https://urjc-my.sharepoint.com/personal/j_lammering_2023_alumnos_urjc_es/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fj%5Flammering%5F2023%5Falumnos%5Furjc%5Fes%2FDocuments%2FIntelegencia%20de%20la%20Seguridad&view=0

Práctica 3: Inteligencia de la Seguridad

Ingeniería de la Ciberseguridad

Jakob Lammering
Diego Tejada Merinero

Introducción

En esta primera parte de la práctica de forense digital, nos sumergimos en los fundamentos de la investigación de incidentes a través de un ejercicio focalizado en el malware WannaCry. Crearemos un escenario controlado con una Máquina Virtual Windows 7 Professional y la someteremos a un simulacro de ataque de WannaCry.

Simularemos las tácticas del ransomware para entender su propagación, vulnerabilidades explotadas y las implicaciones de un ataque exitoso en la máquina comprometida.

Posteriormente, generamos un volcado de memoria de la máquina comprometida, capturando una instantánea detallada del estado de la memoria en el momento del ataque, preservando así información valiosa sobre las actividades maliciosas.

La siguiente fase estará conformada por el uso de la herramienta Volatility, una plataforma potente en forense digital. Utilizaremos Volatility para desentrañar la complejidad del ataque, identificando indicadores de compromiso, vulnerabilidades explotadas y otros artefactos digitales dejados por WannaCry. Explicaremos cada evidencia con capturas, ofreciendo una visión completa de las vulnerabilidades identificadas y las tácticas de WannaCry.

A través de esta práctica, no solo exploramos las amenazas de WannaCry, sino que también fortaleceremos nuestras habilidades en forense digital, mejorando nuestra capacidad para investigar, analizar y responder a incidentes de seguridad en entornos digitales complejos.

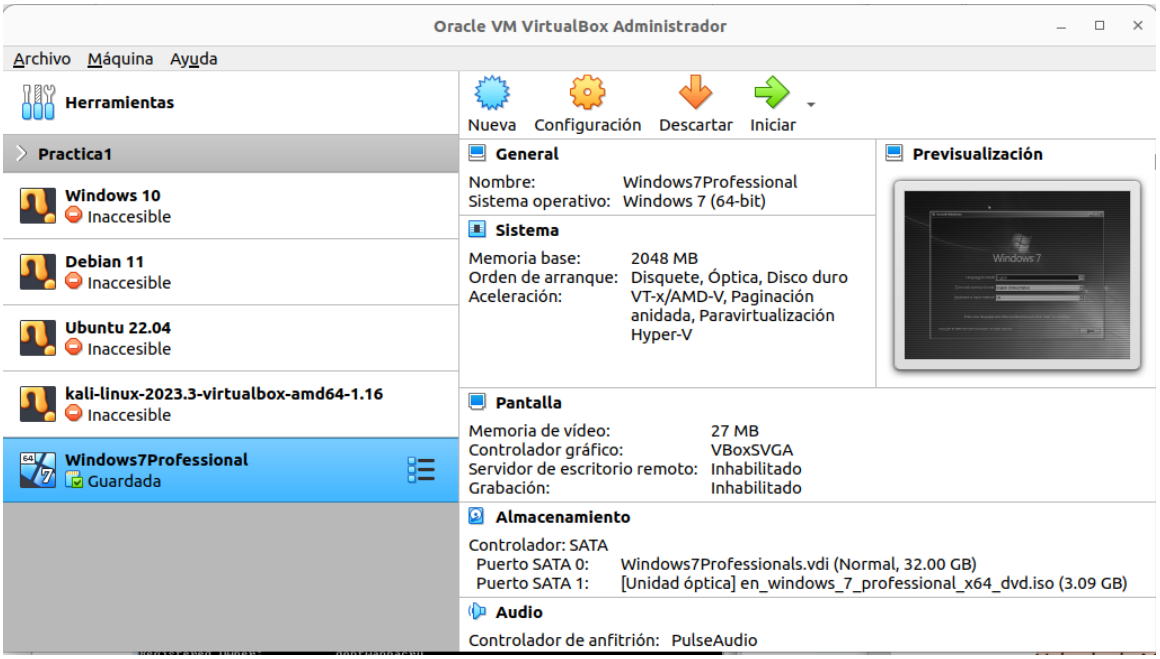
El volcado de memoria creado de nuestra pasantía en formato ".raw", que se puede utilizar para el análisis en Volatility, se puede encontrar en el siguiente enlace: https://urjc-my.sharepoint.com/:i:/g/personal/j_lammering_2023_alumnos_urjc_es/ESYXedAJ_GRLj6bQh4PY5aoBsFAJ3IV0z0ySP9PvFT8Eeg?e=yFNbjS

Preparación del Entorno

Instalación de la máquina virtual

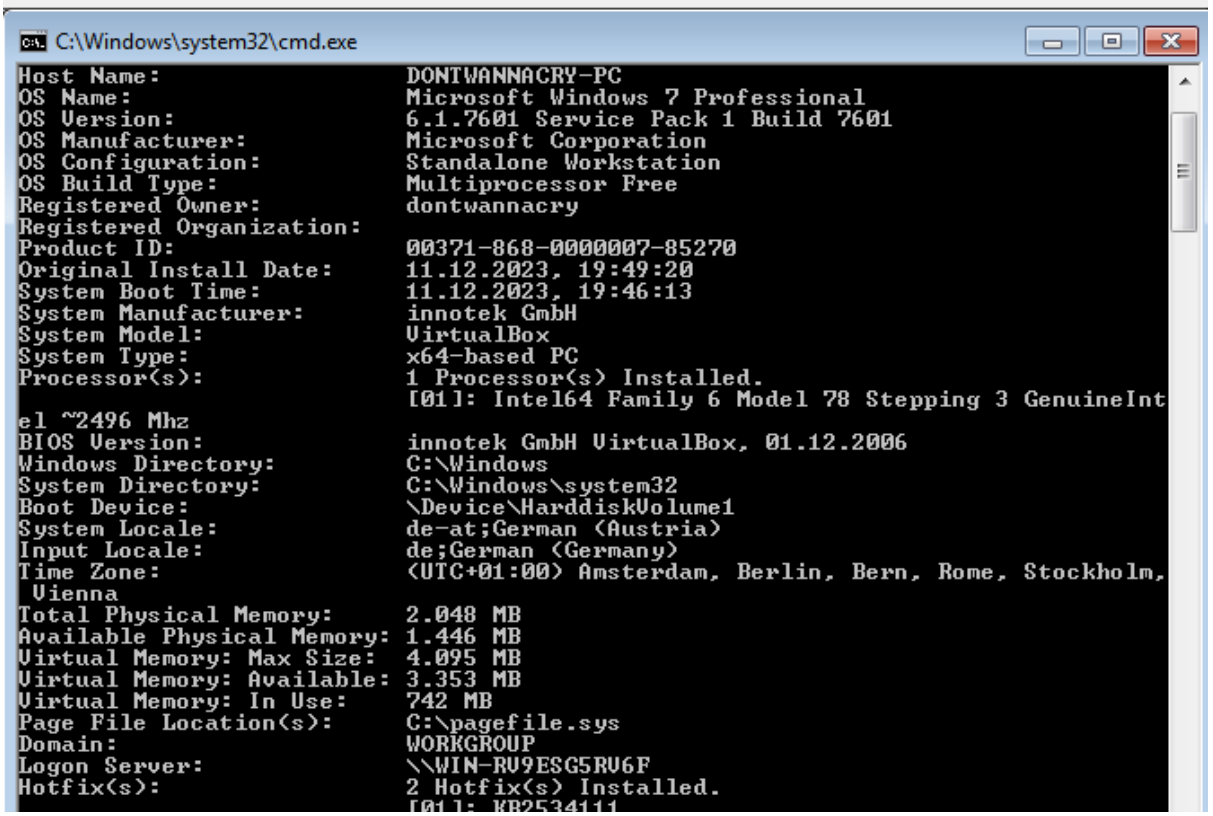
Para simular el ataque de WannaCry sin causar ningún daño a nuestra computadora anfitriona, primero debemos configurar el entorno virtual. Para ello, utilizaremos VirtualBox e instalaremos Windows 7 Professional en una nueva máquina virtual. Windows 7 Professional x64 suele tener 2 GB de RAM de forma predeterminada, por lo que adoptaremos esta configuración para nuestra memoria principal y procederemos con la instalación de la máquina virtual. La elección de la máquina Windows 7 Professional se

justifica porque versiones más recientes de Windows, como Windows 10, ya han sido parcheadas contra el ataque de WannaCry, lo que hace que la simulación sea imposible.

