UNIVERSITAT DE BARCELONA

Trabajo de Final de Grado

grado de ingeniería informàtica
Facultat de Matemàtiques i Informàtica

Universitat de Barcelona

Análisis forense de una infección por malware

Autor:
Sergio Agruña Álvarez

Director:
Prof. Raül Roca Cànovas

22 de enero de 2021

Resumen

Abstract (English)

Today cybersecurity is a concept in progress in this society, given the state of pandemic due to CoVid-19 many companies have had to adapt to the new normal by increasing the number of people teleworking, due to the rush and lack of guidance , 2020 has become a goldmine for cybercriminals.

This paper presents the topic of forensic analysis of malware on a Windows 10 system. First, a small introduction is made and the reason for the selection of this work, followed by an explanation about the rise of cyber attacks today, statistics on the use of computers in families and / or companies and why we are currently in a time where having good security in our system is of vital importance to avoid catastrophes.

The main intention of this work will be exposed, which is to perform a mock forensic analysis on an infected computer. The different phases of this are analyzed following international regulations and a short explanation of the different types of malware that currently exist and how they work is also exposed. Finally, we will do a practical job infecting a virtual machine with a Windows 10 snapshot using a backdoor malware called Gcat, we will analyze how it works, how we can infect the victim and what options this malware has once infected, we will analyze what the attack is backdoor and how it works and finally we will carry out a forensic analysis doing all the real tests and making a final report explaining what evidence we have found on the infected computer.

Abstract (Castellano)

Hoy en día la ciberseguridad en un concepto en auge en esta sociedad, dado el estado de pandemia por culpa del CoVid-19 muchas empresas se han tenido que adaptar a la nueva normalidad aumentando el número de personas teletrabajando, por las prisas y la falta de orientación, 2020 se ha convertido en una mina de oro para los ciberdelincuentes.

En este trabajo se presenta el tema del análisis forense de malware en un sistema Windows 10. Primeramente se hace una pequeña introducción y el porqué de la selección de este trabajo, seguido de una explicación sobre el auge de los ataques cibernéticos en la actualidad, estadísticas sobre el uso de ordenadores en familias y/o empresas y el porqué actualmente estamos en una época donde tener una buena seguridad en nuestro sistema es de vital importancia para evitar catástrofes.

Se expondrá la intención principal de este trabajo que es conseguir realizar un simulacro de análisis forense en un ordenador infectado. Se analizan las diferentes fases de este siguiendo la normativa internacional y también se expone una pequeña explicación de los diferentes tipos de malware que existen en la actualidad y como funcionan. Por último haremos un trabajo práctico infectando una máquina virtual con una snapshot de Windows 10 mediante un malware backdoor llamado Gcat, analizaremos como funciona, como podemos infectar a la víctima y que opciones tiene este malware una vez infectado, entraremos a analizar que es el ataque backdoor y como funciona y por último realizaremos un análisis forense haciendo todas las pruebas reales y realizando un informe final explicando que evidencias hemos encontrado en el ordenador infectado.

Abstract (Català)

Avui dia la ciberseguretat en un concepte en avenç en aquesta societat, donat l'estat de pandèmia per culpa de l'CoVid-19 moltes empreses s'han hagut d'adaptar a la nova normalitat augmentant el nombre de persones teletreballant, per les presses i la manca d'orientació, 2020 s'ha convertit en una mina d'or per als ciberdelinqüents.

En aquest treball es presenta el tema de l'anàlisi forense de malware en un sistema Windows 10. Primerament es fa una petita introducció i el perquè de la selecció d'aquest treball, seguit d'una

explicació sobre l'auge dels atacs cibernètics en l'actualitat, estadístiques sobre l'ús d'ordinadors en famílies o empreses i el perquè actualment estem en una època on tenir una bona seguretat en el nostre sistema és de vital importància per evitar catàstrofes.

S'exposarà la intenció principal d'aquest treball que és aconseguir realitzar un simulacre d'anàlisi forense en un ordinador infectat. S'analitzen les diferents fases d'aquest seguint la normativa internacional i també s'exposa una petita explicació dels diferents tipus de malware que existeixen en l'actualitat i com funcionen. Finalment farem un treball pràctic infectant una màquina virtual amb una snapshot de Windows 10 mitjançant un malware backdoor anomenat Gcat, analitzarem com funciona, com podem infectar la víctima i que opcions té aquest malware un cop infectat, entrarem a analitzar que és l'atac backdoor i com funciona i finalment elaborarem una anàlisi forense fent totes les proves reals i realitzant un informe final explicant que evidències hem trobat a l'ordinador infectat.

Índice

Índice de figuras

1. Introducción

Hoy en día, la informática es una rama indispensable en la sociedad. Según el INE (Instituto Nacional de Estadística), el 78,2 % de las mujeres y el 77,0 % de los hombres utiliza internet a diario. El 80,9 % de la población española tiene un ordenador en casa y el 98,5 % un teléfono móvil [dE19].

Si hablamos del ámbito empresarial los porcentajes se disparan, actualmente como empresa necesitas tener un sistema informático para poder sobrevivir en esta sociedad. Las empresas y la ciudadanía confían en sus sistemas informáticos grandes cantidades de información personal de muy alto valor para agentes maliciosos (contraseñas, datos bancarios, correos, direcciones), a su vez, muchas empresas también guardan información confidencial de sus clientes (páginas de compra online, banca online...).

Aunque la prevención sigue siendo la mejor medida para reducir ataques cibernéticos es imposible estar 100 % seguro que no se vaya a producir una fuga porque día a día se crean nuevos códigos maliciosos y aparecen nuevas fallas de seguridad.

Microsoft Windows es con diferencia el Sistema Operativo más utilizado alrededor del mundo con casi un 85 % de uso. En el entorno profesional un 90 % de las empresas utilizan Windows. Esto significa que, dado que la mayoría de usuarios utilizan este SO, la mayoría de ataques ejecutados actualmente se centran en este.

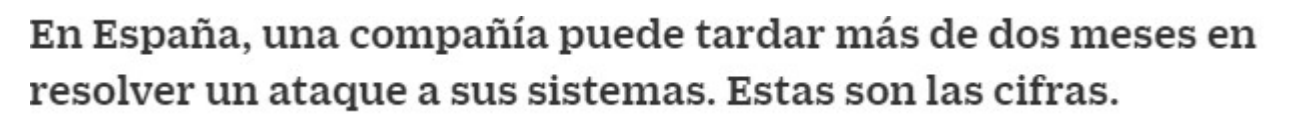


Figura 1: Titular articulo revista retina. (Fuente:`https://retina.elpais.com/retina/2020/07/17/tendencias/1594958904_685745.html`).

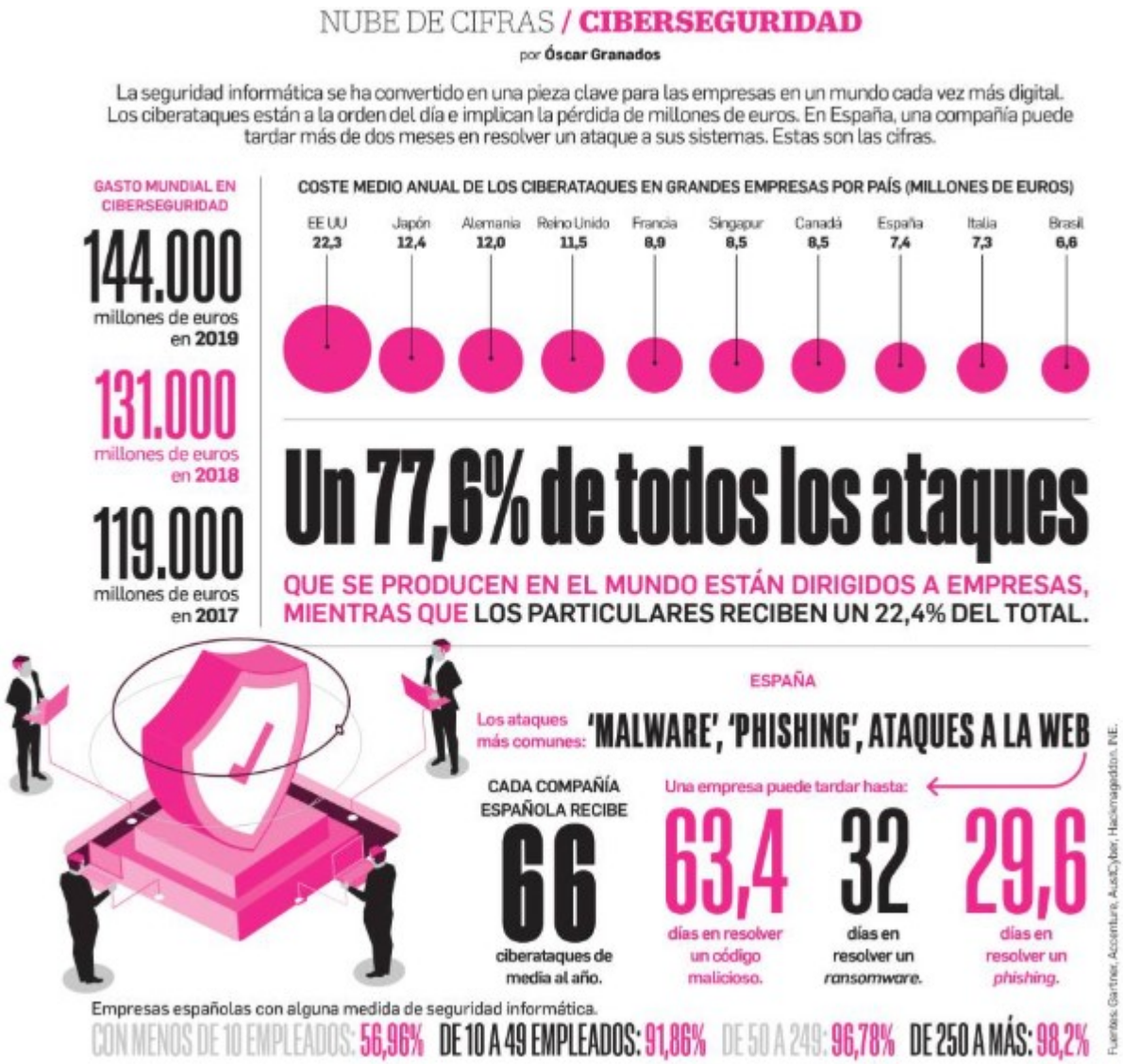


Figura 2: Cifras expuestas por la revista Retina en su artículo. (Fuente: `https://retina.elpais.com/retina/2020/07/17/tendencias/1594958904_685745.html`).

2. Objetivos

2.1. Objetivo general

El objetivo principal de este proyecto es conseguir hacer una simulación de análisis forense en un sistema infectado y conseguir extraer un informe preciso del ataque. Para poder hacer un buen análisis forense primeramente debemos saber que normativas sigue, como se hace y a que tipos de malware nos podemos enfrentar.

Utilizando el componente práctico quiero exponer un trabajo teórico sobre el análisis forense y la importancia de este cuando se produce un ataque a gran escala. Haciendo este proyecto se pretende:

- Enseñar los tipos de malware y lo expuestos que estamos ante la red.

