**Sesión 3**

**Laboratorio con WannaCry**

Gabriel Martin Blázquez

Grupo 1 Francisco Pinto Santos

Contenido

[Introducción 2](#_Toc33972276)

[Protocolo de actuación ante un ciberataque masivo 2](#_Toc33972277)

[Análisis forense del fichero binario del ransomware WannaCry 3](#_Toc33972278)

[Análisis forense de RAM de equipo afectado por ransomware WannaCry 5](#_Toc33972279)

[Fuentes 10](#_Toc33972280)

## Introducción

Esta sesión consto de dos partes: una primera en la que se expuso el protocolo de actuación seguido por Deloitte ante un ciberataque a gran escala, tras lo cual se procedió a la segunda parte, la cual consistió en cómo realizar una análisis forense sobre un volcado de memoria principal de un equipo afectado por el ransomware "WannaCry".

## Protocolo de actuación ante un ciberataque masivo

En esta primera parte, vimos cómo se actúa ante un ciberataque masivo que afecta a todos o una gran cantidad de los equipos de una empresa.

Para comenzar, como es un proceso que debe tener validez legal, tiene que haber un notario presente y se tienen que tomar actas de todo el proceso, para lo cual en Deloitte tienen una plataforma llamada "DoyFe" que genera las actas automáticamente.

Tras ello, se procede a tomar una muestra de los equipos afectados en dos fases:

* En una primera fase, se toman muestras de la memoria volátil de los equipos afectados que continúen encendidos (RAM, caches, buffers, …).
* En una segunda fase se toman muestras de la memoria secundaria de los equipos afectados, tanto encendidos como apagados.

Dentro de los equipos apagados, se toman muestras de los equipos que se hayan apagado mediante un protocolo ordenado y los apagados de una manera más brusca (como puede ser tirando del cable).

Una vez hecho esto, se toma una copia de seguridad de cada una de las evidencias tomadas y para trabajar sobre ellas se hacen copias de estas para poder adulterarlas de forma segura sin alterar las evidencias originales ni las copias de las evidencias.

Por último, se nos enseño como se hace el proceso de copia, con maquinas copiadoras especializadas en realizar distintas copias de distintos dispositivos (memoria magnética, semiconductora, …) de una forma muy rápida.

El único problema que tenían estos equipos copiadores es que eran muy caros, delicados y difíciles de conseguir.

Por último, en esta parte, se nos dio el consejo de que, ante un ataque informático, apaguemos nuestros equipos de forma abrupta para facilitar el posterior análisis forense.

## Análisis forense del fichero binario del ransomware WannaCry

Un ransomware es un software de carácter malicioso, que cifra los ficheros de un equipo. Tras ello se le indica al usuario que para descifrarlos y recuperar su información tiene que pagar una cantidad de dinero significativa como chantaje.

En este caso, estuvimos tratando con el malware WannaCray, que fue un ransomware utilizado en 2017 para lanzar un ciberataque a escala global, supuestamente realizado por un agente del gobierno norcoreano.

Muchas empresas se vieron afectadas por este malware, pero en España las principales afectadas fueron unas de las empresas mas grandes a nivel nacional, como son Telefónica, Iberdrola y Gas natural, y algunos organismos de carácter público como el CNI.

En cuanto a la manera de actuar de este malware, se establecía en un host y se distribuía por el protocolo SAMBA, utilizado por los equipos Windows para el intercambio de archivos e información en redes locales, y el cual viene activado por defecto en todos los equipos Windows. Debido a esto, el malware se distribuyó fácilmente por varias redes empresariales y de organismos públicos.

Para neutralizar el ataque a nivel mundial, tras varios días de investigación, se descubrió un killswitch, consistente en un domino que cuando respondiera a una petición GET pararía el ataque. No obstante, hasta que se descubrió causo una gran cantidad de pérdidas económicas, considerándose uno de los ciberataques mas destructivos hasta la fecha actual.