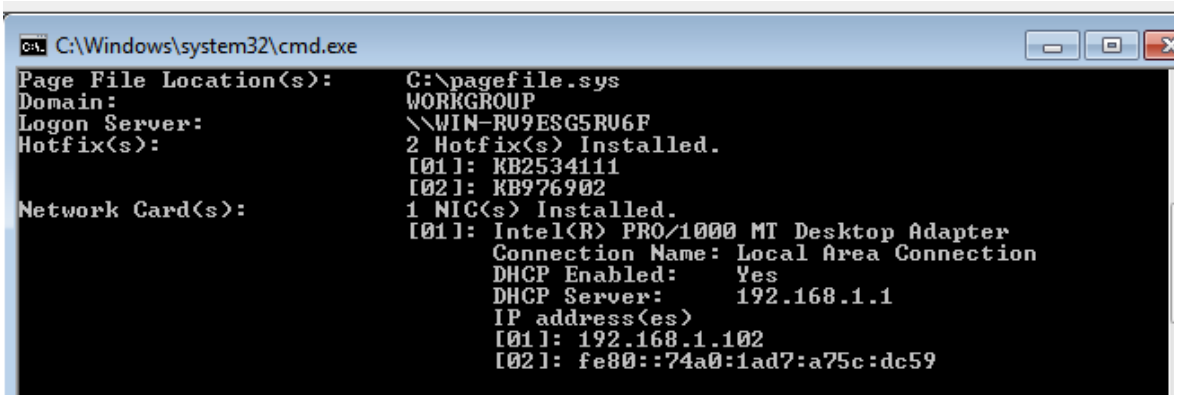


Información del sistema

Una vez que hemos instalado con éxito la máquina virtual, vamos a echar un vistazo más de cerca a la información del sistema para obtener una mejor visión general de nuestro entorno virtual. En el primer paso, ahora abrimos CMD y ejecutamos el comando "systeminfo", que tiene la siguiente salida.



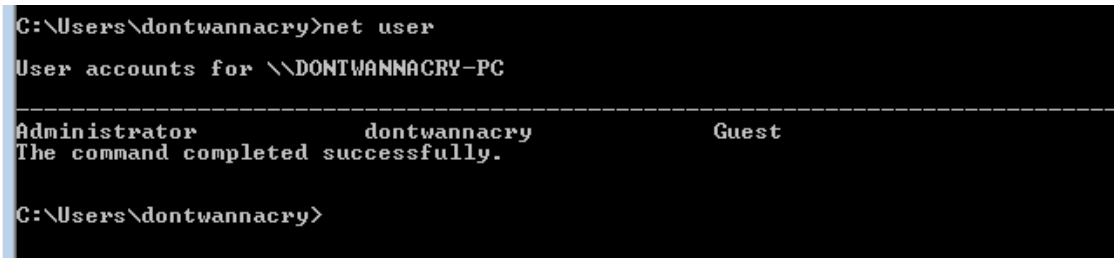
Como podemos ver en la salida, estamos en el host "DONTWANNACRY-PC" y se está ejecutando la versión deseada de Windows 7 Professionals. Nuestra máquina virtual se está ejecutando en una arquitectura de ordenador Windows basada en x64. La máquina tiene 2048 MB (2 GB) de RAM y 4 GB adicionales de memoria virtual. El directorio de Windows de nuestra máquina se encuentra en "C:Windows" y el directorio del sistema en "C:\Windows\system32". El comando "systeminfo" también muestra información sobre nuestra tarjeta de red:



Esto nos dice que nuestro servidor DHCP se está ejecutando en 192.168.1.1 y nos ha asignado la dirección IP4 192.168.1.102 y la dirección IP6 fe80::74a0:1ad7:a75c:dc59. Como en nuestro host local se está ejecutando un sistema Linux, en este caso no tenemos que preocuparnos de que el virus se propague al host local, ya que el virus WannaCry sólo funciona en sistemas operativos Windows. De lo contrario, tendríamos que asegurar adicionalmente el tráfico de red de la máquina virtual y también comprobar las posibles carpetas compartidas antes de ejecutar el virus.

Información del usuario

Para ver qué usuarios están presentes en nuestro sistema, ejecutamos el comando "net user", que devuelve la siguiente salida:



En consecuencia, en nuestro sistema hay un usuario que tiene derechos de administrador en la máquina virtual y se llama "dontwannacry".

Información sobre los programas instalados

Nuestra máquina virtual Windows 7 Professional tiene instalados todos los programas predeterminados de Windows 7 Professional, que se pueden visualizar de la siguiente manera:

Menú Inicio: Podemos encontrar muchos de estos programas pulsando el botón "Inicio" y navegando por el menú "Todos los programas" o "Programas". He aquí una breve lista de los programas más importantes:

Internet Explorer: El navegador web por defecto en Windows 7.

Git: Un sistema de control de versiones distribuido que permite realizar un seguimiento de los cambios en el código fuente y facilita la colaboración entre varios desarrolladores en proyectos de software.

7-Zip: archivador de archivos gratuito y de código abierto que admite varios formatos de archivo, incluido ZIP. Ofrece una interfaz potente y fácil de usar.

En nuestro caso, sin embargo, los programas instalados no juegan un papel importante y sólo utilizamos Internet Explorer para instalar git para descargar el virus WannaCry y 7-ZIP para descomprimir finalmente nuestro archivo zip descargado.

Vulneración Ética

Descripción del contexto de WannaCry

WannaCry es un ransomware que ganó notoriedad a nivel mundial en mayo de 2017. Este malware se propaga a través de una vulnerabilidad en el protocolo SMB (Server Message

Block) de Microsoft Windows, conocida como EternalBlue, que había sido previamente filtrada por el grupo de hackers Shadow Brokers. Una vez que infecta un sistema, WannaCry cifra los archivos del usuario y exige un rescate en bitcoins para desbloquear los datos.

- Características clave de WannaCry:

Expansión Rápida: WannaCry se destacó por su capacidad para propagarse rápidamente a través de redes, afectando tanto a sistemas individuales como a grandes organizaciones. La velocidad de propagación se debió, en gran medida, a su capacidad para explotar la vulnerabilidad mencionada.

Encriptación de Archivos: El principal objetivo de WannaCry es cifrar archivos en la computadora infectada, lo que impide el acceso del usuario a sus datos. Los archivos se vuelven inaccesibles hasta que se pague un rescate.

Demanda de Rescate en Bitcoin: Como es común en los ataques de ransomware, WannaCry exige un pago en bitcoins para proporcionar la clave de desencriptación. Este aspecto lo convierte en un ataque de tipo ransomware.

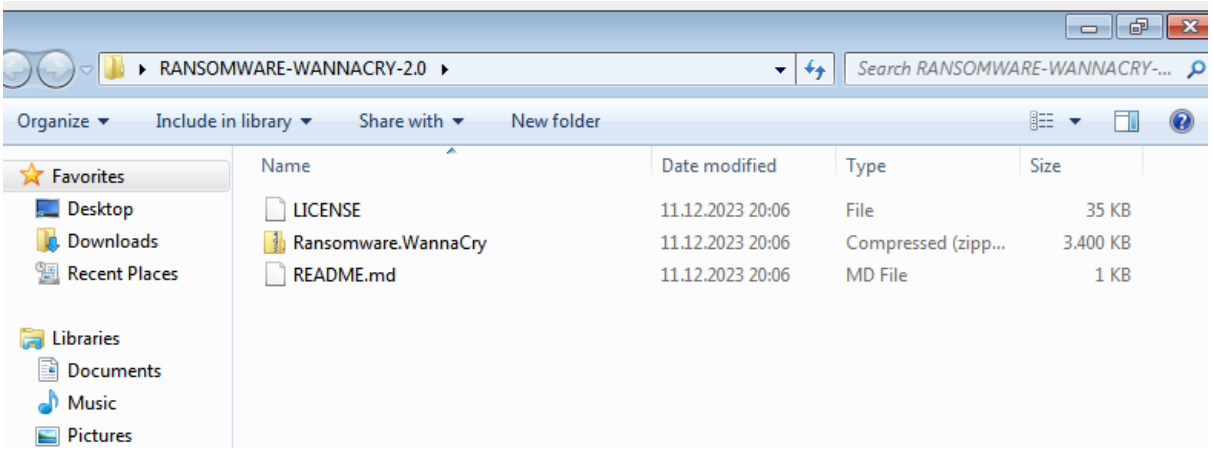
Impacto Global: WannaCry afectó a una amplia variedad de organizaciones en todo el mundo, incluyendo sistemas de salud, empresas y servicios gubernamentales. Su propagación a gran escala resaltó la importancia de mantener actualizados los sistemas y de aplicar parches de seguridad.

Detección y Kill Switch: Un investigador de seguridad, accidentalmente, encontró un "kill switch" o interruptor de apagado en el código de WannaCry. Este descubrimiento permitió frenar parcialmente la propagación del malware, pero no antes de que causara un impacto significativo.

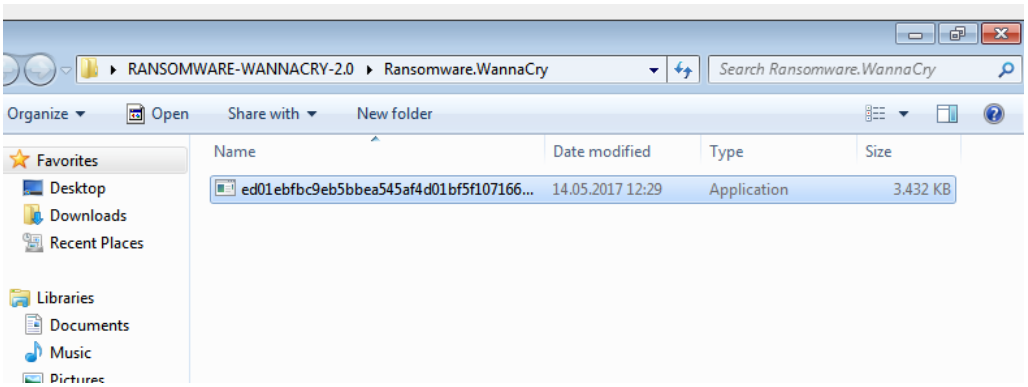
WannaCry sirvió como un recordatorio de la importancia de la ciberseguridad, las actualizaciones regulares de software y la concienciación sobre las amenazas en línea. Además, impulsó discusiones sobre la responsabilidad de las organizaciones en la protección de sus sistemas y la necesidad de compartir información sobre vulnerabilidades para prevenir ataques similares en el futuro.