- Aprender a hacer un análisis forense.
- Ver las diferentes maneras que se puede infectar un sistema y como actúa un malware de tipo *backdoor*.

2.2. Objetivos específicos

Estos objetivos principales se desglosan en los siguientes objetivos específicos:

- Recopilación de información sobre malware: recopilar toda la información importante sobre el malware y los ataques más sonados.
- Exponer las diferentes fases de un análisis forense: ver que partes se desglosa un análisis forense y exponerlas.
- Poner en práctica dichas fases: crear una simulación de ataque utilizando una máquina virtual y conseguir una línea de tiempo junto a un informe del ataque aplicando las fases explicadas en este proyecto.
- Investigar las herramientas que están en internet para la ayuda del análisis forense.

3. Introduccion al análisis forense

La ciencia forense es el uso de métodos científicos o experiencia para investigar delitos o examinar pruebas que podrían presentarse en un tribunal de justicia. La ciencia forense comprende una amplia gama de disciplinas, desde análisis de huellas dactilares y ADN hasta antropología y análisis forense de vida silvestre. Aunque representan disciplinas variadas, todos los científicos forenses enfrentan un conjunto común de desafíos. ¿Cómo se asegura de que los métodos forenses produzcan resultados fiables? ¿Cómo comunica los hallazgos a un jurado u otros no expertos de una manera precisa y comprensible? ¿Cómo puede mantenerse al día con las nuevas tecnologías sin quedarse atrás en el trabajo de casos? Hacer frente a estos y otros desafíos es fundamental para garantizar que la ciencia forense siga siendo una fuerza poderosa en apoyo de la justicia y la seguridad pública.[oST19].

Un análisis forense es capaz de arrojar información de gran valor sobre qué acciones han sido llevadas a cabo en un equipo. Esto no es solo la infección, también si alguien ha obtenido información con ese malware.
Para entender mejor la base principal de un análisis forense debemos explicar que es el Principio de Locard.

3.1. El principio de Locard

En el año 1910 el Doctor Edmun Locard escribió uno de los principios fundamentales que tenemos que tener presente a la hora de hacer un análisis forense en cualquier ámbito, sea policial o informático. “Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto” [Loc34]. Esta frase significa que cualquier delito, es decir, cualquier intento de infectar un ordenador dejan un rastro por lo cual siempre se pueden encontrar evidencias de este. Esto se puede aplicar a la ciencia forense digital, pruebas como las claves de registro, los archivos de registro pueden servir como equivalente digital del cabello y la fibra.

Hay dos ejemplos claros que ponen en práctica este principio:

- Visitar un sitio web: a la hora de visitar un sitio web se deja un rastro único para cualquier PC, primeramente, en el registro del servidor web aparecerá tu visita a la página web, después, en tu navegador se almacenará en caché una copia de las páginas que se ha visitado para evitar excesivas llamadas a servidor y en último lugar tu navegador guarda en un historial todas las páginas que has visitado. Es decir, aunque parezca que no has dejado ningún rastro a la hora de visitar una web ya que no has interactuado con nadie o no has hecho ninguna compra igualmente siempre dejas un rastro inequívoco.
- Intentos de inicio de sesión: cada vez que intentas realizar un inicio de sesión en un sistema se queda registrado, da igual si es exitoso o no.

4. Tipos de incidentes

Existen miles de contextos para realizar un ataque hacia un sistema, a continuación, voy a explicar las más usuales.

4.1. Botnet móviles

No es para sorpresa de nadie que en los últimos años se haya visto aumentada el número de amenazas contra dispositivos móviles, cada día millones de personas transmiten o guardan información sensible en sus teléfonos móviles (fotos personales, tarjetas bancarias, direcciones.). Los cibercriminales están explorando este mercado.
Las *botnets* móviles son redes que controlan de forma remota los dispositivos para fines maliciosos. Se trata de un malware cada vez más común.

4.2. Chantaje informático

El chantaje informático sigue siendo uno de las mayores fuentes de ingresos para hackers informáticos. Un chantaje típico es apoderarse de los fondos de una tarjeta de crédito , de una cuenta bancaria o información personal de un usuario o empresa a partir de un ransomware.
El método es fácil, el hacker introduce un *Cryptolocker* el cual cifra todos los datos personales del sistema infectado, luego el atacante pide un rescate por esa información.

Un ejemplo muy claro fue el famoso ataque WannaCry donde se cifraron millones de datos de empresas famosas como Telefónica o incluso hospitales y luego se pidió un rescate por ellos.

4.3. Criptomonedas

Los bitcoins están muy valorados por tener un sistema de pago descentralizado y lo difícil que es de rastrear por todo ello es muy popular entre los cibercriminales, la pueden utilizar como intercambio monetario entre víctima y atacante o incluso puede ser objetivo de un ciberataque

5. Tipos de ataques

Un ataque informático es "un asalto a la seguridad del sistema, derivado de una amenaza inteligente; es decir, un acto inteligente y deliberado (especialmente en el sentido de método o técnica)para eludir los servicios de seguridad y violar la política de seguridad de un sistema"[For00].

5.1. Ataques dirigidos

En el pasado, las agencias y el gobierno llevaban a cabo la mayoría de atraques dirigidos, ahora esta práctica ya no es única de ellos, hoy en día no se trata solo de robo de datos, también se pueden intentar borrar datos, colapsar los equipos, robar dinero o causar importantes daños a la reputación de una marca.
Un ejemplo claro de ataque dirigido es el denominado *phishing*, este está orientado en intentar robar nuestras credenciales y contraseñas personales.

La característica principal de un ataque dirigido es que detrás normalmente hay una planificación por parte del atacante, no se trata de un ataque al azar, sino que el objetivo ha sido elegido por un motivo, ya sea que se ha descubierto una vulnerabilidad explotable o que tiene un activo muy valioso. Este ataque es severamente peligroso, si el atacante ejecuta un buen trabajo de ingeniería social sobre el usuario (investigar sus redes, sus gustos, etc.) puede hacerse con el activo muy fácilmente.

Entrando en el ámbito del análisis forense, un ataque dirigido se puede detectar mediante el análisis de la red y los registros, estos nos indican si el ataque ha sido centralizado en un solo dispositivo o ha sido global. También se puede estimar que tipo de ataque si analizamos la duración de este, si el atacante se ha dirigido directamente a la información deseada podemos concluir que sabía dónde dirigirse, había estado informándose de su víctima, en cambio si el tiempo de ataque es mayor significa que el ataque era global y no había un objetivo claro.

Un ataque dirigido consta de las siguientes fases:

1. Recogida de información: los ciberdelincuentes identifican y recopilan información disponible públicamente sobre su objetivo para personalizar sus ataques. La información recopilada puede abarcar desde el software y las aplicaciones de negocio a las relaciones internas.

2. Punto de entrada: se pueden utilizar métodos variados para infiltrarse en la infraestructura del objetivo como phishing de correo electrónico personalizado, *exploits* de día cero o de *software*, o técnicas de *watering hole*. También pueden utilizarse plataformas de mensajería instantánea y redes sociales para hacer que los objetivos pinchen en un enlace o descarguen malware.

3. Comunicaciones CC: una vez accedido a los sistemas los ciberdelincuentes se comunican constantemente con el malware para ejecutar rutinas maliciosas o recopilar información a través de servidores de comando y control (CC). Se intenta ocultar este tipo de comunicación para mantener sus movimientos ocultos.

4. Movimiento lateral: una vez dentro de la red los ciberdelincuentes se mueven de manera lateral por toda esta para buscar información clave o infectar otros sistemas valiosos.

5. Descubrimiento de activos y datos: una vez detectados los activos valiosos, estos se aíslan para una futura exfiltración a través de herramientas como Troyanos de Acceso Remoto (RAT) y otras legítimas.

6. Exfiltración de los datos: se trata del objetivo principal de los ataques dirigidos. La transferencia de estos datos, que incluyen propiedad intelectual, secretos comerciales e información al cliente, puede realizarse rápida o gradualmente. Los ataques dirigidos se esfuerzan por permanecer sin ser detectados en la red con el fin de acceder a las joyas de la corona de la compañía o datos valiosos. Además, los actores de la amenaza también pueden buscar otros datos confidenciales como documentos de alto secreto de instituciones gubernamentales o militares.

Información extraída de [Itd17].

Los ataques se dividen en dos tipos, ataques activos y ataques pasivos.

5.2. Ataques activos

Un ataque activo es aquel que altera el sistema o red atacado modificando el flujo de datos transmitido. Los ataques activos pueden clasificarse de la siguiente manera:

- Enmascaramiento o suplantación de identidad (*Spoofing*): el atacante se hace pasar por una entidad diferente, por ejemplo, las secuencias de autenticación pueden ser capturadas y repetidas después de que una secuencia válida haya tenido lugar.

- Réplica o re-actuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado debido a que realiza una retransmisión subsecuente

- Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mismos mensajes son retardados o reordenados.

- Interrupción del servicio: impide el uso o la gestión normal de las utilidades de la comunicación.

5.3. Ataque pasivo

Estos ataques reciben su nombre debido a que el atacante no altera en ningún momento la información directa, es decir, su trabajo se limita a monitorear y escuchar la información transmitida.

Un ataque pasivo tiene los siguientes objetivos:

- Interceptación de datos: consiste en interceptar información sensible del usuario una vez ha sido enviado o esperando la recepción.

- Análisis de tráfico: se trata de observar el tráfico que pasa por una red en concreto.

6. Malware

El *malware*, también conocido como código malicioso, se refiere a un programa que se inserta de forma encubierta en otro programa con la intención de destruir datos, ejecutar programas destructivos o intrusivos, o comprometer de otro modo la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo de la víctima. El malware es la amenaza externa más común para la mayoría de los hosts, que causa daños e interrupciones generalizados y necesitando grandes esfuerzos de recuperación dentro de la mayoría de las organizaciones.[oST13b]

Existen muchos tipos de malware que varían según su origen o función:

- Virus.
- Gusanos.
- Troyanos.
- Keyloggers.
- Spyware.
- Botnets.
- Adware.
- Ransomware.

6.1. Virus

Un virus es un programa que se puede copiar a sí mismo e infectar un sistema informático sin permiso ni conocimiento del usuario. Un virus puede corromper o borrar datos de tu sistema, puede utilizar e-mails o programas de mensajería para enviar el virus a otros ordenadores o incluso borrar todo el contenido de un disco duro. [oST17b]

Una vez el virus se ha reproducido por tu sistema ejecuta las instrucciones de código escrito por el autor de este. La pregunta principal que nos hacemos es porque hay tanto aumento de los incidentes relacionado con virus, normalmente se trata de malware menos agresivo que otros, ya que la función principal es borrar información o molestar al usuario, esto es lo que pensamos todos y por esta misma razón ha recibido relativamente poca atención.

