Blue Team Labs Online: Memory Analysis - Ransomware

The following writeup is for Memory Analysis - Ransomware on Blue Team Labs Online, it's an easy lab that involves analysing a memory dump using volatility. This was my first ever BLTO challenge, and I thoroughly enjoyed doing it. Those who are knew to memory forensics should definitely check this room out.

Scenario: The Account Executive called the SOC earlier and sounds very frustrated and angry. He stated he can't access any files on his computer and keeps receiving a pop-up stating that his files have been encrypted. You disconnected the computer from the network and extracted the memory dump of his machine and started analyzing it with Volatility. Continue your investigation to uncover how the ransomware works and how to stop it!

Run "vol.py -f infected.vmem --profile=Win7SP1x86 psscan" that will list all processes. What is the name of the suspicious process?

I prefer using volatility 3, so I am simply going to run the volatility3 equivalent to this command:

```
python .\vol.py -f .\infected.vmem windows.psscan | Out-GridView
```

After looking at the output, it becomes immediately obviously that @WanaDecryptor is the malicious process (WannaCry ransomware):

2688	2732	@WanaDecryptor	0x1ef9ed40	0	-	1	False	2021-01-31 18:24:49.000000 UTC	...
268	4	smss.exe	0x1efb5418	2	29	N/A	False	2021-01-31 18:01:10.000000 UTC	N/A ...
2232	496	SearchIndexer.	0x1efc1d40	10	704	0	False	2021-01-31 18:01:18.000000 UTC	...
2432	496	sppsvc.exe	0x1fcbc0f0	4	147	0	False	2021-01-31 18:03:14.000000 UTC	...
3968	2732	@WanaDecryptor	0x1fcc6800	1	59	1	False	2021-01-31 18:02:48.000000 UTC	...

What is the parent process ID for the suspicious process?

The PPID can be found in the second column of the psscan output, in this instance it is 2732.

What is the initial malicious executable that created this process?

If we execute the following command, we can see that @WannaDecyptor's parent process is or4qtckT.exe:

```
python .\vol.py -f .\infected.vmem windows.pstree | Out-GridView
```

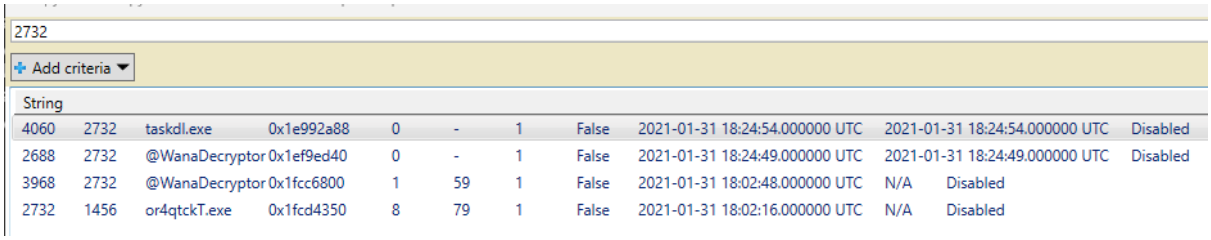
*	2732	1456	or4qtckT.exe
**	3968	2732	@WanaDecryptor

We know this based on the hierarchy and how the PPID of @WannaDecyptor matches the PID of or4qtckT.exe.

If you drill down on the suspicious PID (vol.py -f infected.vmem --profile=Win7SP1x86 psscan | grep (PIDhere)), find the process used to delete files

If we run psscan we can see taskdl.exe which is relatively suspicious:

```
python .\vol.py -f .\infected.vmem windows.psscan | Out-GridView
```



psscan is able to identify processes that are hidden or terminated, which is why we cant see this process through running pslist or pstree.

Find the path where the malicious file was first executed?

For this question I am going to use cmder so I have access to grep. All we need to do is use the filescan plugin like as follows:

```
λ python vol.py -f infected.vmem windows.filescan | grep or4
WARNING  volatility3.framework.layers.vmware: No metadata file
ected.vmem and infected.vmss.
0x1ed75ae8 100.0\Users\hacker\Desktop\or4qtckT.exehed
0x1fcaf798      \Users\hacker\Desktop\or4qtckT.exe
```

Here we can see that the file path for the malicious file is \Users\hacker\Desktop\or4qtckT.exe

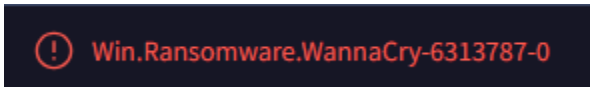
Can you identify what ransomware it is? (Do your research!)

This is textbook WannaCry, and this is obvious due to the @WannaDecyptor process which is what displays a GUI demanding a ransom. Alternatively, you can dump the executable of the @WannDecyptor process, generate its hash, and search that in VirusTotal:

```
python .\vol.py -f .\infected.vmem windows.pslist --pid 3968 --dump
```

```
Get-FileHash -Algorithm SHA1 .\3968._WanaDecryptor.0x400000.dmp
```

Detections such as those from ClamAV categorise it as WannaCry ransomware:



What is the filename for the file with the ransomware public key that was used to encrypt the private key? (.eky extension)

Seeing as we are given the file extension, we can follow the same technique we used to find the malicious executable to find the public key file:

```
λ python vol.py -f infected.vmem windows.filescan | grep eky
WARNING  volatility3.framework.layers.vmware: No metadata file
ected.vmem and infected.vmss.
0x1fca6268 100.0\Users\hacker\Desktop\00000000.ekyhed
```

The answer is 00000000.eky (ignore hed).