 0xad818d1912c0 1 - 1 True 2023-05-21 22:31:53.000000 N/A \Device\HarddiskVolume3\Windows\SysWOW64\rundll32.exe
```

Q2  What is the child process name of the suspicious process?

Weight : 0 | Solved : 1569 | Average Solve Time: 3min

rundll32.exe

Question three

Using netscan

```
$ python vol.py -f MemoryDump.mem windows.netscan
```

Volatility 3 Framework 2.7.0
Progress: 100.00

Offset	Proto	LocalAddr	LocalPort	PDB scanning finished	ForeignAddr	ForeignPort	State	PID	Owner	Created
xad81861e2310	TCPv4	0.0.0.0	49668	0.0.0.0	0	LISTENING	1840	spoolsv.exe	2023-05-21	22:28:09.000000
xad81861e2310	TCPv6	::	49668	::	0	LISTENING	1840	spoolsv.exe	2023-05-21	22:28:09.000000
xad81861e2470	TCPv4	0.0.0.0	5040	0.0.0.0	0	LISTENING	1196	svchost.exe	2023-05-21	22:30:31.000000
xad81861e2730	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING	952	svchost.exe	2023-05-21	22:27:36.000000
xad81861e2b50	TCPv4	0.0.0.0	49665	0.0.0.0	0	LISTENING	552	wininit.exe	2023-05-21	22:27:36.000000
xad81861e2b50	TCPv6	::	49665	::	0	LISTENING	552	wininit.exe	2023-05-21	22:27:36.000000
xad81861e2e10	TCPv4	0.0.0.0	49665	0.0.0.0	0	LISTENING	552	wininit.exe	2023-05-21	22:27:36.000000
xad81861e3230	TCPv4	0.0.0.0	49664	0.0.0.0	0	LISTENING	696	lsass.exe	2023-05-21	22:27:36.000000
xad81861e3390	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING	952	svchost.exe	2023-05-21	22:27:36.000000
xad81861e3390	TCPv6	::	135	::	0	LISTENING	952	svchost.exe	2023-05-21	22:27:36.000000
xad81861e34f0	TCPv4	0.0.0.0	49664	0.0.0.0	0	LISTENING	696	lsass.exe	2023-05-21	22:27:36.000000
xad81861e34f0	TCPv6	::	49664	::	0	LISTENING	696	lsass.exe	2023-05-21	22:27:36.000000
xad81861e37b0	TCPv4	0.0.0.0	49666	0.0.0.0	0	LISTENING	1012	svchost.exe	2023-05-21	22:27:49.000000
xad81861e37b0	TCPv6	::	49666	::	0	LISTENING	1012	svchost.exe	2023-05-21	22:27:49.000000
xad81861e3910	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	448	svchost.exe	2023-05-21	22:27:58.000000
xad81861e3910	TCPv6	::	49667	::	0	LISTENING	448	svchost.exe	2023-05-21	22:27:58.000000
xad81861e3a70	TCPv4	0.0.0.0	49668	0.0.0.0	0	LISTENING	1840	spoolsv.exe	2023-05-21	22:28:09.000000
xad81861e3bd0	TCPv4	0.0.0.0	49666	0.0.0.0	0	LISTENING	1012	svchost.exe	2023-05-21	22:27:49.000000
xad81861e3e90	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	448	svchost.exe	2023-05-21	22:27:58.000000
xad818662ecb0	TCPv4	0.0.0.0	445	0.0.0.0	0	LISTENING	4	System	2023-05-21	22:29:04.000000
xad818662ecb0	TCPv6	::	445	::	0	LISTENING	4	System	2023-05-21	22:29:04.000000
xad818662f390	TCPv4	0.0.0.0	7680	0.0.0.0	0	LISTENING	5476	svchost.exe	2023-05-21	22:58:09.000000
xad818662f390	TCPv6	::	7680	::	0	LISTENING	5476	svchost.exe	2023-05-21	22:58:09.000000
xad81878518f0	UDPv4	192.168.190.141	138	*	0	4	System	2023-05-21	22:27:56.000000	
xad8187852250	UDPv4	192.168.190.141	137	*	0	4	System	2023-05-21	22:27:56.000000	
xad818902a5d0	TCPv4	192.168.190.141	139	0.0.0.0	0	LISTENING	4	System	2023-05-21	22:27:56.000000
xad818971f870	UDPv4	0.0.0.0	56250	*	0	6644	SkypeApp.exe	2023-05-21	22:58:07.000000	
xad818971f870	UDPv6	::	56250	*	0	6644	SkypeApp.exe	2023-05-21	22:58:07.000000	
xad81897eb010	TCPv4	10.0.85.2	55439	20.22.207.36	443	CLOSED	448	svchost.exe	2023-05-21	23:00:40.000000
xad81898a6d10	UDPv4	127.0.0.1	57787	*	0	448	svchost.exe	2023-05-21	22:28:54.000000	
xad81898bc7f0	UDPv4	0.0.0.0	5355	*	0	1448	svchost.exe	2023-05-21	22:57:37.000000	
xad81898bc7f0	UDPv6	::	5355	*	0	1448	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.