Frecuentemente un ataque por virus se trata a la ligera en el diseño y mantenimiento de ordenadores y sistemas. Además, ahora los usuarios que utilizan ordenadores frecuentemente están muy bien informados, por lo que conocen los errores y las lagunas de la mayoría de fabricantes de software y hardware, con la masificación del uso general de los ordenadores gracias a que ahora un ordenador está al alcance de cualquiera la seguridad de estos carece de mecanismos efectivos para evitar la intrusión de software malicioso.
Las vulnerabilidades de los virus informáticos y las amenazas relacionadas tienen más probabilidades de explotar son las siguientes:

- Falta de conocimiento del usuario:

  Los usuarios son la vulnerabilidad más explotable en cualquier sistema, cualquier atacante siempre intenta investigar antes que usuarios utilizan el sistema y sus debilidades, el ser humano es irregular, piensa, razona y lo más importante, se equivoca. Por ello es uno de los posibles causantes de la infección y propagación de los virus. Da igual que tengas el mejor software defensivo y el mejor *firewall* si hay un usuario que tiene unos métodos de gestión de contraseñas con muchos riesgos o incluso que tiene en un post-it su clave de inicio de sesión, a la vista de cualquier otro trabajador, está revisando su correo y hace clic a algún ejecutable o archivo PDF víctima de una campaña de Phishing. Antes de invertir en sistemas de ciberseguridad, enseña a los trabajadores a como trabajar en un entorno seguro libre de vulnerabilidades por parte suya.

- Ausencia o controles de seguridad inadecuados:

  Muchas empresas carecen de ningún sistema defensivo importante en su sistema lo que facilita mucho a los cibercriminales la intrusión de virus en este.

- Software desactualizado o carencia de medidas defensivas y de mitigación de daños:

  Muchas empresas no invierten en actualizar su software o revisar sus servidores lo que comporta que la mayoría de ellos no estén actualizados a la última versión. Por ello muchas de las vulnerabilidades que han conseguido arreglar en la última versión no se aplican y el servidor sigue siendo explotable.

6.2. Gusanos

Un gusano es programa informático que puede ejecutarse de forma independiente, puede propagar una versión funcional completa de sí mismo a otros hosts de la red y puede consumir recursos informáticos de forma destructiva.[oST15]

Los gusanos son una de las amenazas a la seguridad más graves y peligrosas a las que se enfrentan los sectores comerciales, políticos etc. Una vez el gusano ha infectado un colectivo de hosts, estos se utilizan colectivamente para ejecutar ataques como por ejemplo DDoS (*Distributed Denial of Service*) o una campaña de phishing.

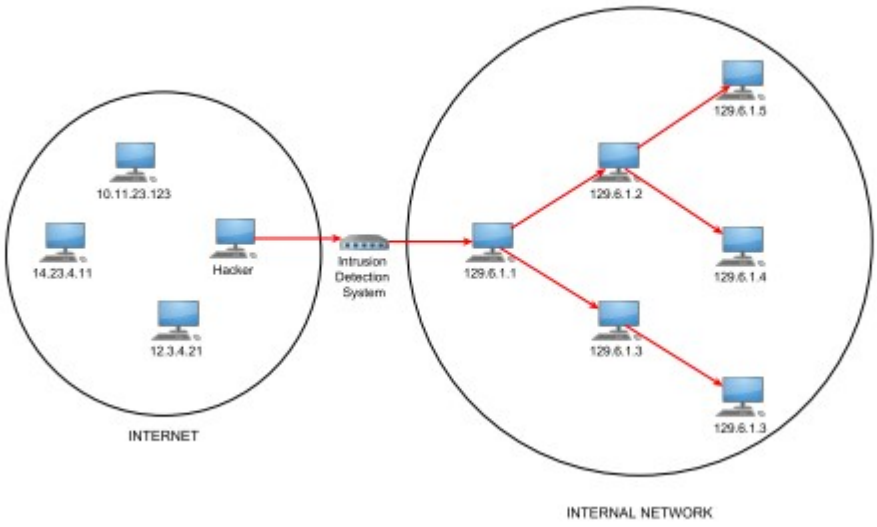


Figura 3: Esquema de la propagación de un gusano en la red. (Fuente: Propia).

La diferencia fundamental entre un gusano y un virus es la forma de propagación de estos. Una vez el gusano entra en su sistema no necesita ninguna ayuda externa para poder autorreplicarse, no es ni necesario que el PC esté en uso para que se propague.

6.2.1. Gusanos de e-mail

El método de propagación de estos gusanos se basa en el phishing a través del correo electrónico. Envían correos trampa a todos los usuarios de su lista, una vez uno de ellos cae en la trampa se replica enviando a todos los usuarios de la primera víctima. La mayoría de estos correos contienen URL maliciosas o archivos ejecutables.

6.2.2. Gusanos de mensajería instantánea

La forma de propagación de estos gusanos es idéntico a los del e-mail descritos anteriormente salvo que utilizan los servicios de mensajería instantánea como medio para expandirse, plataformas tales como Skype, Telegram o Whatsapp son las preferidas. El mensaje intenta atraer la atención de la víctima para que haga clic en el enlace.

6.2.3. Gusanos de intercambio de archivos

Las plataformas de transferencias de archivos de *peer to peer* (igual a igual) tales como Bitorrent se han vuelto muy populares estos últimos años y por consecuencia un objetivo claro de los atacantes para depositar los gusanos en algunos archivos. Estas redes de intercambio de archivos operan sin control ni regulación lo que facilita mucho la tarea de los cibercriminales para incrustar gusanos en archivos con una gran demanda.

6.2.4. Gusanos de red

Los gusanos de internet no interactúan con el usuario para propagarse, no tienen esa necesidad, como bien dice el nombre estos se propagan a través de la red en un sistema de ordenadores, desde el equipo

infectado el gusano busca a través de la red LAN otro sistema para infectar y así poder detectar las vulnerabilidades de estos.

Los gusanos en sí no son un gran problema, el mayor daño que pueden causar a un ordenador es el bloqueo o la excesiva lentitud. Pero, los cibercriminales lo utilizan como un transporte de otro tipo de malware más difícil de introducir al sistema de la víctima, tales como ransomware, malwares para recopilar datos útiles de la víctima o incluso instalar una puerta trasera en el sistema del afectado son uno de los muchos ejemplos de malware que puede llevar un gusano consigo mismo.

6.3. Troyanos

Un troyano es un programa informático que parece tener una función útil, pero que también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces mediante la explotación de autorizaciones legítimas de una entidad del sistema que invoca el programa.[oST17a]
Un troyano es un malware muy versátil capaz de eliminar, modificar y bloquear datos confidenciales del sistema o incluso interrumpir el rendimiento de ordenadores. Hay diferentes tipos de troyanos dependiendo de cómo puede afectar a tu dispositivo:

6.3.1. Troyanos de puerta trasera

Un troyano de puerta trasera se utiliza para dar el control del dispositivo al atacante remotamente. Estos troyanos permiten al ciberdelincuente controlar por completo el ordenador infectado y tener acceso tanto a su información como los contactos que tenga este usuario.

6.3.2. Rootkit

Un rootkit es un programa diseñado para ocultar ciertos objetos o actividades en el sistema. A menudo su objetivo principal es evitar que el usuario detecte programas maliciosos que han infectado su sistema y así permitir que estos trabajen con total impunidad.

6.3.3. Resto

Existen una clase de troyanos donde solo tienen un objetivo, estos son. Troyano bancario, troyano DDoS, troyano downloader, troyano dropper... Y una larga lista que sigue de diferentes tipos de troyano, esto lo que nos indica que este malware es de los más usados por los hackers dada si polivalencia a la hora de atacar a un sistema.

6.4. Keyloggers

Un *keylogger* es un programa que registra y graba las pulsaciones de teclas. Esta información es recolectada y enviada a la persona que haya instalado el malware. Con esto el atacante tiene la información de todas las teclas que se han pulsado y el orden con lo cual tiene acceso a todas las contraseñas que hayas introducido al largo del día. Actualmente existen tres importantes tipos de keylogger.

6.4.1. Hardware

Pequeños dispositivos colocados entre el teclado y el PC. Debido a su pequeño tamaño puede pasar desapercibido durante largos periodos de tiempo para la víctima. Estos dispositivos tienen el poder de

capturar las pulsaciones de las teclas y almacenarlas, el problema principal recae a la hora de colocación y extracción. El cibercriminal debe de estar en contacto con el dispositivo infectado dos ocasiones para manipularlo lo que consiste que se debe de arriesgar a ser visto manejando el PC.

6.4.2. Software

Este tipo de registro de teclas se realiza mediante la función de Windows SetWindowsHookEx que supervisa todas las pulsaciones de teclas. El software espía generalmente aparecerá empaquetado como un archivo ejecutable que inicia la función de enlace, además de un archivo DLL para manejar las funciones de registro.

6.4.3. Kernel

Este tipo de registrador de teclas se encuentra en el nivel del *kernel* y recibe datos directamente del dispositivo de entrada (normalmente un teclado). Reemplaza el software principal para interpretar las pulsaciones de teclas.

Este tipo de keylogger puede ser programado para que sea virtualmente indetectable si se ejecuta cuando se enciende el PC, antes de que se inicie cualquier aplicación a nivel de usuario.
Dado que el programa se ejecuta a nivel de kernel, una desventaja de este enfoque es que no logra capturar contraseñas de autocompletar, ya que esta información se pasa en capa de aplicación. Con respecto a las keyloggers por software, a actualmente son las más comunes, orientadas a robar datos confidenciales o privados del usuario.

6.5. Botnets

Una red *botnet* se trata de una red de robots informáticos que se ejecutan de manera autónoma y automática. Eso significa que el atacante puede controlar toda una red de ordenadores de forma remota.

Generalmente un *hacker* crea un botnet usando un malware que infecta una gran cantidad de máquinas (un gusano, por ejemplo). El uso más común de un botnet es el ataque DDoS (Denial of Service), estos ataques utilizan la potencia del ordenador y el ancho de banda de cientos de dispositivos para enviar una gran cantidad de tráfico a una página web y sobrecargarla. Es decir, el objetivo principal es sobrecargar un sitio web, también se utiliza para otras operaciones como envió masivo de spam o fraudes a gran escala.

6.6. Spyware

El *spyware* es el software que se instala secretamente en un sistema de información para recopilar información sobre personas u organizaciones sin su conocimiento. Como en los casos anteriores tenemos diferentes tipos de spyware dependiendo del objetivo a atacar una vez infectado el sistema.

6.6.1. Ladrones de contraseñas

Se tratan de aplicaciones que se ejecutan en segundo plano y pueden recopilar información privada del usuario, información sobre el sistema y sobre la actividad de red. Esa misma información se transmite a un destino especificado por el autor del malware.

Este spyware puede ser transmitido a través de un software gratuito en línea, por correo electrónico o enmascarado en un programa inofensivo. El peligro de este malware reside en el poco conocimiento que puede tener el sistema de su infección, ya que estas se llevan a cabo silenciosamente y no muestran ningún signo al usuario de infección (lentitud en el ordenador, desaparición de archivos, etc...).

6.6.2. Troyanos bancarios

Ya mencionados anteriormente, este spyware se encarga específicamente de conseguir las credenciales de instituciones financieras. Estos aprovechan las vulnerabilidades que presenta la seguridad del navegador para modificar páginas web, alterar el contenido de transacciones o incluso añadir de nuevas de manera totalmente silenciosa. Pueden afectar un amplio espectro de entidades desde agencias de bolsa, portales financieros, carteras digitales llegando hasta bancos.