Descarga del virus WannaCry

Ahora queremos ejecutar intencionadamente el virus en nuestra máquina virtual para poder analizar después el volcado de memoria. Para descargar el virus a nuestra máquina virtual Windows 7 Professional primero clonamos el siguiente repositorio de Github con el comando "git clone https://github.com/chronosmiki/RANSOMWARE-WANNACRY-2.0". A continuación, obtenemos la carpeta que se muestra en la imagen, que contiene el archivo Ransomware.WannaCry.zip.



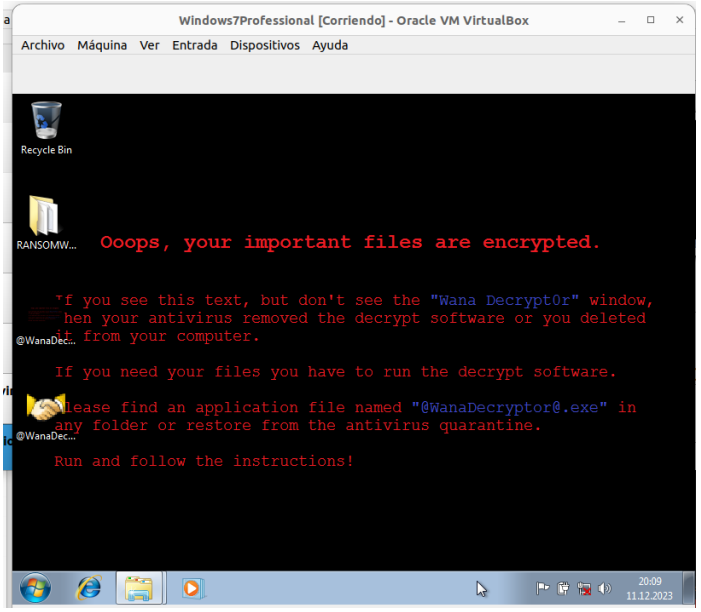
En el siguiente paso, descomprimimos el archivo con la herramienta 7-Zip y obtenemos el siguiente archivo, que contiene un único archivo .exe que representa nuestro virus.



Ejecutando el virus WannaCry

Ahora todo lo que tenemos que hacer es ejecutar el archivo ".exe" en nuestro ordenador y el virus WannaCry cobrará vida. Inmediatamente después, podemos ver cómo los archivos de nuestro sistema se van cifrando poco a poco y el proceso ya no se puede detener, seguido de la imagen tan familiar del "Wana Decrypt0r" pidiendo el pago de Bitcoin a cambio de la clave privada para descifrar todos nuestros archivos.

Incluso si ahora volvemos a nuestro escritorio, podemos ver que el fondo de pantalla ha cambiado y todos nuestros archivos han sido cifrados. Esto asegura que el virus WannaCry se ha ejecutado con éxito en nuestra máquina virtual.



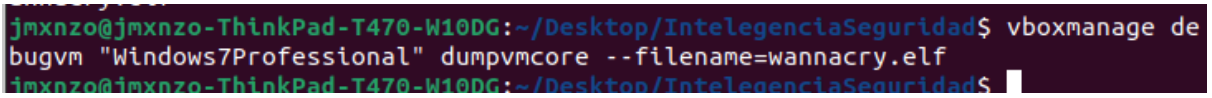
WannaCry fue conocido por su capacidad para propagarse rápidamente a través de redes utilizando una vulnerabilidad en el protocolo SMB. Esta característica permitió que el malware se extendiera a otros sistemas conectados a la misma red.

En su propagación inicial, WannaCry aprovechó una vulnerabilidad en sistemas Windows que no estaban actualizados con el parche de seguridad correspondiente. Una vez que infecta un sistema, busca activamente otros sistemas vulnerables en la red para infectarlos también.

Volcado de Memoria

Creación del volcado de memoria en VirtualBox

Como hemos alojado nuestro sistema infectado en una máquina virtual de VirtualBox, afortunadamente es mucho más fácil crear un volcado de memoria de nuestra máquina virtual y se puede implementar con un solo comando usando "vboxmanage".



El comando `vboxmanage`, específicamente `vboxmanage debugvm`, se utiliza en VirtualBox para llevar a cabo diversas operaciones de depuración y análisis en una máquina virtual (VM). Aquí tenemos una explicación para el comando de la captura anterior:

`vboxmanage`: Esta es la herramienta de línea de comandos de VirtualBox para la gestión de máquinas virtuales.

`debugvm`: Este subcomando de `vboxmanage` permite realizar operaciones de depuración en una máquina virtual.

"Windows7Professional": Aquí se especifica el nombre de nuestra máquina virtual en la que se realizará la depuración.

`dumpvmcore`: Este comando indica que se debe crear un volcado de núcleo (Core Dump) de la máquina virtual. Un Core Dump es una instantánea de la memoria y el estado de la VM en un momento específico.

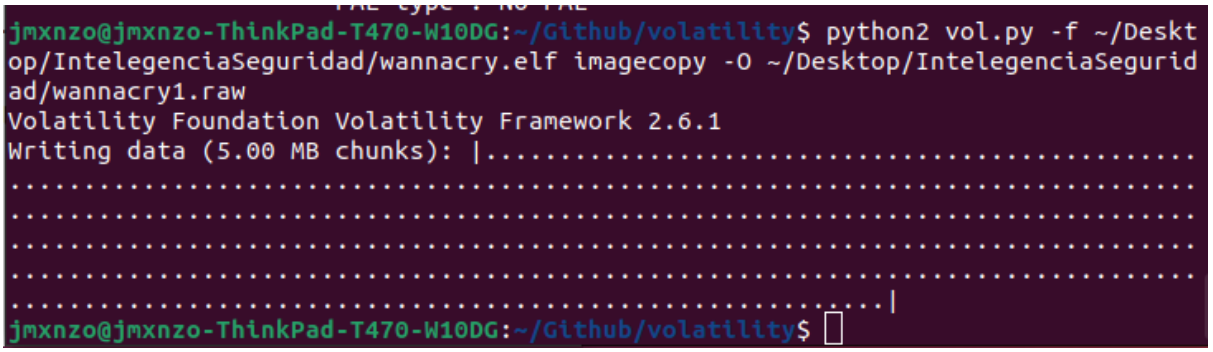
`--filename=wannacry.elf`: Aquí se proporciona el nombre de archivo para el Core Dump creado. En nuestro caso elegimos wannacry.elf.

Normalmente, el volcado de memoria se guarda en el formato del sistema operativo invitado. Dado que nuestro sistema operativo invitado es un sistema operativo Windows, la extensión del archivo debería haber sido ".dmp" y no ".elf", que es la convención de nomenclatura para los sistemas Linux. Sin embargo, como se trata sólo de una cuestión de nomenclatura y la imagen se convierte ahora en un archivo ".raw" de todos modos, se puede prescindir aquí de la confusa nomenclatura, que tampoco tiene ningún efecto sobre el resultado final. No obstante, queríamos mencionarlo brevemente en este punto para evitar cualquier confusión al respecto.

Convertir el volcado de memoria en un imagen .raw

El archivo ".raw" que se creará a continuación describe una representación binaria de toda la memoria de trabajo en el momento del volcado de memoria. Contiene información sobre procesos, estructuras del núcleo y otros contenidos de la memoria.

La conversión al formato “.raw” permite seguir utilizando el volcado de memoria con otras herramientas de análisis. Volatility ofrece entonces la posibilidad de acceder a este formato “.raw” y realizar análisis como la identificación de procesos, sockets abiertos o conexiones de red.



El comando python2 vol.py -f ~/Desktop/IntelegenciaSeguridad/wannacry.elf imagecopy -O ~/Desktop/IntelegenciaSeguridad/wannacry1.raw en Volatility realiza una conversión indirecta en la que el área de memoria se extrae del archivo .dmp (wannacry.elf) y se copia en un archivo .raw independiente (wannacry1.raw).

python2 vol.py: Llama a Volatility, donde python2 especifica la versión del intérprete Python 2.

-f ~/Desktop/IntelegenciaSeguridad/wannacry.elf: Especifica la ruta al archivo .dmp desde el que se copia la zona de memoria.

imagecopy: El comando de Volatility que copia el área de memoria.

-O ~/Desktop/IntelegenciaSeguridad/wannacry1.raw: Especifica la ruta de salida y el nombre del archivo .raw en el que se escribe el área de memoria copiada.

