

1. Flag: Identificación del proceso sospechoso



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

+00	200	wintogon.exe	UXODUUSUSU	3	112	Т	raise	2021-01-31 10:01:11.000000	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

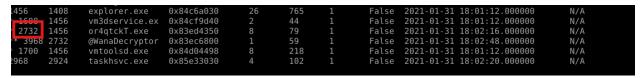
Observando el árbol de procesos de explorer.exe, identifiqué un proceso llamado or4qtckT.exe, el cual a su vez inició un proceso sospechoso con el nombre @WanaDecryptor.



2- Flag Parent PID del proceso malicioso

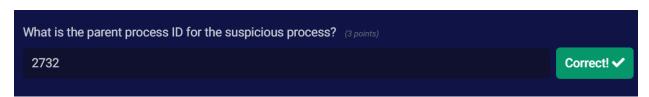


Al revisar nuevamente el árbol de procesos, noté que el proceso or4qtckT. exe tiene como PID padre (PPID) el valor **2732**.



Por lo cual la flag seria Esta

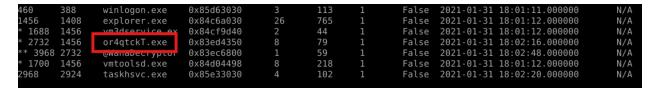
Flag:2732



3- Flag: Nombre del proceso que inició el malware



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



Flag: or4qtckT.exe

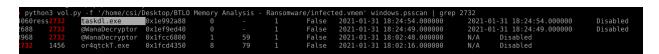


4-Flag: Tarea generada por el proceso malicioso

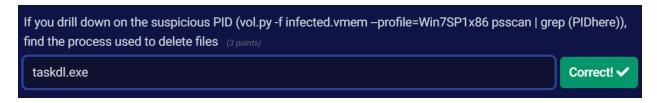
Filtrando por el PID **2732** y utilizando el plugin **psscan**, identifiqué que el proceso malicioso creó una tarea (task) con el propósito de eliminar archivos, una acción común en ataques de ransomware.



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.



Flag: taskdl.exe



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

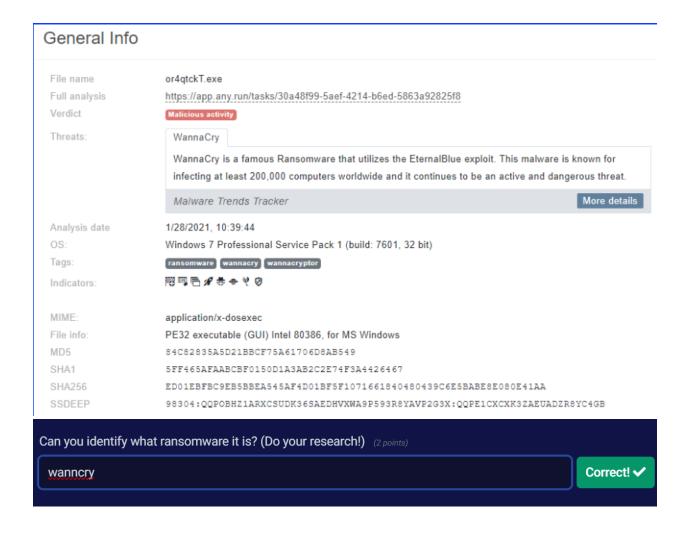


La ruta de ejecución identificada fue:

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



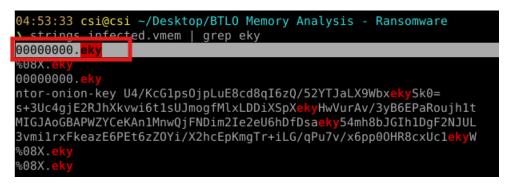
6-flag Can you identify what ransomware it is? (Do your research!)





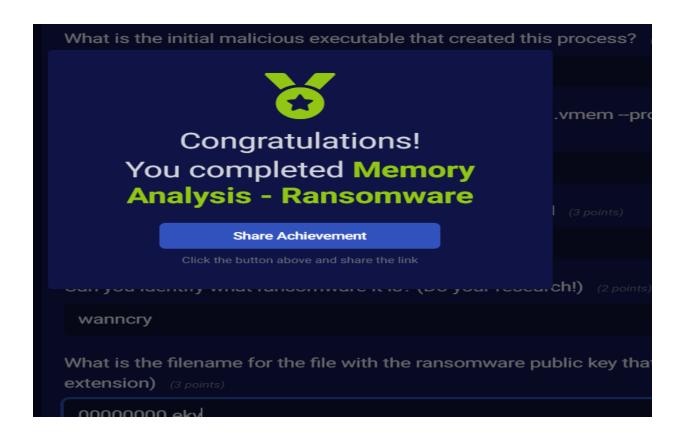
Para encontrar la clave pública, utilicé el comando **strings** en conjunto con **grep**, buscando archivos con la extensión **.eky**, la cual es común en variantes de ransomware para almacenar claves

strings infected.vmem | grep eky



Flag: 0000000.eky





BY Manuel Perez

NK Maloweer