6.6.3. Infostealers

Se trata de aplicaciones capaces de analizar un ordenador infectado y buscar distintos tipos de datos, información sensible del usuario. Estos, al igual que los troyanos bancarios, se aprovechan de las vulnerabilidades de seguridad del navegador para recopilar información en sitios y foros en línea.

6.7. Adware

El *adware* es un software malicioso diseñado para mostrar una gran cantidad de anuncios por pantalla una vez iniciado el explorador. Se trata de un virus muy molesto pero muy poco peligroso, su única función es incordiar al usuario con *pop-ups* masivos y redirecciones a páginas de publicidad.

El método de infección se trata de camuflarlo tras un software legal o un archivo ejecutable. El fin del adware es generar ingresos para su propietario, este ganará dinero cada vez que se hace clics en uno de los anuncios mostrados. Hacer un seguimiento de la navegación de la víctima y así puede presentarle anuncios tentadores para esta aparte de poder vender esta información a terceros.

6.8. Ransomware

El *ransomware* se trata de un software malicioso el cual secuestra tu información impidiendo el acceso a ella y solicitando un rescate para volver a obtenerla. Normalmente el secuestro de la información se hace a partir de un cifrado, este malware cifra la información y el atacante pide un rescate para enviar la clave privada la cual dará acceso a la información.
Este tipo de malware se utiliza asiduamente contra empresas porque estas son las que guardan mucha información sensible tanto suya como de terceros y pueden pagar un alto precio por un rescate.

Debido a los avances de la criptografía, el aumento cada vez de más dispositivos inteligentes y el auge de los sistemas anónimos de pago como las criptomonedas el ataque por ransomware cada vez es más habitual contra empresas. Normalmente las infecciones por ransomware suceden como habitualmente suceden todas las infecciones por malware, por descuido humano. Un correo electrónico que adjunta archivos maliciosos, vulnerabilidades en el navegador o en la nube (sistemas de transmisión FTP, SSH, etc....) son las causas más grandes de infección.

El ransomware se trata de un malware muy sigiloso, normalmente se manifiesta una vez los archivos ya han sido codificados por lo cual es muy difícil de detectar cuando un sistema ha sido infectado y de qué manera.

Figura 4: Ejemplo de un sistema infectado por malware. (Fuente: `https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware`).

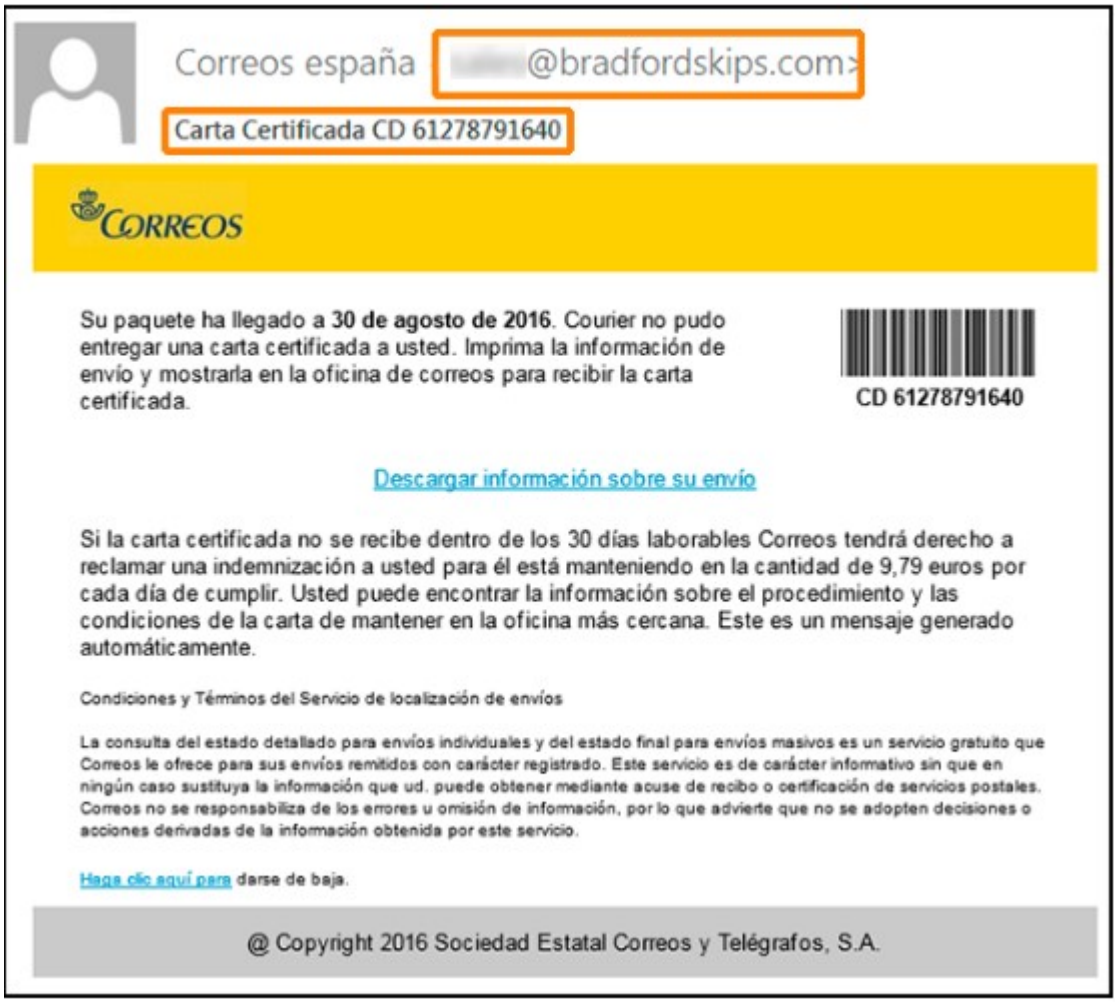


Figura 5: Ejemplo de un correo phishing. (Fuente: `https://www.incibe.es/protege-tu-empresa/avisos-seguridad/otra-oleada-ransomware-suplantando-correos`).

Hay 3 tipos de ransomware los cuales se clasifican dependiendo del nivel de dificultad de estos:

6.8.1. Scareware

Este tipo de ransomware no es tan agresivo ni temible. Su principal ataque es la publicidad agresiva hacia las víctimas. Una vez infectada esta recibirá mensajes emergentes avisando de qué se ha detectado un malware malicioso en el sistema y la única forma de deshacerse de él es pagando, se trata de un bombardeo constante que puede llegar a molestar al usuario, pero los archivos nunca se verán afectados.

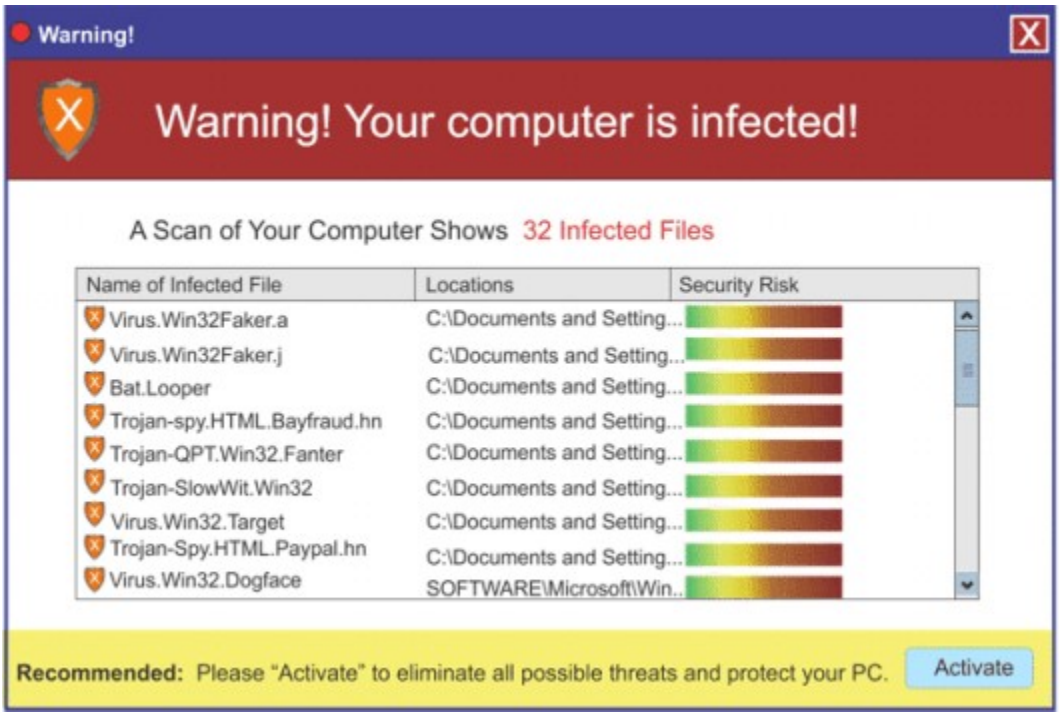


Figura 6: Ejemplo de falso aviso en un ordenador infectado por un scareware. (Fuente: `https://derechodelared.com/scareware/`).

6.8.2. Bloqueadores de pantalla

Este tipo de ransomware ya empieza a ser más peligroso, ya que afecta a tu uso del PC. Este malware bloquea totalmente la pantalla de tu sistema poniendo un falso aviso sobre que las autoridades han detectado un uso ilícito de este PC por lo cual queda confiscado o debe pagar una cantidad de euros en bitcoins de multa a una cartera digital. Obviamente este comunicado es totalmente falso, la intención del atacante es engañar a la víctima que esta, presa del pánico, abonara el importe indicado para poder desbloquear el PC.

Figura 7: Ejemplo de un sistema infectado por un ransomware bloqueador de pantalla (Fuente:Google imágenes).

6.8.3. Ransomware cifrado

Este es el tipo de ransomware del cual he hablado antes, este tipo de ataque normalmente está destinado a las empresas, secuestra sus archivos cifrándolos y luego piden una alta cantidad de dinero por ellos. Su peligro reside en que una vez estos archivos estén cifrados no hay ningún software capaz de descifrarlos a no ser que se posea la clave privada del cifrado.

El cifrado no existe para ayudar a los ciberdelincuentes a poder secuestrar tus documentos sino totalmente, al contrario, si un atacante consigue robar información, pero esta está cifrada se trata de papel mojado, no sirve de nada, pero con este malware lo utilizan para el chantaje. En general, cualquier aplicación que dañe el sistema de un usuario se puede considerar como malware.

Es uno de los ataques más usuales dado la facilidad que tienen a la hora de entrar en el sistema (mediante un ejecutable, un archivo torrent, un banner etc.). Por eso es el arma más utilizada para los ciberdelincuentes a la hora de infectar un sistema, lo que nos deja estos datos sorprendentes:

- Según la multinacional de seguridad informática Bitdefender, en 2014, los códigos maliciosos les reportaron a los hackers alrededor de 30 millones de dólares de beneficio, cosa que ha ido aumentando al cabo de los años.
- Aproximadamente un tercio de los ordenadores del mundo han sido afectados por malware de una forma u otra.