El comando copia toda el área de memoria, ya que no se han especificado otras opciones específicas, como --pid o --address. Esto significa que toda la memoria física de la máquina virtual o del proceso se copia en el archivo .raw. Dado que se trata de un análisis de virus y no se dispone de información específica sobre identificadores de proceso (--pid) o direcciones de memoria específicas (--address) en el momento de ejecutar el comando, en nuestro caso es necesario copiar todo el espacio de memoria. Este es a menudo el caso dada la naturaleza de un análisis de virus, ya que necesitamos toda la información disponible para un examen exhaustivo y por lo tanto necesitamos copiar todo el espacio de memoria, incluso si esto resulta en archivos de mayor tamaño.

Por último, ya hemos creado el archivo "wannacry1.raw", que contiene la información necesaria sobre procesos, estructuras del kernel y otros contenidos de la memoria y que puede analizarse en el siguiente paso en la herramienta Volatility con el fin de identificar posibles vulnerabilidades, indicadores de compromiso (IoC) y otros artefactos digitales.
El volcado de memoria creado de nuestra pasantía en formato ".raw", que se puede utilizar para el análisis en Volatility, se puede encontrar en el siguiente enlace:

https://urjc-my.sharepoint.com/:i:/g/personal/j_lammering_2023_alumnos_urjc_es/ESYXedAJ_GRLj6bQh4PY5aoBsFAJ3IV0z0ySP9PvFT8Eeg?e=yFNbjS

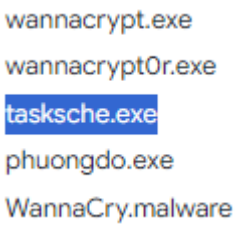
Análisis con Volatility

Información de la imagen

En primer lugar es necesario aclarar lo siguiente: Para identificar variantes específicas de WannaCry, se utiliza un hash criptográfico único asociado a su código. Un ejemplo de este hash es "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa".

El nombre del archivo ejecutable vinculado a WannaCry puede variar, y uno de los nombres comunes asociados es "tasksche.exe". Es importante señalar que los nombres de archivo pueden ser cambiados por los autores del malware para confundir la detección.

Al utilizar servicios como VirusTotal, es posible obtener información sobre el malware mediante la consulta de su hash. En este caso, el hash mencionado se asocia con la variante WannaCry que utiliza el nombre de archivo "tasksche.exe".



Ahora si pasamos al análisis de volatility. Una vez realizamos el ataque y todo el volcado de memoria para poder analizarlo, vamos a usar volatility para poder reconstruir en el tiempo todas actividades realizadas en el sistema infectado y confirmar que el ataque fue realizado y además que fue este en concreto. Para ello, primero lanzamos el volatility a la imagen en

formato .raw que tenemos en el directorio de la siguiente captura y nos arroja la siguiente información:

As Layer1: WindowsAMD64PagedMemory (Kernel AS): Indica que la primera capa es la memoria paginada del kernel para sistemas operativos Windows de 64 bits.

As Layer2: FileAdressSpace (/home/jmxnzo/Desktop/InteligenciaSeguridad/wannacry1.raw): La segunda capa es el espacio de direcciones del archivo proporcionado (wannacry1.raw). Esto significa que Volatility está utilizando este archivo como fuente de información de memoria para el análisis.

PAE type: No PAE: Indica que el sistema operativo en cuestión no utiliza Physical Address Extension.

DTB: 0x187000L: Es la dirección base de la tabla de directorios utilizada por el sistema operativo. En este caso, la dirección es 0x187000L.

KDBG: 0xf800028430a0L: La dirección base del bloque del depurador del kernel. Este es un importante elemento en la memoria del kernel y es utilizado para el análisis del kernel.

Number of Processors: 1: Indica que el sistema tiene un solo procesador.

Image Type (Service Pack): 1: Muestra que la imagen del sistema operativo está utilizando un Service Pack. El valor 1 podría indicar un Service Pack instalado.

KPCR for CPU 0: 0xfffff80002844d00L: La dirección base de la región de control del procesador del kernel para el CPU 0.

KUSER_SHARED_DATA: 0xfffff78000000000L: La dirección base de la estructura KUSER_SHARED_DATA. Esta estructura contiene información compartida entre el kernel y los procesos de usuario.

Image date and time: 2023-12-11 19:19:19 UTC+0000: La fecha y hora de creación de la imagen del sistema operativo en formato UTC.

```
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$ python2 vol.py -f ~/Deskt
op/IntelegenciaSeguridad/wannacry1.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win200
8R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7S
P1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/jmxnzo/Desktop/Intelege
nciaSeguridad/wannacry1.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800028430a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002844d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2023-12-11 19:19:19 UTC+0000
     Image local date and time : 2023-12-11 20:19:19 +0100
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$
```