Para realizar análisis forense, utilizamos una imagen del propio malware "WannaCry", y un volcado (o dump) de la memoria volátil (RAM) de un equipo afectado por el ransomware WannaCray, sobre el cual realizamos los siguientes pasos:

Primero analizamos el propio malware, ubicado en el fichero 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.bin, con el comando strings sobre dicho fichero:

strings 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.bin

Tras lo cual procedimos a filtrar los resultados obtenidos con el comando grep:

grep [-n] regex

Nota: con -n obtienes el número de línea en el que se encuentra el match

Concretamente, filtramos por los siguientes campos:

* En primer lugar, al tratarse de un software, realizamos búsqueda por ficheros compilados y scripts con las extensiones .bat, .o, .class, .pyc, … pero no obtuvimos resultados. Tras lo cual probamos con ficheros de enlazado dinámico (.dll) sin obtener resultado.
* Tras el fracaso anterior, y debido a que sabíamos que se desactivaba mediante una petición http al dominio de killswitch, realizamos una búsqueda con grep por http, tras la cual obtuvimos que la URL que actuaba de killswitch es la siguiente:

http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

* Después, debido a que sabíamos que se transmitía mediante el protocolo samba, buscamos por smb que es el principio de las URL/URIs del protocolo SAMBA. Pero a diferencia de antes, no obtuvimos resultado.
* Por último, seguimos las recomendaciones de Carlos buscando por el nombre del malware WNcry@2017 y por attrib y realizamos nuestro primer descubrimiento.

Este consistía en que de las líneas 1800 a 18003 del malware, había un conjunto de comandos, entre ellos 1800:attrib +h ., con el cual se ponían los ficheros en oculto, tras lo cual se procede a cifrarlos.

## Análisis forense de RAM de equipo afectado por ransomware WannaCry

Una vez encontrado en el fichero binario del malware WannaCray donde se realiza el cifrado y ocultación de los ficheros, procedimos a analizar el dump de memoria volátil de un equipo afectado por este malware.

Para proceder, utilizamos la herramienta volatility, programada en Python 2.X, la cual es un framework que nos ofrece un set de herramientas para extraer información de dumps de memoria RAM de una gran cantidad de versiones, distribuciones de sistemas operativos, tanto Linux, como Windows y MacOS.

Lo primero que hicimos, fue obtener información del equipo afectado, como sistema operativo, versión, … para proveer dicha información a volatility, y poder hacer así un análisis más exhaustivo. Esto se realizó mediante el comando:

python ../volatility-master/volatility-master/vol.py -f malware.raw imageinfo > volatility\_imageinfo.txt

tras lo cual, conseguimos saber que el sistema del equipo afectado consistía en un WindowsXP Service pack 3 con una arquitectura de procesador de x86; información que aportamos en el resto de los comandos (con la opción --profile=WinXPSP2x86), para poder realizar un análisis más preciso.

Una vez obtenida la información del host, se procedió a investigar sobre los siguientes elementos:

* Se buscaron "apIhooks" sobre el dump, los cuales consisten en eventos significativos del sistema operativo. En estos obtuvimos que solo había uno que era taskdl, el cual se trata de un evento generado por el propio sistema de Windows para gestionar el administrador de tareas, por lo que no se consideró sospechoso.

python ../volatility-master/volatility-master/vol.py -k apihooks malware.raw

* Tras esto, se procedió a examinar los procesos activos en el momento del volcado de memoria.

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 pslist > pslist.txt

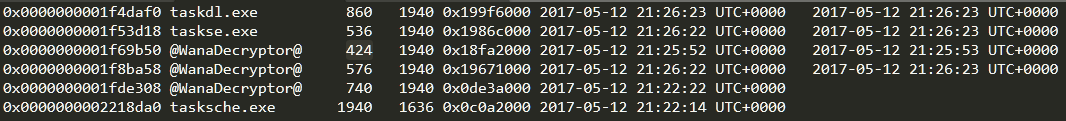
Tras lo cual, vimos unos 20 procesos, entre los cuales se contaban smss.exe, svchost.exe, ctfmon.exe, … y una gran cantidad de servicios del sistema. No obstante, se apreciaba un proceso sospechoso, ya que tenia el nombre del malware a analizar, @WanaDecryptor@. Este proceso estaba identificado por el PID 740 y el PPID 1940.