- En junio de 2019 casi dos billones de entradas de *big data* fueron hackeados afectando a un largo número de víctimas, tales como el FBI.
- En 2020 se han registrado 1077,45 millones de malwares diferentes.
- Actualmente existen varias páginas web donde te muestran a tiempo real los ciberataques que se ejecutan.

Figura 8: Titular del articulo extraido de https://www.nbcnews.com/tech/security/thousands-identities-personal-information-published-fbi-related-hack-n994366.

Dado la importancia de estos incluso las personas que no están introducidas en este tema han escuchado hablar de famosos malware que han conseguido poner en jaque a la mayoría de multinacionales como el caso del famoso ransomware WannaCry.

Figura 9: El Ransomware Wannacry siendo portada en el diario digital de El País. (Fuente: `https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html`.

7. Procedimiento buen análisis forense

Para que un análisis forense sea válido y pueda ser expuesto como prueba de peso ante un juicio deberá de poseer ciertas características esenciales [dC14]:

- Verificable: se deben poder comprobar la veracidad de las conclusiones extraídas de la realización de estos análisis.
- Reproducible: se debe poder montar un entorno donde se puede reproducir la investigación y mostrarlo a cualquiera que lo requiera.
- Documentado: todos los procesos del análisis como sus evidencias encontradas y las conclusiones deben de estar correctamente documentados, bien detallados y estructurados.
- Independiente: no debe influir ningún factor externo a la toma de conclusiones después de la recaptación de evidencias.

7.1. Metodología

El procedimiento de un análisis forense consta de unas fases las cuales corresponden a una base común de cualquier análisis forense informático. Sí que es verdad que existen varios protocolos ampliamente

conocidos en otros países, pero las bases generales son las que explicaré a continuación:

- Identificación de evidencias: primeramente, antes de empezar a buscar evidencias se debe de asegurar la escena para saber si durante el ataque se han creado por ejemplo usuarios administradores que pueden borrar datos o robar información y paralizar la investigación. Una vez asegurada la escena debemos de identificar el sistema que vamos a analizar, e identificar el hardware que pueda contener información.

- Adquisición y preservación de evidencias: la evidencia digital incluye información en computadoras, archivos de audio, grabaciones de video e imágenes digitales. Esta evidencia es esencial en delitos informáticos y en Internet, pero también es valiosa para el reconocimiento facial, las fotos de la escena del crimen y las cintas de vigilancia. Los investigadores del NIST están desarrollando herramientas, métodos de medición, estándares y datos para respaldar el análisis forense de evidencia digital.

Para que esto sea posible las evidencias deben de tener ciertas características:

- Admisible: toda prueba debe de tener un valor legal.

- Auténtica: toda prueba no debe de tener signos de manipulación alguna.

- Completa: no se debe de valorar subjetivamente ninguna prueba a la hora de ser expuesta.

- Confiable: las técnicas utilizadas para la obtención de evidencias deben de ser fiables y verídicas.

Una vez adquiridas las pruebas estas se tienen que preservar correctamente para garantizar que no se pierdan o se dañen dado que el desconocimiento sobre qué tipo de ataque puede generar que se pierda información relevante y decisiva.

A veces estos aspectos son sencillos de seguir, pero va un poco en contra de la lógica humana como por ejemplo nunca se debe de apagar el equipo, se podría perder la información volátil o incluso dañar alguna parte del hardware.

- Análisis de las evidencias: antes de empezar el análisis debemos de tener en cuenta el tipo de incidente que estamos investigando. Si conocemos el incidente podemos indagar en las zonas donde sabemos que puede haber evidencias.

- Documentación: esta fase es fundamental en el proceso del análisis forense. Todo el trabajo realizado anteriormente no serviría para nada si no se documentara bien los datos conseguidos. Para ello se debe de hacer un trabajo metódico siguiendo unas pautas ya marcadas.

4 pasos (identificación, adquisición, análisis y documentación) están recogidas en 4 fases que son las que seguiré en mi caso práctico. Estas se corresponden con una base común de cualquier análisis forense informático, extraídas de RFC 3227 [For02]. A pesar de que existen varios protocolos conocidos tales como el modelo DFRWS, el modelo Casey..., todos ellos recogen las mismas acciones comentadas anteriormente cambiando levemente las acciones.

8. Fase 1: Identificación de evidencias

La identificación y preservación de las evidencias es uno de los pasos más importantes durante un análisis forense y muchas veces el más ignorado. El objetivo principal de identificar y asegurar las evidencias es primeramente evitar que nadie pueda accidentalmente o a propósito alterar o destruir alguna evidencia.

Uno de los problemas más comunes durante el manejo de incidentes de malware es la mala comunicación y coordinación. Cualquier persona involucrada en un incidente, incluidos los usuarios, puede causar inadvertidamente problemas debido a una visión o comprensión limitada de la situación. Para mejorar la comunicación y coordinación, una organización debe designar de antemano algunas personas o un pequeño equipo para ser responsable de coordinar las respuestas de la organización a los incidentes de malware.

El objetivo es mantener la conciencia de la situación mediante la recopilación de toda la información pertinente, tomando decisiones que son en el mejor interés de la organización, y comunicando la información y las decisiones pertinentes a todas partes relevantes de manera oportuna. Para los incidentes de malware, las partes relevantes a menudo incluyen a los usuarios finales a quién se le pueden dar instrucciones sobre cómo evitar infectar a sus huéspedes, cómo reconocer los signos de una infección y qué hacer si un anfitrión parece estar infectado. El coordinador también debe proporcionar orientación e instrucciones para todo el personal que ayuda con los esfuerzos de contención, erradicación y recuperación. Otro posible papel del coordinador es interactuar con partes externas, como otros equipos de respuesta a incidentes que enfrentan problemas similares de malware. [oST13a]

También debemos tener en cuenta que algunas evidencias deben de ser almacenadas y tratadas en entornos especiales tales como dispositivos magnéticos u ópticos. Estas evidencias deben ser protegidas de campos electromagnéticos o aumentos de tensión para evitar que se dañe.

8.1. Asegurar la escena

Como hemos dicho anteriormente asegurar la escena antes de empezar con la identificación es un paso muy importante de cara a conseguir un análisis forense satisfactorio. Es importante recalcar que el investigador no solo se debe enfocar en el análisis técnico del equipo, sino que también debe asegurarse que la escena donde se ha producido el incidente no haya sido alterada bajo ningún concepto desde el descubrimiento del mismo hasta el inicio de un análisis.

Todos los implicados en la investigación deben de ser conscientes que cualquier acto que lleven a cabo puede comportar unas consecuencias fatales e irreversibles.

Antes de empezar a manipular la escena es recomendable realizar fotografías generales del equipo y el entorno para introducir dentro del informe el estado inicial, justo cuando se ha encontrado el incidente antes de la actuación de los investigadores.

Por otra parte, también se deberá seguir en parte la actuación de un crimen cuando investiga la policía, se deberá crear un perímetro para evitar que todo personal externo pueda tener acceso directo al equipo implicado o alrededores. Cada paso inicial debe de estar totalmente consensuado entre los investigadores los cuales deben asegurarse que no se perderá ni se alterará información. Una vez finalizada esta fase y con la escena bien asegurada teniendo en cuenta todos los puntos expuestos anteriormente podremos

pasar a la segunda fase, la identificación de evidencias y la posterior recolección de las mismas.

8.2. Identificación de evidencias

Durante la fase de identificación el investigador deberá tomar decisiones importantes que marcaran el resto de los acontecimientos de esta. Una de las más importantes es la siguiente, ¿Se debe detener el sistema a analizar o dejarlo e investigar encendido? La respuesta nunca ni es sencilla ni es general, ya que hay que tener en cuenta una serie de factores que son intrínsecos a casa caso. No podemos decidir bajo un manual de instrucciones, el investigador debe de analizar y decidir si se debe apagar el equipo una vez llegados a la escena (con la perdida de información que eso comporta) o intentar obtener las evidencias volátiles que desaparecerán una vez desconectado el equipo.

En lo referente a las evidencias contenidas en el sistema a analizar podemos hacer una clasificación teniendo en cuenta su volatilidad, desde el hardware más volátil que son los registros y la memoria caché hasta las evidencias menos volátiles como es la documentación, disco duro, etc.

La diferencia entre la volatilidad de los elementos es crucial, los elementos más volátiles deben de ser investigados y trabajados en la misma escena sin haber desconectado el sistema en cambio las evidencias menos volátiles se pueden analizar mediante herramientas forenses una vez extraído el sistema y llevándolo a un entorno más seguro utilizando copia de datos.

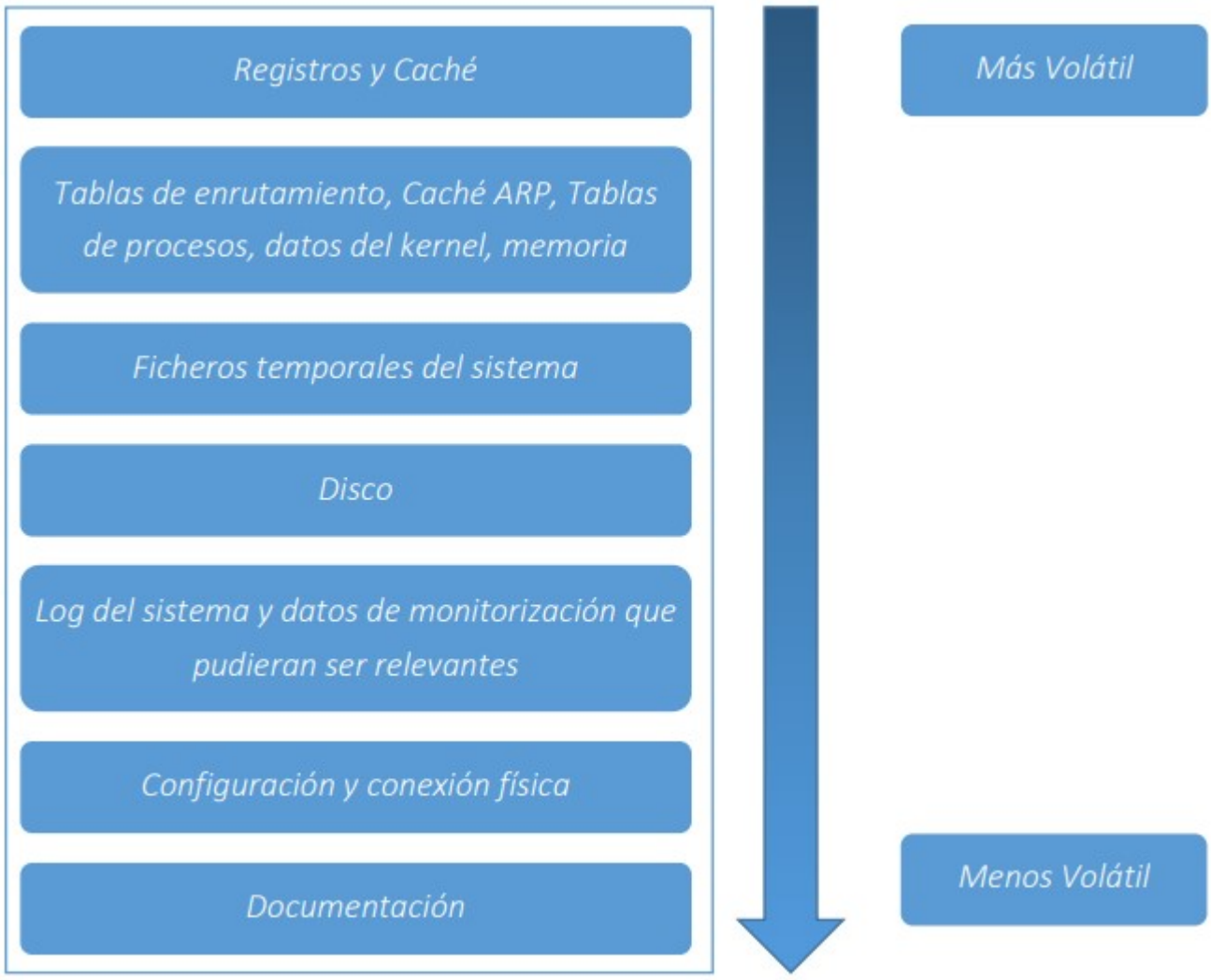


Figura 10: Orden de volatilidad (Fuente: propia).