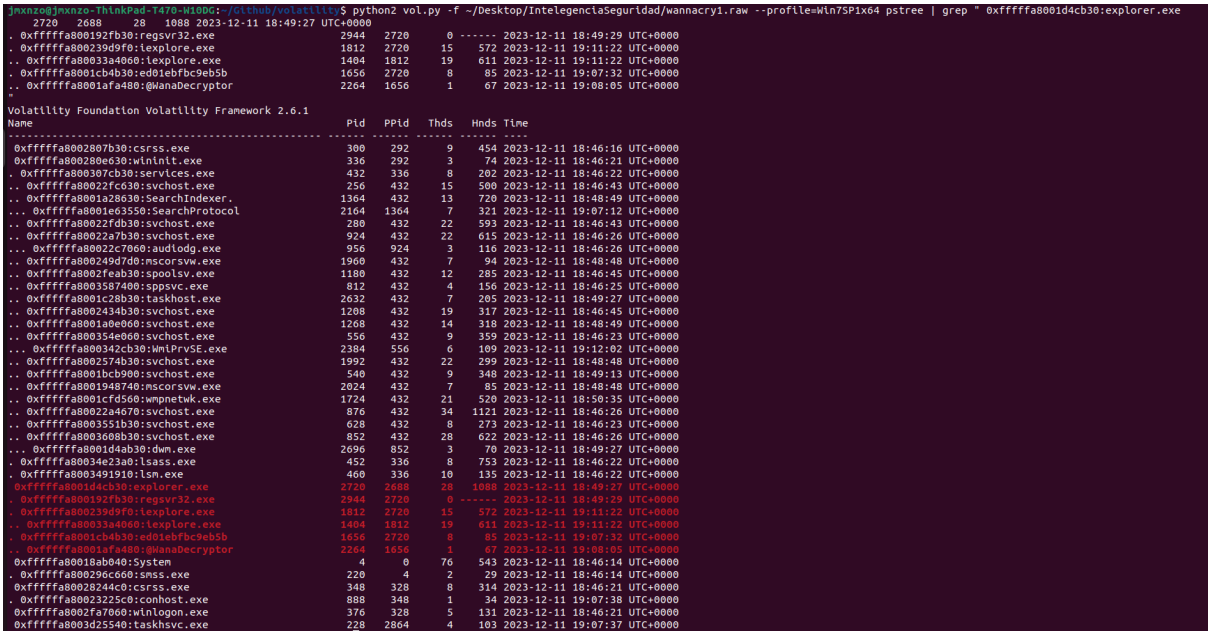
Procesos

Una vez realizado el análisis vamos a pasar a ver las evidencias. Si listamos los procesos con el comando pslist podemos ver como los procesos, 2264 y 1656, parecen extraños y ya vimos como el archivo ed01ebfbc9eb5b (tasksche.exe). Por el otro lado, el proceso @WannacryDecryptor parece desconocido y por el nombre parece que algo tiene que ver con el ataque y como ya vimos cuando probamos el ataque, WannacryDecryptor, era la ventana que nos aparecía informandonos del cifrado de nuestro sistema. Así que tiene una estrecha relación.

```
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$ python2 vol.py -f ~/Desktop/IntelegenciaSeguridad/wannacry1.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa80018ab040 System                    4      0     76      543 ------      0 2023-12-11 18:46:14 UTC+0000
0xfffffa800296c660 smss.exe                220      4      2       29 ------      0 2023-12-11 18:46:14 UTC+0000
0xfffffa8002807b30 csrss.exe               300    292      9      454      0      0 2023-12-11 18:46:16 UTC+0000
0xfffffa800280e630 wininit.exe             336    292      3       74      0      0 2023-12-11 18:46:21 UTC+0000
0xfffffa80028244c0 csrss.exe               348    328      8      314      1      0 2023-12-11 18:46:21 UTC+0000
0xfffffa8002fa7060 winlogon.exe            376    328      5      131      1      0 2023-12-11 18:46:21 UTC+0000
0xfffffa800307cb30 services.exe            432    336      8      202      0      0 2023-12-11 18:46:22 UTC+0000
0xfffffa80034e23a0 lsass.exe               452    336      8      753      0      0 2023-12-11 18:46:22 UTC+0000
0xfffffa8003491910 lsm.exe                 460    336     10      135      0      0 2023-12-11 18:46:22 UTC+0000
0xfffffa800354e060 svchost.exe             556    432      9      359      0      0 2023-12-11 18:46:23 UTC+0000
0xfffffa8003551b30 svchost.exe             628    432      8      273      0      0 2023-12-11 18:46:23 UTC+0000
0xfffffa8003587400 sppsvc.exe              812    432      4      156      0      0 2023-12-11 18:46:25 UTC+0000
0xfffffa8003608b30 svchost.exe             852    432     28      622      0      0 2023-12-11 18:46:26 UTC+0000
0xfffffa80022a4670 svchost.exe             876    432     34     1121      0      0 2023-12-11 18:46:26 UTC+0000
0xfffffa80022a7b30 svchost.exe             924    432     22      615      0      0 2023-12-11 18:46:26 UTC+0000
0xfffffa80022c7060 audiodg.exe             956    924      3      116      0      0 2023-12-11 18:46:26 UTC+0000
0xfffffa80022fdb30 svchost.exe             280    432     22      593      0      0 2023-12-11 18:46:43 UTC+0000
0xfffffa80022fc630 svchost.exe             256    432     15      500      0      0 2023-12-11 18:46:43 UTC+0000
0xfffffa8002feab30 spoolsv.exe            1180    432     12      285      0      0 2023-12-11 18:46:45 UTC+0000
0xfffffa8002434b30 svchost.exe            1208    432     19      317      0      0 2023-12-11 18:46:45 UTC+0000
0xfffffa800249d7d0 mscorsvw.exe           1960    432      7       94      0      1 2023-12-11 18:48:48 UTC+0000
0xfffffa8002574b30 svchost.exe            1992    432     22      299      0      0 2023-12-11 18:48:48 UTC+0000
0xfffffa8001948740 mscorsvw.exe           2024    432      7       85      0      0 2023-12-11 18:48:48 UTC+0000
0xfffffa8001a0e060 svchost.exe            1268    432     14      318      0      0 2023-12-11 18:48:49 UTC+0000
0xfffffa8001a28630 SearchIndexer.         1364    432     13      720      0      0 2023-12-11 18:48:49 UTC+0000
0xfffffa8001bcb900 svchost.exe             540    432      9      348      0      0 2023-12-11 18:49:13 UTC+0000
0xfffffa8001c28b30 taskhost.exe           2632    432      7      205      1      0 2023-12-11 18:49:27 UTC+0000
0xfffffa8001d4ab30 dwm.exe                2696    852      3       70      1      0 2023-12-11 18:49:27 UTC+0000
0xfffffa8001d4cb30 explorer.exe           2720   2688     28     1088      1      0 2023-12-11 18:49:27 UTC+0000
0xfffffa800192fb30 regsvr32.exe           2944   2720      0 --------      1      0 2023-12-11 18:49:29 UTC+0000   2023-12-11 18:49:30 UTC+0000
0xfffffa8001cfd560 wmpnetwk.exe           1724    432     21      520      0      0 2023-12-11 18:50:35 UTC+0000
0xfffffa8001e63550 SearchProtocol         2164   1364      7      321      0      0 2023-12-11 19:07:12 UTC+0000
0xfffffa8001cb4b30 ed01ebfbc9eb5b         1656   2720      8       85      1      1 2023-12-11 19:07:32 UTC+0000
0xfffffa8003d25540 taskhsvc.exe            228   2864      4      103      1      1 2023-12-11 19:07:37 UTC+0000
0xfffffa80023225c0 conhost.exe             888    348      1       34      1      0 2023-12-11 19:07:38 UTC+0000
0xfffffa8001afa480 @WanaDecryptor         2264   1656      1       67      1      1 2023-12-11 19:08:05 UTC+0000
0xfffffa800239d9f0 iexplore.exe           1812   2720     15      572      1      1 2023-12-11 19:11:22 UTC+0000
0xfffffa80033a4060 iexplore.exe           1404   1812     19      611      1      1 2023-12-11 19:11:22 UTC+0000
0xfffffa800342cb30 WmiPrvSE.exe           2384    556      6      109      0      0 2023-12-11 19:12:02 UTC+0000
```

Si usamos ahora el comando pstree podemos visualizar la jerarquía de los procesos capturados en el volcado de memoria. En este contexto, notamos que el proceso previamente destacado, llamado @WanaDecryptor, es en realidad procesos secundarios de otro proceso identificado como "ed01ebfbc9eb5b".

La denominación de este proceso sugiere fuertemente la presencia del ransomware WannaCry. En este escenario, WannaCry establecía comunicación con su servidor de comando y control a través de la red Tor. El ransomware también distribuía, junto con su carga maliciosa, un servidor de Tor local que era renombrado y ejecutado como "taskhsvc.exe". Este comportamiento es característico de WannaCry y su estrategia de ocultación a través de la red Tor.



Ahora usaremos otra herramienta para seguir recolectando evidencias, esta vez correremos el psscan que nos lista todos los procesos corriendo con sus tiempos de creación. Como podemos ver en la siguiente captura nos aparecen muchos subprocesos ocultos que antes no nos aparecían con el comando pslist. Muchos de ellos, son subprocesos de nuestro archivo sospechoso tasksche.exe, como por ejemplo, taskse.exe o taskdl.exe.

```
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$ python2 vol.py -f ~/Desktop/IntelegenciaSeguridad/wannacry1.raw --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB              Time created                   Time exited
------------------ ---------------- ------ ------ ---------------- ------------------------------ ------------------------------
0x000000002207c42d0 dllhost.exe        2572    556 0x0000000013be6000 2023-12-11 19:07:36 UTC+0000   2023-12-11 19:07:41 UTC+0000
0x0000000002327ab30 @WanaDecryptor     2656   1656 0x0000000000913000 2023-12-11 19:13:05 UTC+0000   2023-12-11 19:13:05 UTC+0000
0x000000002328d540 taskhsvc.exe         228   2864 0x00000000240ed000 2023-12-11 19:07:37 UTC+0000
0x000000007e008b30 svchost.exe          852    432 0x000000000b0c9000 2023-12-11 18:46:26 UTC+0000
0x000000007e22cb30 WmiPrvSE.exe        2384    556 0x000000005f630000 2023-12-11 19:12:02 UTC+0000
0x000000007e291910 lsm.exe              460    336 0x0000000013419000 2023-12-11 18:46:22 UTC+0000
0x000000007e2e23a0 lsass.exe            452    336 0x0000000013412000 2023-12-11 18:46:22 UTC+0000
0x000000007e34e060 svchost.exe          556    432 0x000000000010ad0000 2023-12-11 18:46:23 UTC+0000
0x000000007e351b30 svchost.exe          628    432 0x000000000fa2e000 2023-12-11 18:46:23 UTC+0000
0x000000007e387400 sppsvc.exe           812    432 0x000000000b8fb000 2023-12-11 18:46:25 UTC+0000
0x000000007e5a4060 iexplore.exe        1404   1812 0x0000000053c64000 2023-12-11 19:11:22 UTC+0000
0x000000007e67cb30 services.exe         432    336 0x000000001490d000 2023-12-11 18:46:22 UTC+0000
0x000000007e74fb30 TrustedInstall      2064    432 0x0000000001050000 2023-12-11 19:03:08 UTC+0000   2023-12-11 19:13:10 UTC+0000
0x000000007e9a7060 winlogon.exe         376    328 0x0000000017188000 2023-12-11 18:46:21 UTC+0000
0x000000007e9eab30 spoolsv.exe         1180    432 0x0000000075dee000 2023-12-11 18:46:45 UTC+0000
0x000000007ee07b30 csrss.exe            300    292 0x0000000021cbb000 2023-12-11 18:46:16 UTC+0000
0x000000007ee0e630 wininit.exe          336    292 0x000000006de81000 2023-12-11 18:46:21 UTC+0000
0x000000007ee244c0 csrss.exe            348    328 0x000000006dec2000 2023-12-11 18:46:21 UTC+0000
0x000000007ef6c660 smss.exe             220      4 0x000000002ae83000 2023-12-11 18:46:14 UTC+0000
0x000000007f234b30 svchost.exe         1208    432 0x0000000075aeb000 2023-12-11 18:46:45 UTC+0000
0x000000007f29d7d0 mscorsvw.exe        1960    432 0x000000006a8a3000 2023-12-11 18:48:48 UTC+0000
0x000000007f374b30 svchost.exe         1992    432 0x00000000676ef000 2023-12-11 18:48:48 UTC+0000
0x000000007f483b30 reg.exe             1716   2816 0x0000000024b63000 2023-12-11 19:08:05 UTC+0000   2023-12-11 19:08:05 UTC+0000
0x000000007f4a4670 svchost.exe          876    432 0x000000000ab0e000 2023-12-11 18:46:26 UTC+0000
0x000000007f4a7b30 svchost.exe          924    432 0x000000000ac98000 2023-12-11 18:46:26 UTC+0000
0x000000007f4c7060 audiodg.exe          956    924 0x000000000abc5000 2023-12-11 18:46:26 UTC+0000
0x000000007f4fc630 svchost.exe          256    432 0x0000000005df5000 2023-12-11 18:46:43 UTC+0000
0x000000007f4fdb30 svchost.exe          280    432 0x000000000666e000 2023-12-11 18:46:43 UTC+0000
0x000000007f5225c0 conhost.exe          888    348 0x000000000530ce000 2023-12-11 19:07:38 UTC+0000
0x000000007f59d9f0 iexplore.exe        1812   2720 0x0000000038da4000 2023-12-11 19:11:22 UTC+0000
0x000000007f5afb30 taskdl.exe          1300   1656 0x0000000077aa9000 2023-12-11 19:14:05 UTC+0000   2023-12-11 19:14:05 UTC+0000
0x000000007f863550 SearchProtocol      2164   1364 0x000000003d72b000 2023-12-11 19:07:12 UTC+0000
0x000000007fa28b30 taskhost.exe        2632    432 0x000000003ca85000 2023-12-11 18:49:27 UTC+0000
0x000000007fab4b30 ed01ebfbc9eb5b      1656   2720 0x0000000000149e000 2023-12-11 19:07:32 UTC+0000
0x000000007fafd560 wmpnetwk.exe        1724    432 0x000000004a075000 2023-12-11 18:50:35 UTC+0000
0x000000007fb4ab30 dwm.exe             2696    852 0x000000003b013000 2023-12-11 18:49:27 UTC+0000
0x000000007fb4cb30 explorer.exe        2720   2688 0x000000003b6d8000 2023-12-11 18:49:27 UTC+0000
0x000000007fbe0060 taskdl.exe          1088   1656 0x0000000052295000 2023-12-11 19:13:05 UTC+0000   2023-12-11 19:13:05 UTC+0000
0x000000007fc0e060 svchost.exe         1268    432 0x0000000006707d000 2023-12-11 18:48:49 UTC+0000
0x000000007fc28630 SearchIndexer.      1364    432 0x000000000665c3000 2023-12-11 18:48:49 UTC+0000
0x000000007fc9eb30 VSSVC.exe            744    432 0x0000000028467000 2023-12-11 19:07:57 UTC+0000   2023-12-11 19:10:58 UTC+0000
0x000000007fcfa480 @WanaDecryptor      2264   1656 0x000000003c814000 2023-12-11 19:08:05 UTC+0000
0x000000007fdcb900 svchost.exe          540    432 0x00000000482e8000 2023-12-11 18:49:13 UTC+0000
0x000000007fe87740 mscorsvw.exe        2024    432 0x0000000672f6000 2023-12-11 18:48:48 UTC+0000
0x000000007feeeb30 regsvr32.exe        2944   2720 0x000000003870d000 2023-12-11 18:49:29 UTC+0000   2023-12-11 18:49:30 UTC+0000
0x000000007ff6a040 System                 4      0 0x0000000000187000 2023-12-11 18:46:14 UTC+0000
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$
```