0x81fde308 @WanaDecryptor@ 740 1940 2 70 0 0 2017-05-12 21:22:22 UTC+0000

* Una vez detectado un proceso sospechoso, procedimos a obtener más información de este. Concretamente a que otros procesos ha afectado, para lo cual utilizamos el siguiente comando:

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 psscan | grep 1940 > salida1940.txt

Del cual obtenemos la siguiente salida:



De la que se pueden obtener dos conclusiones: La primera de ellas es, que WannaCry toma el control del taskdel.exe que se trata del administrador de tareas, y la segunda, debido a los tiempos de ejecución, es que se ejecuta de forma periódica cada 30 segundos aproximadamente.

Esto último, según nos indicó Carlos, es una característica muy común en malware de este tipo, pues una de las primeras cosas que hace, es persistirse, y crear un servicio que ejecute el malware al inicio del sistema y de forma periódica, para hacer aún más daño.

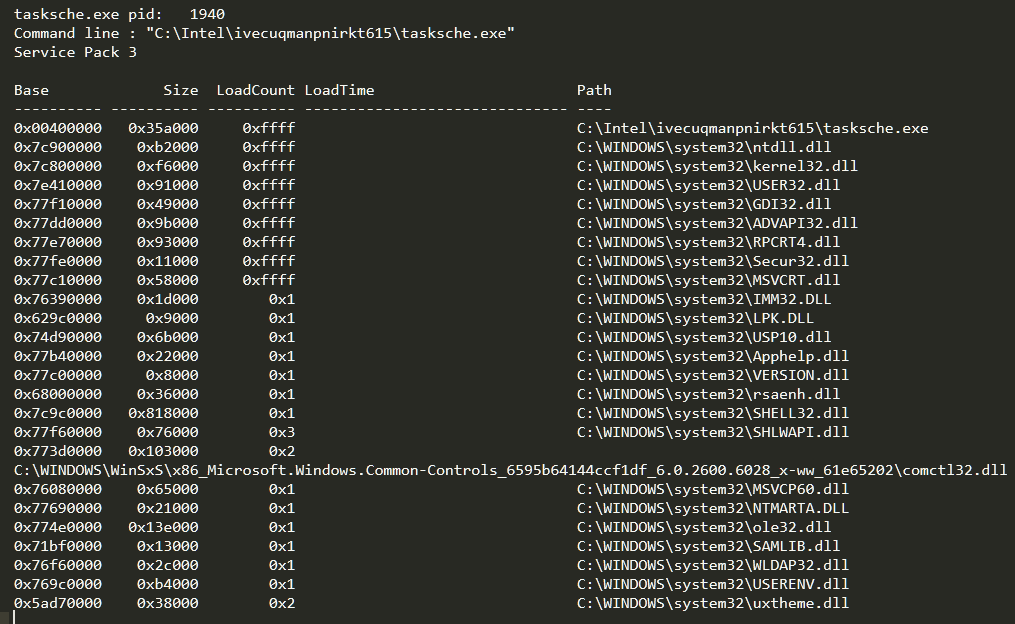
En este caso, WannaCray se aprovecha de la invocación periódica del demonio taskdl, para provocar que también se cree el demonio propio de WannaCry.