Identificar las evidencias que pueden contener cada trozo de hardware es esencial para poder responder la pregunta previamente planteada y valorar cuáles son cruciales para la investigación y se deberán de adquirir y cuáles no. En esta fase es importante poder etiquetar los equipos y obtener información de sus características, también se deberán tener en cuenta que personas han estado en contacto previamente con el equipo para poder rastrear sus acciones para completar la línea temporal.
Por otra parte, si el ataque ha sido a varios equipos de la red se debe de dibujar una estructura de la misma, en ella se deben de incluir los cables que están conectados, hacia donde van y los periféricos que pueden estar implicados (impresora, fax, router...). Los discos duros deben de estar identificados correctamente para poder trabajar con ellos sin peligro, la identificación comporta anotar marca y modelo, número de serie y capacidad. Debido al trasiego de personal en la escena es importante que se documenten que agentes interfieren en la manipulación de las evidencias identificadas, así como la actividad que realicen en ellas y el marco temporal en el que se han llevado a cabo dichas acciones, con esto nos aseguramos de poder comprobar quien ha manipulado que evidencia a la hora de encontrar algún error en la cadena de custodia. Cabe mencionar especialmente los ficheros de hibernación y paginación, estos dos ficheros nos pueden permitir realizar un análisis de memoria sin la necesidad de tener el equipo encendido. Pero para hablar de esto debemos de saber antes que son estos dos ficheros.

El fichero de hibernación es una imagen de la memoria RAM de la máquina comprimida la última vez que el equipo cambio su estado a hibernación. Cuando la cantidad de memoria que utilizan todos los procesos del PC supera a la cantidad de memoria RAM disponible se utiliza el archivo de paginación. Esta vuelca aquellos datos que sobrepasan su capacidad de tal manera que aquellos datos que la memoria volátil no puede manejar se pasan al disco duro. Se podría decir que el archivo de paginación es una memoria RAM secundaria que Windows asigna a un espacio en el almacenamiento para utilizarla de manera exclusiva de manera que cuando tengamos muchos procesos cargados en memoria RAM que la sobrepasemos se puedan seguir ejecutando más lentamente sin que el usuario se entere.

9. Fase 2: Adquisición y preservación de evidencias

Una vez identificadas todas las evidencias se debe llevar a cabo su correcta recolección. Esta debe de ser un proceso sistemático y, a ser posible, lineal. Para ello utilizaremos la copia bit a bit de los discos que se requiera su análisis en el laboratorio, hay que copiar exactamente el contenido de los discos, sin ningún mínimo detalle diferente.

La copia de los discos se debe de volcar en un hardware limpio y preparado previamente para su conservación, una vez realizada la copia bit a bit se deberá comprobar si ha habido algún error o cambio en esta, para ello utilizaremos el hash de la copia, este lo compararemos con el hash del disco original y si son idénticos significa que la copia se ha realizado correctamente.

Si se trata de un caso que se va a llevar de forma jurídica esta primera copia será entregada al secretario judicial, y realizaremos una segunda copia, esta será guardada como un *backup* en el laboratorio por si a la hora de trabajar sobre la tercera copia corrompemos algún dato.

De acuerdo con la tabla de volatilidad debemos seguir un procedimiento para conseguir el máximo de evidencias, para ello debemos de seguir un orden de volcado.

1. Volcado de registros y caché.
2. Volcado del estado de red.
3. Volcado de memoria del equipo.
4. Volcado de ficheros de paginación e hibernación.
5. Copiado bit a bit del disco.
6. Estudio del sistema de ficheros.

Para la faceta de preservación hay que seguir con las precauciones anteriormente escritas en la primera fase, una mala preservación de las evidencias, un mal uso o una mala documentación puede provocar que toda la investigación no haya servido de nada, por lo tanto, todas estas evidencias deben de seguir la cadena de copias anteriormente mencionada para así evitar la pérdida total o parcial de la información.

Complementariamente debemos de anotar todas las acciones que ejecutamos sobre una memoria para así mantener un control de todas las evidencias que se dispone. Cada evidencia debe de ser almacenada

debidamente para evitar que se deteriore (por ejemplo, cintas de copias de seguridad deben de estar aisladas y protegidas de la electricidad estática). El lugar donde se almacena debe de reunir las condiciones favorables para la preservación, no solo de acceso físico, sino también ambientales. Todo debe de estar bajo un control estricto.

Toda la cadena de custodia, el transporte y el almacenaje debe de estar previamente documentado, donde ha estado la evidencia quien la manejo, quien la descubrió, cuanto tiempo estuvo en manos de quien, todo eso debe de estar perfectamente documentado.

10. Fase 3: Análisis de evidencias

En esta fase se debe de poder sacar en claro que causó el incidente, como lo hizo y que afectaciones ha tenido en el sistema. Se trata de la parte principal de la investigación, ya que todas esas evidencias deben de poder ser las que especifiquen como ha sido el ataque, un buen análisis determina una buena conclusión forense.

Los resultados que se obtengan de este proceso han de ser verificados y reproducibles delante de un tribunal (si estamos hablando de un caso que va a ser llevado a la justicia). En cualquier instante deberíamos de poder montar un entorno donde poder reproducir la investigación.

Para analizar cada una de estas evidencias el analista puede hacer uso de las herramientas de diversa índole que crea conveniente, así también como referencias externas siempre y cuando no se altere el resultado final. Para ayudar a que el investigador pueda ejecutar sus análisis con presteza nos podemos centrar en varias sub fases y puntos importantes que normalmente se realizan en un análisis general.

- Preparar un entorno seguro y claro para poder trabajar adaptándose a las necesidades del analista.
- Reconstruir una línea temporal con los hechos sucedidos (esta línea temporal debería de estar casi acabada porque la llevamos trabajando a la vez que recolectábamos evidencias)
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar al causante del ataque.
- Evaluar los daños causados.

Estos pasos son generales durante el análisis, por otra parte, el analista debe de decidir que otros pasos hacer dependiendo de muchas variables (sistema operativo, pruebas conseguidas, etc.).

10.1. Preparar un entono seguro y claro para poder trabajar adaptándose a las necesidades del analista

Antes de empezar un análisis se debe de preparar un entorno adecuado para este. Para ello se debe de decidir qué tipo de análisis vamos a ejecutar, análisis en caliente o en frío.

En un análisis caliente se toma el riesgo de hacer la investigación sobre los discos originales, hacer esto conlleva un gran riesgo, un error puede corromper todo el disco lo cual sería catastrófico para la investigación y posiblemente sería el cierre de esta. Un análisis en caliente sería ejecutado cuando el

tiempo es la prioridad. Evitar que el atacante borre sus huellas y así perder todo rastro posible o incluso evitar que el malware siga causando daños al ordenador.

El análisis en frío es el más utilizado, se utilizan las copias previamente creadas del disco y se prepara una máquina virtual con el mismo SO del equipo afectado y se le monta una imagen del disco a partir de las copias de este que se efectuaron con anterioridad. Con esto tendremos total libertad en nuestras acciones, podremos ejecutar archivos, eliminar, copiar carpetas, etc. Ya que si por algún casual corrompemos la imagen siempre se puede volver a montar sin dañar ninguna evidencia.

10.2. Reconstruir una línea temporal con los hechos sucedidos

El primer paso de cualquier análisis forense de malware, sea cual sea el tipo, es crear una línea temporal de los hechos. Con ello podrás saber en qué momento crítico se pudo producir el ataque y que lo causo. Para crear una buena línea temporal debemos de utilizar los tiempos MACD (*Modification, Acces, Change, Delete*) de los archivos, es decir, cuando fueron modificados, cuando se accedió a ellos, cuando se produjo algún cambo en los archivos y si fueron eliminados cuando se produjo.

Primeramente, se debe de buscar la información sobre el SO, fecha en la que se instaló, versión del sistema, última actualización. Para ello se puede buscar en los datos de registro. A partir de esto se debe identificar que usuarios se crearon al principio para comprobar si hay algún usuario no autorizado que se ha creado o alguno fuera de lo común del equipo.
Después de analizar el SO se deben de buscar que programas fueron instalados o modificados en las últimas fechas y que cambios provocaron en el sistema. Lo más habitual es que los programas que causaron el daño al sistema no se instalen en los lugares habituales, sino que se localizan en rutas poco habituales.

Por último, también se deben de analizar los archivos que no se ven a simple vista, se puede encontrar valiosa información en archivos ocultos, borrados.

10.3. Identificar el atacante

Una vez identificado que ataque ha sido con que malware debemos descubrir quien o quienes han sido los autores. Para ello debemos de investigar las conexiones de red para poder relacionar el origen del ataque buscando datos de la red como la dirección IP. Debemos centrarnos en redes que sean abiertas, es decir, sin ninguna clave WiFi y entre ellas las que estén enviando o recibiendo datos.

Normalmente esto no es tan fácil, ya que los atacantes utilizan programas que falsean sus IP mediante repetidores en distintos países para borrar su huella digital y ser imposible rastrear de donde proviene el ataque. Un ejemplo claro de esto último que he comentado es cuando alguien intenta entrar con nuestras credenciales a alguna red social, banco, o página web y en el correo electrónico de la misma avisándote del intento de entrada pone que el país de origen de esta proviene de Vientam, China, Bielorrusia, países donde la ley informática es más laxa. Lo más probable es que se trate de alguien en un país más cercano solo que está utilizando técnicas para evitar que se le pueda rastrear la IP y que salga un país completamente diferente al que él está viviendo.