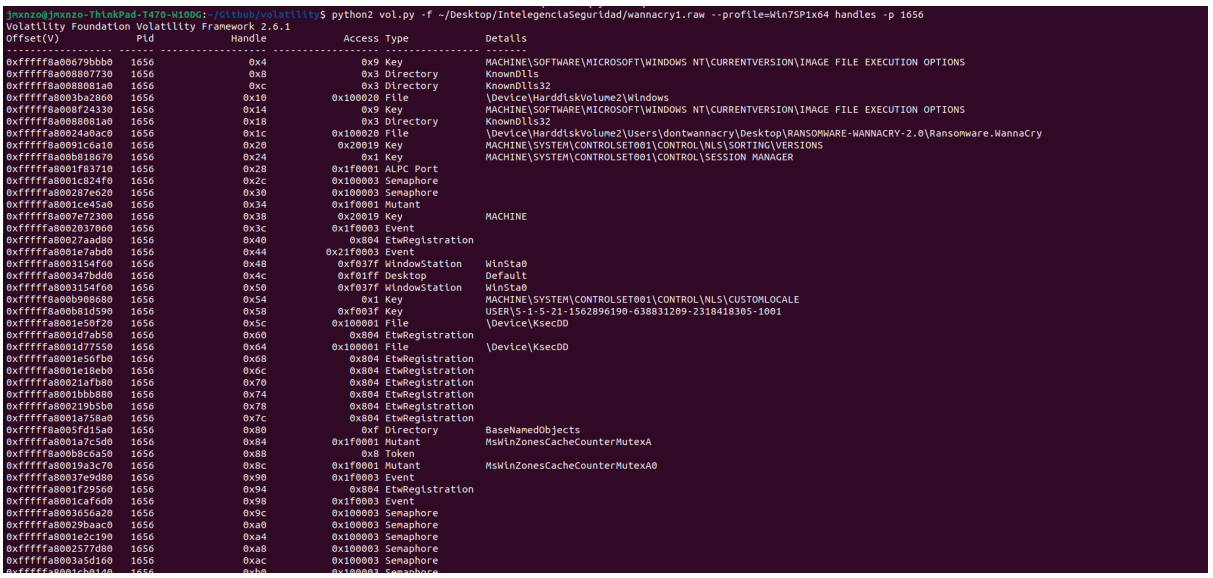
Para asegurarnos de que son subprocesos y que tienen relación entre sí vamos a ordenarlos por tiempo de creación para poder entender mejor cómo se creó todo. Para ello, volcamos el escaneo con psscan en un archivo llamado “createdProcesses” con el cuál trabajaremos con los procesos de manera más clara.

```
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$ python2 vol.py -f ~/Desktop/IntelegenciaSeguridad/wannacry1.raw --profile=Win7SP1x64 psscan > cr
eatedProcesses
Volatility Foundation Volatility Framework 2.6.1
```

Ahora con una regex podemos ordenar los procesos según la sexta columna con el mandato “sort -k 6”, esta sexta columna es el tiempo de creación y por otro lado, con el mandato “tail -n 14” imprimimos las últimas 14 líneas que serán los primeros procesos creados. Como podemos ver en la siguiente captura el proceso ed01ebfbc9eb5b (tasksche.exe) fue el primero en ser creado y de él aparecen los siguientes procesos que conforman el ataque. Entre ellos el @WannacryDecryptor que por el nombre puede ser el proceso que cifra todo el ordenador.

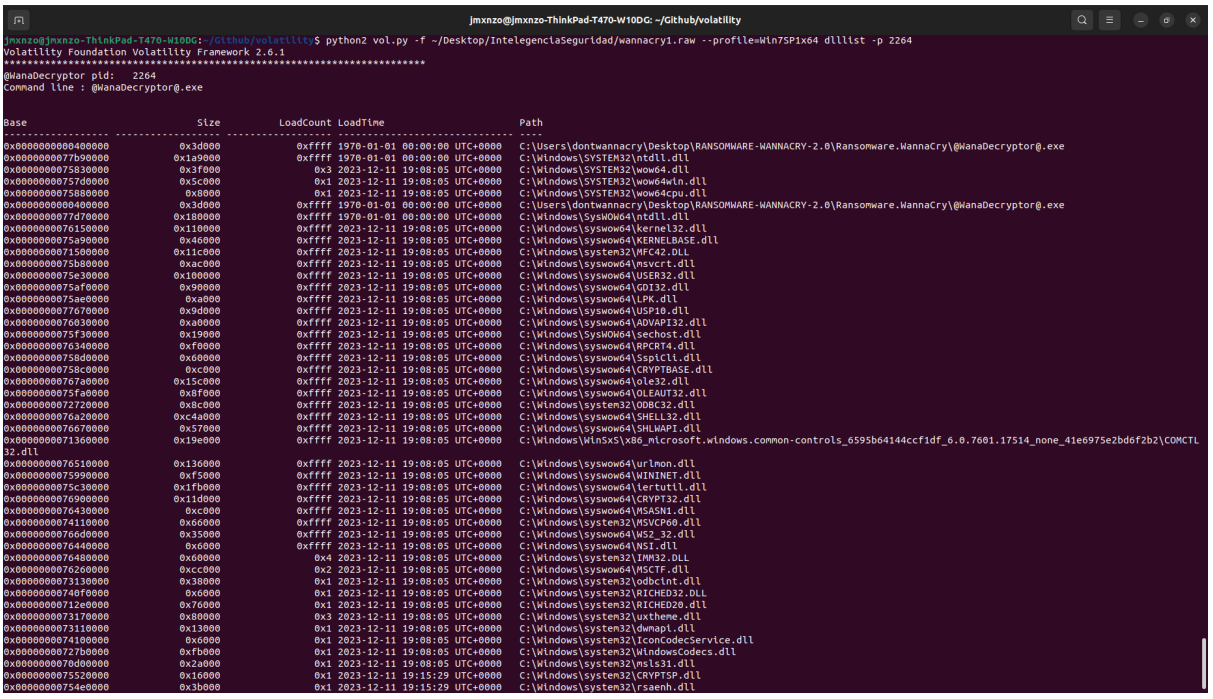
```
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$ cat createdProcesses | sort -k 6 | tail -n 14
0x000000007fab4b30 ed01ebfbc9eb5b      1656   2720 0x0000000000149e000 2023-12-11 19:07:32 UTC+0000
0x000000002207c42d0 dllhost.exe        2572    556 0x0000000013be6000 2023-12-11 19:07:36 UTC+0000   2023-12-11 19:07:41 UTC+0000
0x000000002328d540 taskhsvc.exe         228   2864 0x00000000240ed000 2023-12-11 19:07:37 UTC+0000
0x000000007f5225c0 conhost.exe          888    348 0x000000000530ce000 2023-12-11 19:07:38 UTC+0000
0x000000007fc9eb30 VSSVC.exe            744    432 0x0000000028467000 2023-12-11 19:07:57 UTC+0000   2023-12-11 19:10:58 UTC+0000
0x000000007fcfa480 @WanaDecryptor      2264   1656 0x000000003c814000 2023-12-11 19:08:05 UTC+0000
0x000000007f483b30 reg.exe             1716   2816 0x0000000024b63000 2023-12-11 19:08:05 UTC+0000   2023-12-11 19:08:05 UTC+0000
0x000000007e5a4060 iexplore.exe        1404   1812 0x0000000053c64000 2023-12-11 19:11:22 UTC+0000
0x000000007f59d9f0 iexplore.exe        1812   2720 0x0000000038da4000 2023-12-11 19:11:22 UTC+0000
0x000000007e22cb30 WmiPrvSE.exe        2384    556 0x000000005f630000 2023-12-11 19:12:02 UTC+0000
0x0000000002327ab30 @WanaDecryptor     2656   1656 0x0000000000913000 2023-12-11 19:13:05 UTC+0000   2023-12-11 19:13:05 UTC+0000
0x000000007fbe0060 taskdl.exe          1088   1656 0x0000000052295000 2023-12-11 19:13:05 UTC+0000   2023-12-11 19:13:05 UTC+0000
0x000000007f5afb30 taskdl.exe          1300   1656 0x0000000077aa9000 2023-12-11 19:14:05 UTC+0000   2023-12-11 19:14:05 UTC+0000
Offset(P)          Name                PID   PPID PDB              Time created                   Time exited
```