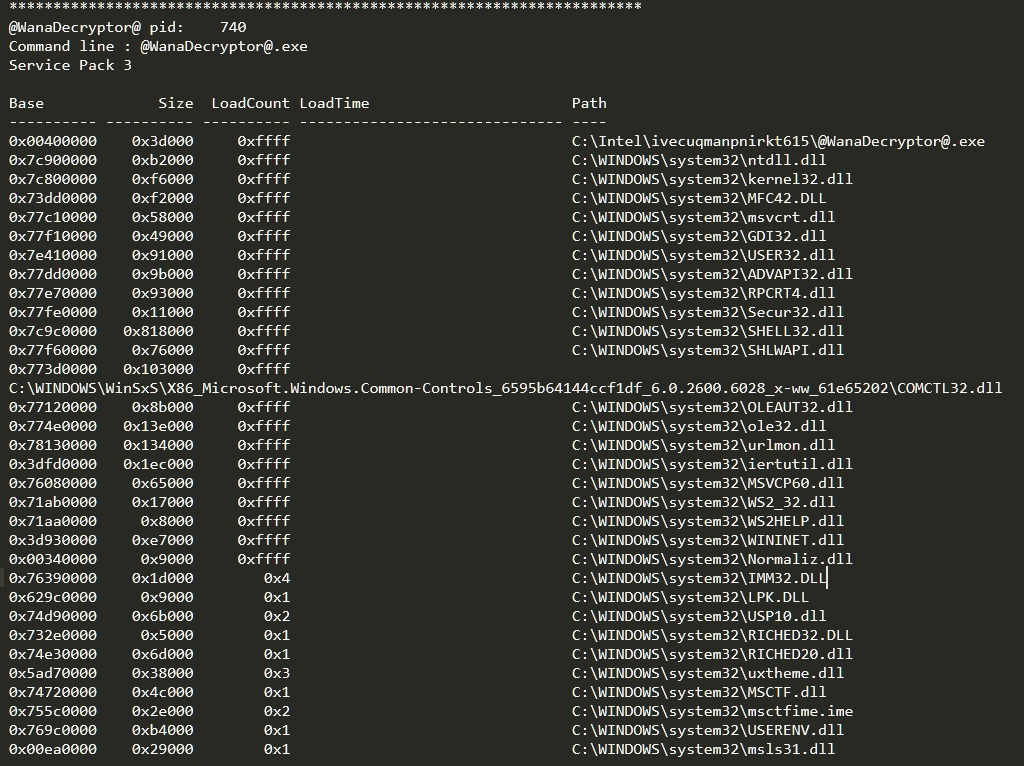
* Una vez conocido esto, intentamos obtener información de que librerías de enlazado dinámico (DLL) utiliza el proceso utilizado por el WannaCry para hacer daño. Para lo cual utilizamos los siguientes comandos:

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 dlllist -p 1940 > dlllist1940.txt

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 dlllist -p 740 > dlllist740.txt

En cuanto a las salidas que se apreciaban de los dos procesos, como se puede ver en las imágenes posteriores, no había ningun DLL que se saliera de lo normal, dado que estaban algunos como ole32.ddll, SMBLIB.dll, USERENV.dll,… que se utilizan por defecto en la mayoría de las aplicaciones de Windows para realizar algunas de las tareas mas básicas. No obstante, había un dll que destacaba ivecuqmanpnirkt615, porque no es uno del sistema y se encontraba en ambos procesos.

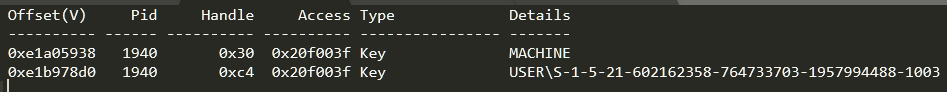




* Una vez detectado en que DLL se podría encontrar el código malicioso instalado en el equipo, procedimos a buscar las funciones manejadoras (handles) de los procesos sospechosos, para las DLL que utilizan, en concreto, para la DLL sospechosa (ivecuqmanpnirkt615), mediante el siguiente comando:

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 handles -p 1940 -t Key > handles1940.txt

En la salida de dicho comando, según las indicaciones de Carlos, se podía apreciar un UserID de Windows en la última línea al final:



No obstante, no se podía obtener mucha información, por lo que procedimos a buscar handles, pero con más detalles como que ficheros de memoria secundaria estaban utilizando y alterando los procesos sospechosos a estudio (1940 y 740):

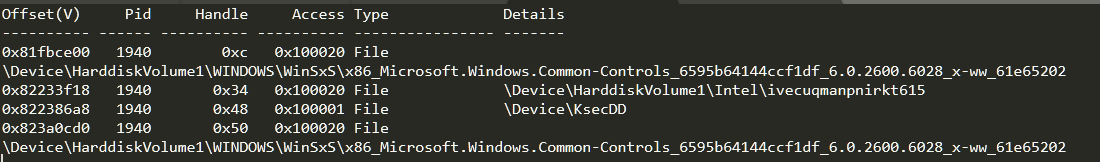
python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 handles -p 1940 -t File > handles1940File.txt

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 handles -p 1940 -t Mutant > handles1940Mutant.txt

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 handles -p 740 -t File > handles740File.txt

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 handles -p 740 -t Mutant > handles740Mutant.txt

De estos, obtuvimos mucha información, pero la mas importante se encuentra en la imagen posterior, resultado de buscar que ficheros estaba alterando el proceso 1940 (taskdl), en la que vemos que esta alterando el DLL en el que se sospecha que se encuentra el código malicioso. Gracias a esto, podemos confirmar que WannaCry lo primero que hace es tomar control del proceso taskdl y persistirse, tras lo cual procede a realizar rutinas periódicas de ocultado y encriptado de ficheros cada 30 segundos.