10.4. Evaluar los daños causados

Nunca se puede calcular exactamente el daño causado por un ataque de malware a un sistema, lo que sí que se pueden hacer son estimaciones con base en distintos factores para conocer una aproximación de los daños causados. Para calcular que gastos nos ha causado económicamente debemos de cuantificar que sistemas y hardware hay que reemplazar y sumarle si debemos contratar algún equipo de reparación o instalación de software. Aparte, para que no vuelva a suceder se intentara invertir más dinero en ciberseguridad lo cual será un coste extra, aunque no sea directamente causado por el incidente se trata de un coste indirecto de este.

Cuando el ataque ha sido más importante aparte del hardware y el software dañados también debemos de hablar del robo e información confidencial, aquí se tendrá que calcular en un futuro cuanto le costara a la empresa perder esta información valiosa. No se trata de daño físico en sí ni cuantificable con dinero, sino que se trata de pérdidas a la larga porque no se sabe con certeza como puede afectar a la empresa y esa pérdida de confianza de los clientes en esta, ya que una empresa que ha sido atacada siempre pierde una parte de prestigio y de confianza por parte de sus clientes.

Cuando Facebook, Instagram, Amazon, Steam... etc. Son atacadas tienen un impacto negativo mundial miles de usuarios se dan de baja, borran sus datos personales o dejan de confiar y acceder a esa página solo por el miedo de que sus datos sean robados de nuevo, esto, visto a escala de una empresa como Amazon donde millones de personas compran y acceden es una nimiedad, pero si se trata de una pequeña o mediana empresa o un startup un ataque cibernético puede llevar a la quiebra total de esta. De modo que cuando hablamos de cálculo de perdidas siempre debemos de tener estos factores presentes para poder hacer un cálculo estimado.

11. Herramientas para el análisis

En parte gracias al código libre actualmente tenemos un gran abanico de herramientas para realizar un estudio forense en Windows 10. Debemos tener en cuenta que el propio sistema operativo nos puede dar la mayoría de información a partir de registros y rastros que deja el ataque, pero dado que el sistema está comprometido debemos utilizar aplicaciones externas ya que no nos podemos fiar de la información que nos muestra. Se debe procurar utilizar herramientas que alteren lo menos posible el escenario, evitando, en la medida de lo posible, el uso de herramientas de interfaz gráfico y aquellas cuyo uso de memoria sea grande.

Por esos mismos motivos adjunto a continuación una lista de las herramientas más eficaces según el Instituto Nacional de Ciberseguridad y explicación de su funcionalidad en el análisis forense, es de imperiosa necesidad estar seguro de que el software a utilizar para analizar dichas evidencias sea no invasivo y se encuentre en dispositivos protegidos contra escritura.

11.1. Kits open source

Para realizar una correcta obtención de evidencias es importante utilizar software no invasivo y que se puedan encontrar en dispositivos protegidos como USB o CD-ROM entre estos destacan los siguientes:

- Caine.
- DEFT.

- SIFT.
- Helix.

11.1.1. Caine

CAINE (*Computer Aided Investigative Enviroment*) es una distribución de Linux que está basada en Ubuntu y que está diseñada para realizar análisis forenses. Fue creada por Giancarlo Giustini y ofrece un entorno Linux completo, integrando herramientas de software existentes y con una interfaz gráfica amigable.

Esta distribución incluye una interfaz fácil de usar que reúne una serie de herramientas forenses conocidas de código abierto. Un entorno actualizado y optimizado para realizar análisis forenses, generador de informes semiautomático mediante el cual el investigador dispone de un documento fácilmente editable y exportable con un resumen de las actividades. Además, Caine utiliza varios parches construidos específicamente para hacer que el sistema no pueda alterar el dispositivo original para ser probado i/o duplicado.

11.1.2. DEFT

DEFT (*Digital Evidence & Forensic Tool*) es una distribución creada para el análisis forense que tiene como objetivo de ser ejecutado de tal manera que asegure la integridad y la no modificación de los elementos estudiados.
Este destaca por incluir la suite DART (*Digital Advanced Response Toolkit*), esta contiene aplicaciones de Windows que todavía no hay equivalencia en el mundo de Unix.

DART es una aplicación que organiza, recopila y ejecuta software en modo seguro con el propósito de análisis forense en vivo y respuesta a incidentes. Una de las características principales es que, para ejecutar aplicaciones en modo seguro, DART inicia una verificación de integridad antes del inicio de cada programa, de manera que podemos estar 100 % seguros que estamos ejecutando las herramientas de manera segura.

11.1.3. SANS Investigative Forensic Toolkit

SIFT (*SANS Investiative Forensic Tool*) es un grupo de herramientas forenses open source diseñado para realizar exámenes forenses digitales detallados en una variedad de entornos.

La última versión de SIFT dispone de más de 200 herramientas de terceros, puede ejecutarse en cualquier sistema que ejecute un SO Ubuntu o Windows. Entre todas esas herramientas destaca Autopsia, se trata de una herramienta muy famosa utilizada incluso por agencias gubernamentales cuando existe una necesidad de análisis forense. Como es lógico, SIFT establece pautas estrictas sobre cómo se analizan las evidencias, asegura que la evidencia no sea alterada (están en solo modo lectura).

11.1.4. HELIX

Helix es una distribución de Linux enfocada hacía el mundo del análisis forense. La característica principal de esta distribución es que se puede trabajar en entornos Mac, Windows y Linux con una única interfaz.

También contiene diversas aplicaciones de código abierto que permite analizar datos de los contenidos de teléfonos móviles. Helix se trata de una herramienta forense muy robusta capaz de ser ejecutada incluso como sistema operativo, esta permite el análisis de muchos sistemas en vivo.

11.2. Análisis de memoria

Otro tipo de herramienta de análisis son las que se utilizan para el análisis de memoria, a continuación, se exponen los más famosos y utilizados.

11.2.1. Dumplt

Dumplt es una herramienta portátil compacta que facilita guardar el contenido de la RAM a un PC externo. Se trata de un programa por consola muy sencillo de utilizar. Una vez finalizado tendremos junto al ejecutable el archivo de la imagen.

11.2.2. Volatility

Volatility es uno de los mejores programas de software de open source para analizar RAM en sistemas de 32/64 bits, puede analizar volcados sin procesar, volcados de memoria y volcados de VMware. Se trata de un sistema basado en Python ejecutable en sistemas Windows, Linux y Mac.

11.2.3. Memorize

Memorize es un programa de análisis forense que se centra en la captura de memoria RAM en Windows y OSC. También existen herramientas para otras partes del análisis, estas las voy a mencionar a continuación, pero no entrar en explicación de ninguna, ya que hay decenas de aplicaciones para cada tarea, la mayoría open source, esto ha ayudado mucho al avance del análisis forense.

- Herramientas para procesos y servicios:

  -Tasklist.

  -Pslist / Psservice.

  -CurrProcess.

- Usuarios de sistemas:

  -Netusers.

  -PSLoggedon.

  -LogonSessons.

- Análisis de red:

  Wireshark.

  -Snort.

  -Nmap.

  -Xplico.

  -TCPDump.

  -Windump.

- Volcado de disco:
  - -Dd.
  - -WinDD.
  - -CloneZilla.
- Ficheros de sistema:
  - -AnalyzeMFT.
  - -Perfecth Parser.
  - -MBRUtil.
  - -NTFSWalk.
- Análisis de Malware:
  - -OllyDbg.
  - -Radare.

12. Fase 4: Redacción de informes

Esta última fase sirve para redactar los informes que explican y documentan las fases anteriores del evento. Se deberá de describir todo el trabajo realizado, que método se ha seguido y como ha sido y las conclusiones del caso. Para poder escribir toda esta información se deben redactar dos informes, el informe técnico y el informe ejecutivo.

12.1. Informe ejecutivo

Este informe está previsto para ser leído por un lector cuyo nivel de informático es el medio de la población, es decir, bajo. Por lo cual se debe de utilizar un lenguaje mundano y sin tecnicismos. Se debe de evitar utilizar palabras y terminologías específicas de la ingeniería y ciencia forense y explicar el caso y la resolución de una manera que sea entendible para alguien que no es asidua a la informática o que por lo menos no se dedique profesionalmente.
El informe debe de ser un resumen lo más compacto posible de todo el proceso que se ha llevado a cabo.

12.2. Informe técnico

En contraposición, el informe técnico se detalla todos y cada uno de los procesos que se han hecho, también se pueden detallar características del sistema, hardware y software utilizado, técnicas, etc. La finalidad de este informe es poder replicar la investigación solamente leyéndolo. Se trata de un informe mucho más extenso y detallado que el anterior.

13. Caso práctico

Para este caso práctico de análisis forense voy a utilizar una imagen de Windows dentro de una máquina virtual. El programa que utilizaré es VMware Workstation. La imagen de Windows la he obtenido mediante la descarga del archivo .iso en la página oficial de Windows. Debido a que estamos hablando de

un entorno totalmente virtual la fase de identificación, adquisición y preservación de evidencias físicas la omitiré, ya que no tenemos ningún disco físico que analizar.

Antes de entrar en materia debo explicar un término que aún no ha salido en este trabajo y que ayudara a entender este caso práctico.

13.1. Mando y control

Esta infraestructura llamada mando y control se trata de la utilización de elementos para controlar el malware que ha infectado un sistema (un ejemplo de ello sería las botnets antes mencionadas). El uso de este es necesario si se quiere controlar esos sistemas infectados para poder infectar otros sistemas o su robo de información. Es una técnica muy utilizada por los atacantes, ya que te permite poder controlar toda una red de malware y poder trabajar con la información de estos libremente.

Este término será necesario para mi caso. Crearé una infraestructura mando y control muy simplificado y enseñaré que fácil es penetrar en un sistema desactualizado y que podría hacer un atacante incluso siendo novato, también tomaré parte de un equipo de análisis forense y analizaré el sistema dañado como una simulación. Cabe destacar que toda esta práctica se está haciendo en un entorno protegido y el sistema infectado se trata de una máquina virtual arrancada en mi propio ordenador para tener un aislamiento total.

13.2. GCAT un malware backdoor

Para esta práctica utilizaremos el malware Gcat, se trata de un backdoor escrito en Python, este tiene la peculiaridad que utiliza Gmail como servidor de CC (Comando y control). Gracias a su facilidad para infectar como para poder controlar el ordenador infectado me he decidido por este malware. Cabe destacar que un atacante más veterano debería de camuflar este ejecutable en alguien programa legal porque el antivirus de Windows detecta fácilmente este malware, pero independientemente de esto nos servirá para ver cómo sería un ataque de malware.

13.3. Atacante

Una vez tenemos ya todo preparado para infectar el ordenador víctima procedemos a descargarnos el malware de su GitHub oficial. Este está compuesto de diferentes archivos, los más importantes son los dos archivos de Python, gcat.py e implant.py.

Nombre	Fecha de modificación	Tipo	Tamaño
data	16/11/2018 14:43	Carpeta de archivos	
.gitignore	16/11/2018 14:43	Archivo GITIGNORE	1 KB
gcat	16/11/2018 14:43	Python File	11 KB
implant	16/11/2018 14:43	Python File	24 KB
LICENSE	16/11/2018 14:43	Archivo	2 KB
README.md	16/11/2018 14:43	Archivo MD	5 KB

Figura 11: Archivos extraídos del malware Gcat (Fuente:propia).