0xad818662f390	TCPv4	0.0.0.0	7680	0.0.0.0	0	LISTENING	5476	svchost.exe	2023-05-21	22:58:09.000000
0xad818662f390	TCPv6	::	7680	::	0	LISTENING	5476	svchost.exe	2023-05-21	22:58:09.000000
0xad81878518f0	UDPv4	192.168.190.141	138	*	0	4	System	2023-05-21	22:27:56.000000	
0xad8187852250	UDPv4	192.168.190.141	137	*	0	4	System	2023-05-21	22:27:56.000000	
0xad818902a5d0	TCPv4	192.168.190.141	139	0.0.0.0	0	LISTENING	4	System	2023-05-21	22:27:56.000000
0xad818971f870	UDPv4	0.0.0.0	56250	*	0	6644	SkypeApp.exe	2023-05-21	22:58:07.000000	
0xad818971f870	UDPv6	::	56250	*	0	6644	SkypeApp.exe	2023-05-21	22:58:07.000000	
0xad81897eb010	TCPv4	10.0.85.2	55439	20.22.207.36	443	CLOSED	448	svchost.exe	2023-05-21	23:00:40.000000
0xad81898a6d10	UDPv4	127.0.0.1	57787	*	0	448	svchost.exe	2023-05-21	22:28:54.000000	
0xad81898bc7f0	UDPv4	0.0.0.0	5355	*	0	1448	svchost.exe	2023-05-21	22:57:37.000000	
0xad81898bc7f0	UDPv6	::	5355	*	0	1448	svchost.exe	2023-05-21	22:57:37.000000	
0xad8189a291b0	TCPv4	0.0.0.0	55972	0.0.0.0	0	LISTENING	5964	svchost.exe	2023-05-21	22:27:57.000000
0xad8189a291b0	TCPv6	::	55972	::	0	LISTENING	5964	svchost.exe	2023-05-21	22:27:57.000000
0xad8189a29470	TCPv4	0.0.0.0	55972	0.0.0.0	0	LISTENING	5964	svchost.exe	2023-05-21	22:27:57.000000
0xad8189a2a7b0	TCPv4	0.0.0.0	49669	0.0.0.0	0	LISTENING	676	services.exe	2023-05-21	22:29:08.000000
0xad8189a2a910	TCPv4	0.0.0.0	49669	0.0.0.0	0	LISTENING	676	services.exe	2023-05-21	22:29:08.000000
0xad8189a2a910	TCPv6	::	49669	::	0	LISTENING	676	services.exe	2023-05-21	22:29:08.000000
0xad8189a30a20	TCPv4	192.168.190.141	53660	38.121.43.65	443	CLOSED	4628	tun2socks.exe	2023-05-21	22:00:25.000000
0xad8189a844e0	UDPv4	10.0.85.2	58844	*	0	5328	msedge.exe	2023-05-21	22:51:53.000000	
0xad8189cea350	UDPv4	0.0.0.0	5050	*	0	1196	svchost.exe	2023-05-21	22:30:27.000000	
0xad818c17ada0	UDPv4	0.0.0.0	52051	*	0	4628	tun2socks.exe	2023-05-21	22:24:14.000000	

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

Q4

What is the name of the process responsible for the VPN connection?

Weight : 0 | Solved : 1451 | Average Solve Time: 43min

outline.exe

Question five

Using also netscan command

xad818da21bd0	UDPv4	0.0.0.0	0	*	0	5964	svchost.exe	2023-05-21	22:27:57.000000
xad818dbc1a60	TCPv4	192.168.190.141	49713	104.119.188.96	443	CLOSE_WAIT	1916	SearchApp.exe	2023-05-21 22:33:11.000000
xad818dd05370	UDPv4	0.0.0.0	5353	*	0	5328	msedge.exe	2023-05-21	23:01:32.000000
xad818dd07440	UDPv4	0.0.0.0	5353	*	0	5328	msedge.exe	2023-05-21	23:01:32.000000
xad818dd07440	UDPv6	:::5353	*	0	5328	msedge.exe	2023-05-21	23:01:32.000000	
xad818de4aa20	TCPv4	10.0.85.2	55462	77.91.124.20	80	CLOSED	5896	oneetx.exe	2023-05-21 23:01:22.000000

Q5

What is the attacker's IP address?

Weight : 0 | Solved : 1434 | Average Solve Time: 1min

77.91.124.20

Question six

Browse the ip in malware bazaar website

MALWARE bazaar

by ABUSE|^{CH}

Browse


U

Intelligence 18

IOCs

YARA 3

SHA256 hash:	cb1db618ce36feea3e333e74e920a763323
SHA3-384 hash:	ba1a35f06d061671a0d90c28cb3221824ek
SHA1 hash:	620ef63298e7061dd9003ec927e40f2f036c
MD5 hash:	99c7e8183aec42f5fd6e4b7fda23e45a
humanhash:	mountain-florida-jupiter-speaker
File name:	99c7e8183aec42f5fd6e4b7fda23e45a.exe
Download:	download sample
Signature	RedLineStealer Alert
File size:	602'112 bytes
First seen:	2023-05-04 09:30:29 UTC

Q6  Based 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



abuse_ch

RedLineStealer C2:


<http://77.91.124.20/store/games/index.php>

Q7  What is the full URL of the PHP file that the attacker visited?

Weight : 0 | Solved : 1331 | Average Solve Time: 1min

<http://77.91.124.20/store/games/index.php>

Question eight

Q8  What is the full path of the malicious executable?

Weight : 0 | Solved : 1323 | Average Solve Time: 3min

C:\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe

Using filescan command

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

```
0xad818d436310 \Windows\System32\winevt\Logs\Microsoft-Windows-Fault-Tolerant-Heap%40operational.evtx 216
0xad818d436630 \CMApi 216
0xad818d436950 \Program Files\VMware\VMware Tools\plugins\vmusr\desktopEvents.dll 216
0xad818d436c70 \Users\Tammam\AppData\Local\Temp\c3912af058\pneetx.exe 216
0xad818d436e00 \Windows\System32\en-GB\edgehtml.dll.mui 216
0xad818d437120 \Windows\System32\en-US\KernelBase.dll.mui 216
```