Ahora para seguir recolectando información podemos usar el comando “dlllis” para obtener información sobre las bibliotecas dinámicas enlazadas (DLL) cargadas del proceso 1656, es decir, ed01ebfbc9eb5b (tasksche.exe).



```
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$ python2 vol.py -f ~/Desktop/IntelegenciaSeguridad/wannacry1.raw --profile=Win7SP1x64 handles -p 1656
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Pid             Handle             Access Type             Details
------------------ ------ ---------------- ---------------- ---------------- -------
0xfffffa80679bbb0   1656              0x4                0x9 Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
0xfffffa8008807730  1656              0x8                0x3 Directory       KnownDlls
0xfffffa8008881a0   1656              0xc                0x3 Directory       KnownDlls32
0xfffffa8003ba2860  1656             0x10           0x100020 File            \Device\HarddiskVolume2\Windows
0xfffffa808f24330   1656             0x14                0x9 Key             MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS
0xfffffa80088081a0  1656             0x18                0x3 Directory       KnownDlls32
0xfffffa80024a0ac0  1656             0x1c           0x100020 File            \Device\HarddiskVolume2\Users\dontwannacry\Desktop\RANSOMWARE-WANNACRY-2.0\Ransomware.WannaCry
0xfffffa8009 1c6a10 1656             0x20            0x20019 Key             MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS
0xfffffa800b810670  1656             0x24                0x1 Key             MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER
0xfffffa8001f83710  1656             0x28           0x1f0001 ALPC Port
0xfffffa8001c824f0  1656             0x2c           0x100003 Semaphore
0xfffffa80287e620   1656             0x30           0x100003 Semaphore
0xfffffa8001ce45a0  1656             0x34           0x1f0001 Mutant
0xfffffa807e72300   1656             0x38            0x20019 Key             MACHINE
0xfffffa8002037060  1656             0x3c           0x1f0003 Event
0xfffffa80027aad80  1656             0x40                0x804 EtwRegistration
0xfffffa8001e7abd0  1656             0x44           0x21f0003 Event
0xfffffa8003154f60  1656             0x48            0xf037f WindowStation    WinSta0
0xfffffa800347bdd0  1656             0x4c            0xf01ff Desktop          Default
0xfffffa8003154f60  1656             0x50            0xf037f WindowStation    WinSta0
0xfffffa800b908680  1656             0x54                0x1 Key             MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE
0xfffffa800b81d590  1656             0x58            0xf003f Key             USER\S-1-5-21-1562896190-638831209-2318418305-1001
0xfffffa8001e50f20  1656             0x5c           0x100001 File            \Device\KsecDD
0xfffffa8001d7ab50  1656             0x60                0x804 EtwRegistration
0xfffffa8001d77550  1656             0x64           0x100001 File            \Device\KsecDD
0xfffffa8001e56fb0  1656             0x68                0x804 EtwRegistration
0xfffffa8001e18eb0  1656             0x6c                0x804 EtwRegistration
0xfffffa80021afb80  1656             0x70                0x804 EtwRegistration
0xfffffa8001bbb880  1656             0x74                0x804 EtwRegistration
0xfffffa800219b5b0  1656             0x78                0x804 EtwRegistration
0xfffffa8001a758a0  1656             0x7c                0x804 EtwRegistration
0xfffffa8005fd15a0  1656             0x80                0xf Directory       BaseNamedObjects
0xfffffa8001a7c5d0  1656             0x84           0x1f0001 Mutant          MsWinZonesCacheCounterMutexA
0xfffffa800b8c6a50  1656             0x88                0x8 Token
0xfffffa800193c70   1656             0x8c           0x1f0001 Mutant          MsWinZonesCacheCounterMutexA0
0xfffffa80037e9d80  1656             0x90           0x1f0003 Event
0xfffffa8001f29560  1656             0x94                0x804 EtwRegistration
0xfffffa8001caf6d0  1656             0x98           0x1f0003 Event
0xfffffa8003656a20  1656             0x9c           0x100003 Semaphore
0xfffffa80029baac0  1656             0xa0           0x100003 Semaphore
0xfffffa8001e2c190  1656             0xa4           0x100003 Semaphore
0xfffffa8002577d80  1656             0xa8           0x100003 Semaphore
0xfffffa8003a5d160  1656             0xac           0x100003 Semaphore
```

Además podemos hacer lo mismo con el proceso 2264, @WannaDecryptor@.exe como podemos ver en la siguiente captura.



```
jmxnzo@jmxnzo-ThinkPad-T470-W10DG: ~/Github/volatility
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$ python2 vol.py -f ~/Desktop/IntelegenciaSeguridad/wannacry1.raw --profile=Win7SP1x64 dlllist -p 2264
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
@WanaDecryptor pid:   2264
Command line : @WanaDecryptor@.exe

Base                             Size          LoadCount LoadTime                       Path
-------------------- ---------------- ---------- ------------------------------ ----
0x0000000000400000           0x3d000             0xffff 1970-01-01 00:00:00 UTC+0000   C:\Users\dontwannacry\Desktop\RANSOMWARE-WANNACRY-2.0\Ransomware.WannaCry\@WanaDecryptor@.exe
0x0000000077b90000           0x1a9000            0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x0000000075830000            0x3f000               0x3 2023-12-11 19:08:05 UTC+0000   C:\Windows\SYSTEM32\wow64.dll
0x000000007 57d0000           0x5c000               0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\SYSTEM32\wow64win.dll
0x0000000075880000            0x8000               0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\SYSTEM32\wow64cpu.dll
0x0000000000400000           0x3d000             0xffff 1970-01-01 00:00:00 UTC+0000   C:\Users\dontwannacry\Desktop\RANSOMWARE-WANNACRY-2.0\Ransomware.WannaCry\@WanaDecryptor@.exe
0x0000000077d70000          0x180000            0xffff 1970-01-01 00:00:00 UTC+0000   C:\Windows\SysWOW64\ntdll.dll
0x0000000076150000          0x110000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\kernel32.dll
0x0000000075a90000           0x46000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\KERNELBASE.dll
0x0000000071500000          0x11c000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\MFC42.DLL
0x0000000075b80000           0xac000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\msvcrt.dll
0x0000000075e30000          0x100000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\USER32.dll
0x0000000075af0000           0x90000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\GDI32.dll
0x0000000075ae0000            0xa000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\LPK.dll
0x0000000077670000           0x9d000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\USP10.dll
0x0000000076030000           0xa0000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\ADVAPI32.dll
0x0000000075f30000           0x19000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\SysWOW64\sechost.dll
0x0000000076340000           0xf0000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\RPCRT4.dll
0x000000007 58d0000          0x60000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\SspiCli.dll
0x000000007 58c0000           0xc000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\CRYPTBASE.dll
0x0000000076 7a0000          0x15c000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\ole32.dll
0x0000000075fa0000           0x8f000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\OLEAUT32.dll
0x0000000072720000           0x8c000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\ODBC32.dll
0x0000000076a20000           0xc4a000           0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\SHELL32.dll
0x0000000076770000           0x57000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\SHLWAPI.dll
0x0000000071360000          0x19e000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\COMCTL
32.dll
0x0000000076510000          0x136000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\urlmon.dll
0x0000000075990000           0xf5000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\WININET.dll
0x0000000075c30000          0x1fb000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\iertutil.dll
0x0000000076900000          0x11d000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\CRYPT32.dll
0x0000000076430000           0xc000             0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\MSASN1.dll
0x0000000074110000           0x66000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\MSVCP60.dll
0x000000007 66d0000          0x35000            0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\WS2_32.dll
0x0000000076440000           0x6000             0xffff 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\NSI.dll
0x0000000076480000           0x60000               0x4 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\IMM32.DLL
0x0000000076260000           0xcc000               0x2 2023-12-11 19:08:05 UTC+0000   C:\Windows\syswow64\MSCTF.dll
0x0000000073130000           0x38000               0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\odbcint.dll
0x0000000740f0000             0x6000              0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\RICHED32.DLL
0x0000000712e0000            0x76000              0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\RICHED20.dll
0x0000000073170000           0x80000              0x3 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\uxtheme.dll
0x0000000073110000           0x13000              0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\dwmapi.dll
0x0000000074100000            0x6000              0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\IconCodecService.dll
0x000000007 27b0000           0xfb000             0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\WindowsCodecs.dll
0x0000000070d00000            0x2a000             0x1 2023-12-11 19:08:05 UTC+0000   C:\Windows\system32\msls31.dll
0x0000000075520000           0x16000              0x1 2023-12-11 19:15:29 UTC+0000   C:\Windows\system32\CRYPTSP.dll
0x00000000754e0000           0x3b000              0x1 2023-12-11 19:15:29 UTC+0000   C:\Windows\system32\rsaenh.dll
```

Según los resultados anteriores, está claro que estos son maliciosos por naturaleza y están utilizando APIs de Windows como Secur32.dll para cifrar Ws2_32 y crear sockets, realizar comunicaciones de red de alto nivel (WININET.DLL), consultar el registro (ADVAPI32.DLL), cifrar (SECURE32.DLL) e interactuar con navegadores (URLMON.DLL) como Internet Explorer, entre otras acciones.