* Una vez conocido como actúa el proceso daemon de WannaCry cuando ya está creado, procedemos a revisar los registros del sistema, para conocer como es el proceso de arranque de WannaCry al inicio del sistema:

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 printkey -K "Microsoft\Windows\CurrentVersion\Run" > printkey.txt

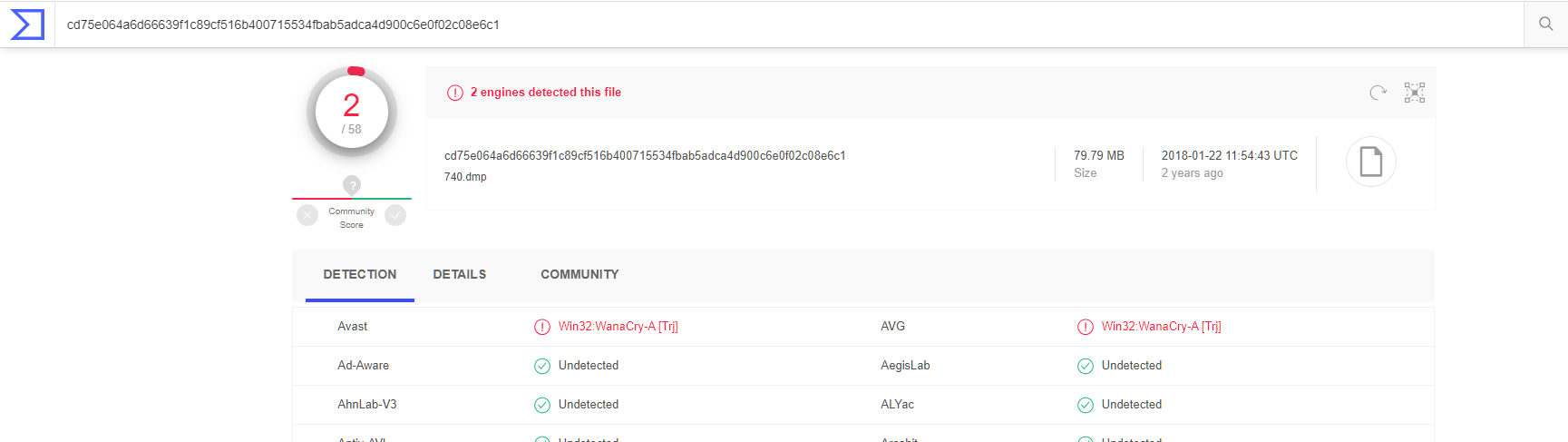
Con el cual, confirmamos nuestras sospechas, y en la salida se aprecia como el malware WannaCry ha creado un registro que hace que se inicie un proceso de WannaCry al comienzo del sistema, haciendo que se dispare el mecanismo de tomar el proceso taskdl (gestor de tareas de Windows) y modificarlo para que lance de forma periódica el proceso de WannaCryDecriptor que va tomando distintos ficheros y los va ocultando y cifrando, a menos que se haya registrado el dominio de killswitch (mencionado anteriormente).

