

Memory Analysis - Ransomware

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!

Volatility

Points

20

Difficulty

Medium

Solves

3061

OS

Windows/Linux

1. Flag: Identificación del proceso sospechoso

Run "vol.py -f infected.vmem --profile=Win7SP1x86 psscan" that will list all processes. What is the name of the suspicious process? (3 points)

Format: @ProcessName

Submit

Para encontrar el proceso sospechoso, decidí analizar el proceso explorer.exe, ya que muchas veces sirve como punto de partida para identificar procesos anómalos iniciados por el usuario o malware.

Comand: **python3 vol.py -f '/home/csi/Desktop/BTLO Memory Analysis - Ransomware/infected.vmem' windows.pstree**

400	568	wintlogon.exe	0x83d03030	3	113	1	False	2021-01-31 18:01:11.000000	N/A
1456	1408	explorer.exe	0x84c6a030	26	765	1	False	2021-01-31 18:01:12.000000	N/A
* 1688	1456	vm3dservice.ex	0x84cf9d40	2	44	1	False	2021-01-31 18:01:12.000000	N/A
* 2732	1456	or4qtckT.exe	0x83ed4350	8	79	1	False	2021-01-31 18:02:16.000000	N/A
** 3968	2732	@WanaDecryptor	0x83ec6800	1	59	1	False	2021-01-31 18:02:48.000000	N/A
* 1700	1456	vmtoolsd.exe	0x84d04498	8	218	1	False	2021-01-31 18:01:12.000000	N/A
2968	2924	taskhsvc.exe	0x85e33030	4	102	1	False	2021-01-31 18:02:20.000000	N/A

Observando el árbol de procesos de **explorer.exe**, identifiqué un proceso llamado **or4qtckT.exe**, el cual a su vez inició un proceso sospechoso con el nombre **@WanaDecryptor**.

Run "vol.py -f infected.vmem --profile=Win7SP1x86 psscan" that will list all processes. What is the name of the suspicious process? (3 points)

@WanaDecryptor

Correct! ✓

2- Flag Parent PID del proceso malicioso

What is the parent process ID for the suspicious process? (3 points)

Parent Process ID (PPID)

Submit

Al revisar nuevamente el árbol de procesos, noté que el proceso **or4qtckT.exe** tiene como PID padre (PPID) el valor **2732**.

1456	1408	explorer.exe	0x84c6a030	26	765	1	False	2021-01-31 18:01:12.000000	N/A
1600	1456	vm3dservice.exe	0x84cf9d40	2	44	1	False	2021-01-31 18:01:12.000000	N/A
2732	1456	or4qtckT.exe	0x83ed4350	8	79	1	False	2021-01-31 18:02:16.000000	N/A
* 3968	2732	@WanaDecryptor	0x83ec6800	1	59	1	False	2021-01-31 18:02:48.000000	N/A
* 1700	1456	vmtoolsd.exe	0x84d04498	8	218	1	False	2021-01-31 18:01:12.000000	N/A
2968	2924	taskhsvc.exe	0x85e33030	4	102	1	False	2021-01-31 18:02:20.000000	N/A

Por lo cual la flag seria Esta

Flag:2732

What is the parent process ID for the suspicious process? (3 points)

2732

Correct! ✓

3- Flag: Nombre del proceso que inició el malware

What is the initial malicious executable that created this process? (3 points)

Format: filename.exe

Submit

Observando de igual manera el árbol de procesos de Explorer vemos que el proceso que creo inicio el malware es:

460	388	winlogon.exe	0x85d63030	3	113	1	False	2021-01-31	18:01:11.000000	N/A
1456	1408	explorer.exe	0x84c6a030	26	765	1	False	2021-01-31	18:01:12.000000	N/A
* 1688	1456	vm3dservice.exe	0x84cf9d40	2	44	1	False	2021-01-31	18:01:12.000000	N/A
* 2732	1456	or4qtckT.exe	0x83ed4350	8	79	1	False	2021-01-31	18:02:16.000000	N/A
** 3968	2732	@WanaDecryptor	0x83ec6800	1	59	1	False	2021-01-31	18:02:48.000000	N/A
* 1700	1456	vmtoolsd.exe	0x84d04498	8	218	1	False	2021-01-31	18:01:12.000000	N/A
2968	2924	taskhsvc.exe	0x85e33030	4	102	1	False	2021-01-31	18:02:20.000000	N/A

Flag: or4qtckT.exe

What is the initial malicious executable that created this process? (3 points)

or4qtckT.exe

Correct! ✓

4-Flag: Tarea generada por el proceso malicioso

Filtrando por el PID **2732** y utilizando el plugin **psscan**, identifiqué que el proceso malicioso creó una tarea (task) con el propósito de eliminar archivos, una acción común en ataques de ransomware.