Secur32.dll: Se utiliza para funciones relacionadas con la seguridad en Windows. En el caso de WannaCry, puede haber sido utilizado para cifrar ciertas partes del código o para manipular aspectos de la seguridad del sistema.

Ws2_32.dll: Esta biblioteca se utiliza para la creación y gestión de sockets, que son fundamentales para las comunicaciones en red. WannaCry puede haber utilizado esta DLL para establecer conexiones de red, posiblemente como parte de su capacidad de propagación.

WININET.DLL: Es una biblioteca que proporciona funciones para realizar operaciones de red de alto nivel. WannaCry pudo haber utilizado esta DLL para la comunicación avanzada a través de la red, facilitando su propagación y la ejecución de acciones maliciosas.

ADVAPI32.DLL: Esta DLL proporciona funciones para interactuar con el Registro de Windows. WannaCry puede haber utilizado estas funciones para realizar consultas en el registro del sistema, posiblemente como parte de su estrategia de persistencia o para obtener información específica del sistema.

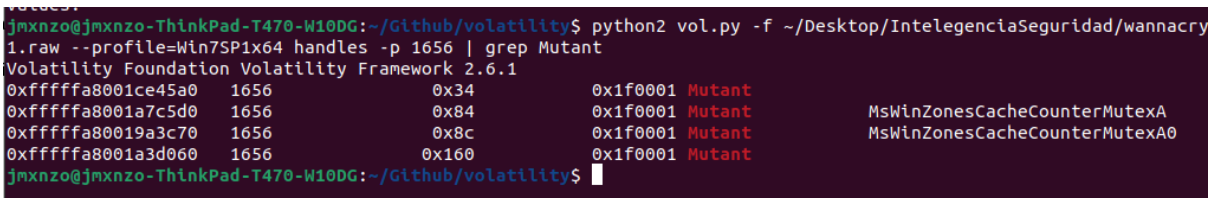
URLMON.DLL: Utilizada para interactuar con URL y manipular datos relacionados con Internet. En el caso de WannaCry, podría haber sido utilizada para interactuar con navegadores web, como Internet Explorer, con el objetivo de propagarse o realizar acciones adicionales.

El análisis de las bibliotecas enlazadas en el contexto de WannaCry revela que el malware aprovecha diversas funciones del sistema operativo Windows para cifrar, comunicarse a través de la red, manipular el registro y posiblemente interactuar con navegadores.

Análisis de Identificadores de Archivos

Por otro lado, encontramos otros objetos de interés relacionados con el ataque cuando analizamos los manejadores de archivos asociados a los ficheros, en concreto a los de tipo mutex, podremos ver como existe un objeto de tipo mutex con PID 1656.

Volatility permite a los analistas visualizar los identificadores (handles) en un proceso. Esto se puede hacer en todos los objetos ejecutables seguros, como eventos, tuberías con nombre, claves de registro y mutexes. Al observar los identificadores, se puede ver el acceso y su tipo.



Lo primero antes de pasar a analizar la captura es entender que es un “mutex”, un mutex, que es una abreviatura de "mutual exclusion" (exclusión mutua), es un concepto

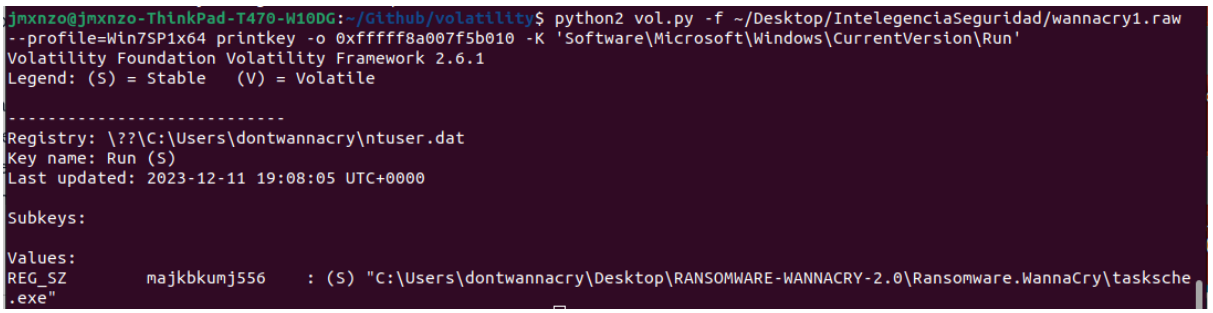
fundamental en la programación concurrente y la gestión de recursos compartidos en sistemas informáticos. Se utiliza para evitar que dos o más procesos o hilos accedan simultáneamente a un recurso compartido, lo que podría llevar a condiciones de carrera y resultados impredecibles.

Este mutex es generado por la muestra de WannaCry con el propósito de evitar la reinfección de la máquina. En el instante inicial de la infección, se crea este mutex, de manera que las ejecuciones posteriores del malware no infectarán la máquina al detectar la existencia previa de este mutex. Este método de evitar reinfecciones es común en el malware y funciona como un mecanismo de defensa para prevenir infecciones en máquinas que aún no han sido comprometidas.

Persistencia

También, es importante recordar que una fase crucial en el código malicioso es establecer la persistencia en los sistemas infectados para asegurar que continúen con sus actividades dañinas incluso después de reiniciar el sistema.

Podemos extraer los valores clave que se utilizan para lograr persistencia utilizando el complemento printkey. Buscamos a través de las claves Run, Runonce, WinlogonKeys, BootExecuteKey, carpetas de inicio y la clave de servicios. En este caso, la clave Run se muestra a continuación:



Para identificar las claves de registro accesibles en el volcado de memoria, podemos emplear el comando PrintKey. Este enfoque nos permite localizar las claves de registro relevantes y comprender cómo el malware busca establecer una presencia persistente en el sistema afectado.

En este caso, ya teníamos conocimiento de la ruta a la clave debido a análisis previos disponibles en Internet para WannaCry. No obstante, en nuestro análisis, es crucial presentar la información explorando todo el registro en busca de nuestro proceso WannaCry, determinando el momento exacto en el que el virus se activó.

Para iniciar nuestro análisis, utilizamos el comando "hivelist" para obtener una descripción general de nuestro registro de claves. La captura inicial de PrintKey nos proporciona una visión integral de las claves de registro accesibles en el volcado de memoria.

Es fundamental destacar que esta metodología nos permite entender cómo el malware opera a nivel de registro, identificar puntos de persistencia y rastrear la actividad del virus en el sistema. Este enfoque analítico nos ofrece una visión más profunda de la amenaza y facilita la implementación de medidas de seguridad efectivas para mitigar el impacto de futuros incidentes similares.

```
jmxnzo@jmxnzo-ThinkPad-T470-W10DG:~/Github/volatility$ python2 vol.py -f ~/Desktop/IntelegenciaSeguridad/wannacry
1.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a00000d0b0 0x000000002d73f0b0 [no name]
0xfffff8a000024010 0x000000002d664010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a00004e010 0x000000002d5ce010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a000ed7410 0x0000000073ec0410 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a0017af010 0x000000002a094010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a003d14410 0x00000000287f1410 \SystemRoot\System32\Config\DEFAULT
0xfffff8a006968010 0x0000000012bcc010 \SystemRoot\System32\Config\SECURITY
0xfffff8a007f5b010 0x000000003f4ff010 \??\C:\Users\dontwannacry\ntuser.dat
0xfffff8a0080ea010 0x000000003c0c8010 \??\C:\Users\dontwannacry\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a008812010 0x0000000011637010 \SystemRoot\System32\Config\SAM
0xfffff8a0088b7010 0x000000000f8d9010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a00905c010 0x000000000adbc010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00bb1b010 0x0000000073e74010 \??\C:\System Volume Information\Syscache.hve
```

En resumen, las printkeys imprimen las claves del registro y estas consisten en una base de datos central que contiene información y configuraciones para el sistema operativo y las aplicaciones instaladas. Los autores de malware pueden utilizar el registro para diversos fines al intentar ocultar o potenciar sus actividades maliciosas. Uno de estos fines sería la persistencia, ya que el malware puede establecer mecanismos persistentes en el registro para asegurarse de que permanezca activo después de un reinicio del sistema. Esto podría hacerse mediante la creación de claves del Registro que apunten a los componentes del malware.