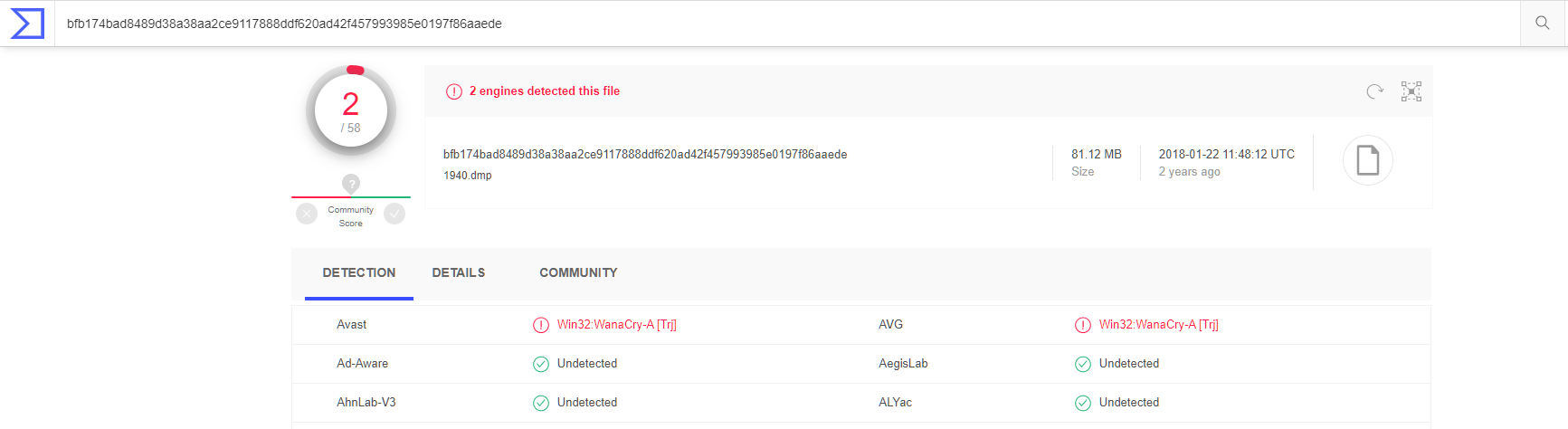
Una vez que conocemos el funcionamiento de este malware, mediante el siguiente comando, extrajimos las imágenes de los procesos 740 y 1940, que son los implicados en el WannaCry como hemos visto:

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 memdump -p 1940,740 -D memdump/

Estas imágenes de procesos, según nos indico Carlos, podemos confirmar que se tratan de los procesos utilizados para atacar por WannaCry si los subimos a la web virustotal.com y lo corroboramos.

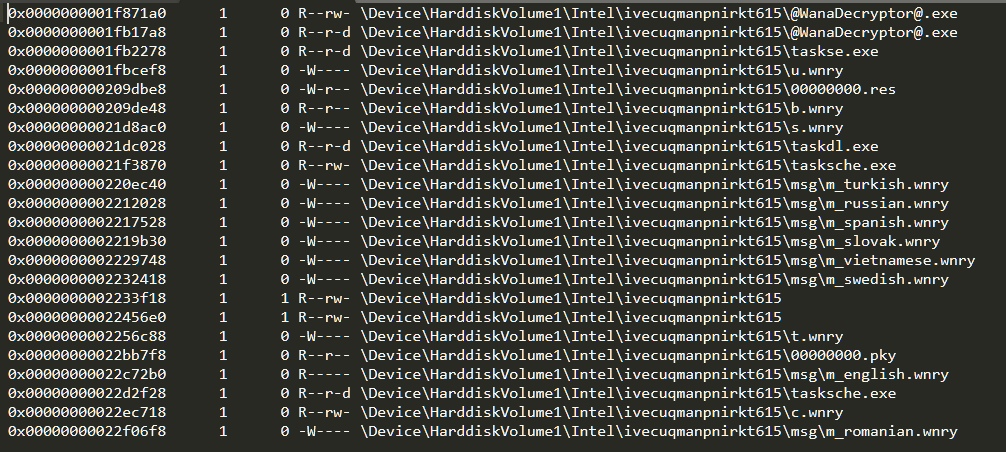
Tras realizar este proceso, como se pude ver en las capturas posteriores, pudimos ver que efectivamente eran dos de los procesos utilizados por WannaCry para realizar el ataque:





Por último, Carlos nos dijo que podíamos ver los ficheros que habían sido cifrados por WannaCry en la imagen del equipo afectado, buscando que ficheros concretos habían modificado los dos procesos sospechosos a estudio:

python ../volatility-master/volatility-master/vol.py -f malware.raw --profile=WinXPSP2x86 filescan | grep ivecuqmanpnirkt615 > filescanivecuqmanp.txt



Por último, Carlos nos comento que este proceso suele ir de la mano con un análisis de los distintos mensaje enviados por la red y de las estructuras de memoria de los procesos implicados en las comunicaciones de red de los equipos, para poder hacer un timeline más detallado del proceso de expansión del malware.

## Fuentes

* <https://www.virustotal.com/gui/>
* <https://es.wikipedia.org/wiki/WannaCry>
* <https://github.com/volatilityfoundation/volatility>