Memory Analysis - Ransomware

Autor: Manuel Pérez

Alias: NK Maloweer

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.

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

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.

Flag: 2732

3. Flag: Nombre del proceso que inició el malware

Siguiendo el análisis del árbol de procesos, determiné que el ejecutable responsable de iniciar el malware fue:

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.

Flag: taskdl.exe

5. Flag: Ruta de ejecución inicial del malware

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:

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

6. Flag: ¿Qué ransomware es?

Basado en el nombre del proceso @WanaDecryptor y los patrones observados durante el análisis, se concluye que el ransomware en cuestión es WannaCry. Este ransomware es conocido por usar ese nombre de ventana y comportamiento específico.

7. Flag: Clave pública utilizada por el ransomware

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: 00000000.eky