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 (3 points)

Format: filename.extension

Submit

Filtrando por el PID **2732** y utilizando el plugin **psscan**, identifiqué que el proceso malicioso creó una tarea (task) con el propósito de eliminar archivos, una acción común en ataques de ransomware.

```
python3 vol.py -f '/home/csi/Desktop/BTLO Memory Analysis - Ransomware/infected.vmem' windows.psscan | grep 2732
000ress 2732 taskdl.exe 0x1e992a88 0 - 1 False 2021-01-31 18:24:54.000000 2021-01-31 18:24:54.000000 Disabled
968 2732 @WanaDecryptor 0x1ef9ed40 0 - 1 False 2021-01-31 18:24:49.000000 2021-01-31 18:24:49.000000 Disabled
968 2732 @WanaDecryptor 0x1fcc6800 1 59 1 False 2021-01-31 18:02:48.000000 N/A Disabled
2732 1456 or4qtckT.exe 0x1fcd4350 8 79 1 False 2021-01-31 18:02:16.000000 N/A Disabled
```

Flag: taskdl.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 (3 points)

taskdl.exe

Correct! ✓

5-Flag: Ruta de ejecución inicial del malware

Find the path where the malicious file was first executed (3 points)

Format: drive:\path\to\filename.extension

Submit

Para determinar cuándo y desde dónde se ejecutó el malware por primera vez, utilicé el plugin **cmdline** junto con **grep** para filtrar por el PID **2732**.

```
python3 vol.py -f '/home/csi/Desktop/BTLO Memory Analysis - Ransomware/infected.vmem' windows.cmdline | grep 2732
```

```
04:41:03 csi@csi /opt/volatility3
> python3 vol.py -f '/home/csi/Desktop/BTLO Memory Analysis - Ransomware/infected.vmem' windows.cmdline | grep 2732
2732 or4qtckT.exe "C:\Users\hacker\Desktop\or4qtckT.exe"
```

La ruta de ejecución identificada fue:

La flag: **C:\Users\hacker\Desktop\or4qtckT.exe**

Find the path where the malicious file was first executed (3 points)

C:\Users\hacker\Desktop\or4qtckT.exe

Correct! ✓

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

General Info

File name	or4qtckT.exe
Full analysis	https://app.any.run/tasks/30a48f99-5aef-4214-b6ed-5863a92825f8
Verdict	Malicious activity
Threats:	<div>WannaCry</div> <div>WannaCry is a famous Ransomware that utilizes the EternalBlue exploit. This malware is known for infecting at least 200,000 computers worldwide and it continues to be an active and dangerous threat.</div> <div>Malware Trends Tracker More details</div>
Analysis date	1/28/2021, 10:39:44
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags:	ransomware wannacry wannacryptor
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84C82835A5D21BBCF75A61706D8AB549
SHA1	5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467
SHA256	ED01EBFBC9EB5BBEA545AF4D01BF5F1071661840480439C6E5BABE8E080E41AA
SSDEEP	98304:QQPOBHZ1ARXCSUDK36SAEDHVXWA9P593R8YAVP2G3X:QQPE1CXCXK3ZAEUADZr8YC4GB

Can you identify what ransomware it is? (Do your research!) (2 points)

wannacry

Correct! ✓

7- Flag: Clave pública utilizada por el ransomware

What is the filename for the file with the ransomware public key that was used to encrypt the private key? (.eky extension) (3 points)

Format: filename.eky

Submit

Para encontrar la clave pública, utilicé el comando **strings** en conjunto con **grep**, buscando archivos con la extensión **.eky**, la cual es común en variantes de ransomware para almacenar claves

strings infected.vmem | grep eky

```
04:53:33 csi@csi ~/Desktop/BTLO Memory Analysis - Ransomware
$ strings infected.vmem | grep eky
00000000.eky
%08X.eky
00000000.eky
ntor-onion-key U4/KcG1ps0jpLuE8cd8qI6zQ/52YTJaLX9WbxekySk0=
s+3Uc4gjE2RJhXkvwi6t1sUJmogfMLxLDDiXSpXekyHwVurAv/3yB6EPaRoujh1t
MIGJAoGBAPWZYCeKAn1MnwQjFNDim2Ie2eU6hDfDsaeky54mh8bJGIh1DgF2NJUL
3vmilrxFkeazE6PEt6zZ0Yi/X2hcEpKmgTr+iLG/qPu7v/x6pp00HR8cxUc1ekyW
%08X.eky
%08X.eky
```

Flag: **00000000.eky**

What is the filename for the file with the ransomware public key that was used to encrypt the private key? (.eky extension) (3 points)

00000000.eky

Correct! ✓

What is the initial malicious executable that created this process?



Congratulations!
You completed **Memory Analysis - Ransomware**

Share Achievement

Click the button above and share the link

Can you identify what ransomware it is? (do your research!) (2 points)

wanncry

What is the filename for the file with the ransomware public key that (3 points)

00000000.exe

BY Manuel Perez

NK Maloweer