Una vez extraído debemos de editar el archivo Gcat.py para poner nuestro correo y contraseña para que el script sepa en qué Gmail tendrá que implantar el CC.

Por último, debemos de convertir el archivo de Python implant.py en un .exe para que nuestra víctima lo ejecute y así instalar el backdoor. Como he dicho anteriormente, este archivo debería de ir camuflado dentro de un programa legal o un worm para evitar ser detectado por el radar del antivirus, como nosotros estamos haciendo una simulación simple sobreentenderemos que se trata de un archivo camuflado dentro de un email phishing y la víctima ha caído y ha ejecutado el archivo. Lo primero que hemos hecho como atacantes es comprobar si nuestro usuario ha caído en la trampa, para ello tenemos un comando en el mismo CC que nos permite saber si le hemos conseguido implementar el backdoor a algún dispositivo.

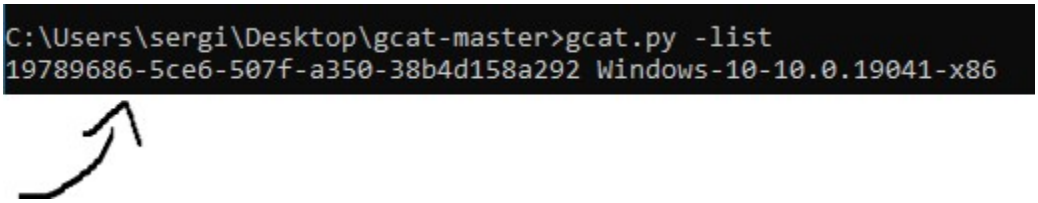


Figura 12: Comando que muestra si algún pc ha ejecutado el archivo malicioso. Aparece el SO del ordenador en cuestión y su UID (Fuente:propia).

Este es el Windows en cuestión que hemos conseguido infectar, con la ID única para poder trabajar con él.

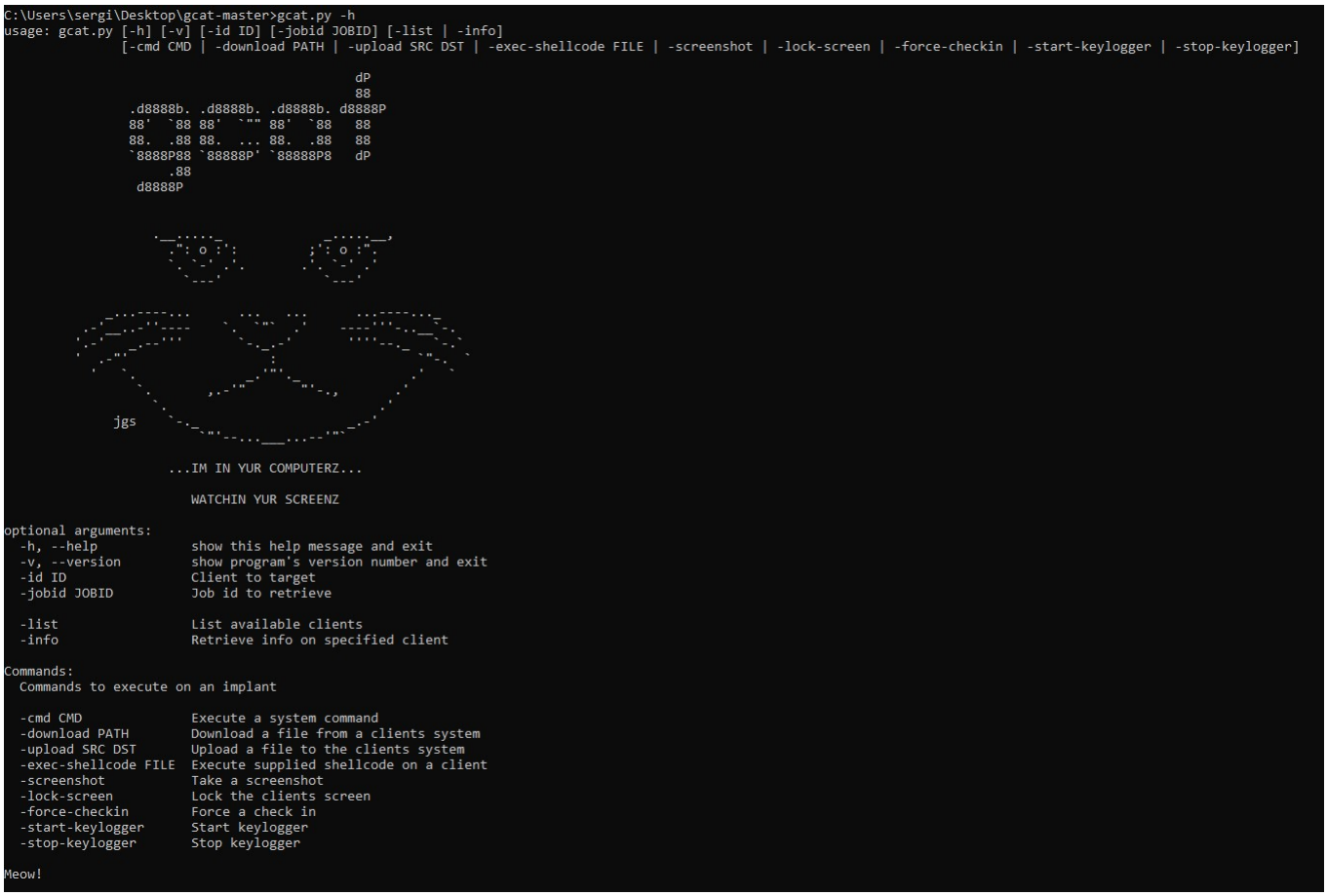


Figura 13: Pantalla inicial del malware donde muestra todos los comandos posibles de actuación (Fuente: propia).

Aquí tenemos el menú por consola del malware, pondré algunos ejemplos de comandos, pero se puede ver que puedes activar la consola del PC infectado, descargar archivos de forma remota y subir archivos, realizar un keylogger, desbloquear el usuario, congelar la pantalla etc. Se puede comprobar unos comandos muy simples la cantidad de daño que le puede provocar a tu PC sin que la víctima se entere.

Lo primero que he hecho ha sido sacar una captura de pantalla para ver que estaba haciendo la víctima en este justo instante.

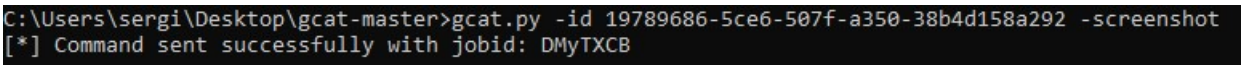


Figura 14: Comando que saca una captura de pantalla del ordenador víctima (Fuente: propia).

Aquí tenemos los comandos necesarios para poder tomar las capturas de pantalla, como podemos ver necesitamos la id del ordenador infectado y una orden. Una vez ha sido realizada el programa nos responde con una id del trabajo.

```
C:\Users\sergi\Desktop\gcat-master>gcat.py -id 19789686-5ce6-507f-a350-38b4d158a292 -jobid DMyTXCB
DATE: 'Sat, 10 Oct 2020 12:10:35 -0700 (PDT)'
JOBID: DMyTXCB
FG WINDOWS: '[u'', u'EL MUNDO - Diario online l\xedder de informaci\xf3n en espa\xf1ol - Google Chrome
Microsoft Store', u'Microsoft Store', u'Configuraci\xf3n', u'Configuraci\xf3n', u'Microsoft Text Input
CMD: 'screenshot'

Screenshot taken

[*] Screenshot saved to ./data/19789686-5ce6-507f-a350-38b4d158a292-DMyTXCB.png
```

Figura 15: Captura de la respuesta del malware (Fuente: propia).

Aquí podemos ver que cuando queremos recuperar el jobID el malware nos responderá con lo que se puede ver en pantalla, que aplicaciones están encendida y que está buscando en el navegador seguido del camino donde esta guardada la foto.

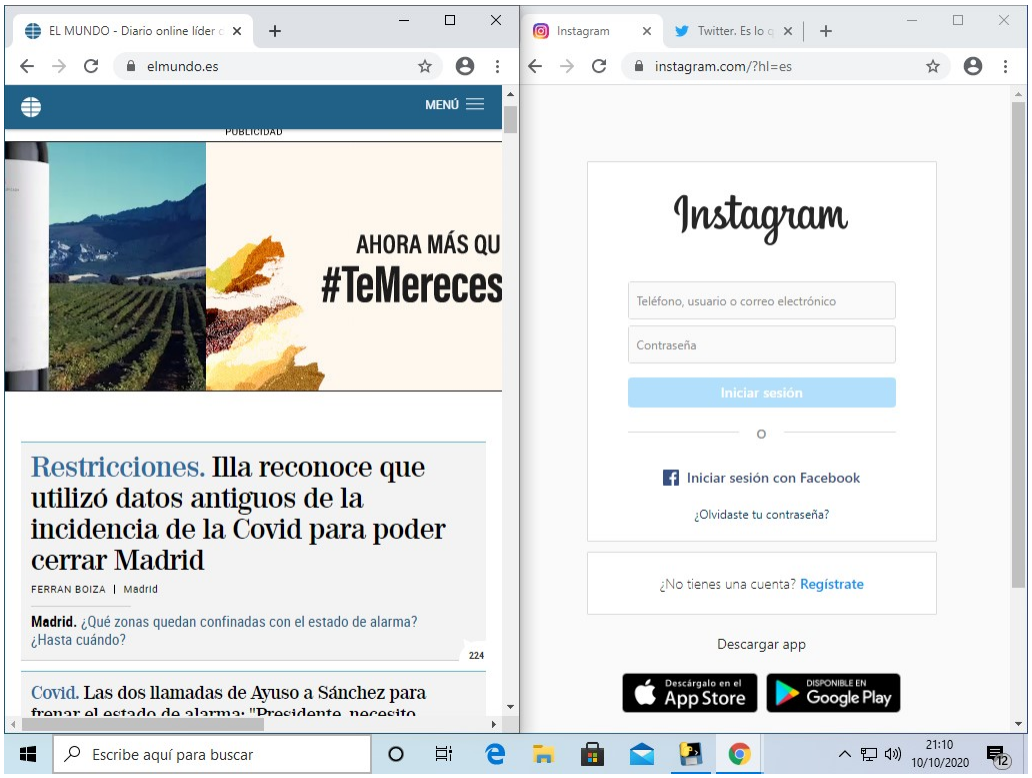


Figura 16: Captura de pantalla realizada por el malware al ordenador víctima (Fuente: propia).

Y aquí tenemos la captura, como se puede ver la privacidad del usuario está totalmente infringida. Y esto no es todo, si vemos que está entrando con contraseñas en sus redes sociales o cuentas bancarias podemos iniciar un keylogger el cual detectara todas las teclas que pulsa el usuario y así podremos extraer toda la información confidencial.

14. Análisis forense de un PC infectado

Iniciaremos este proceso de análisis forense con la única información que se nos ha dado sobre el dispositivo es que se nos ha reportado una posible amenaza desde un sistema donde el usuario ha detectado

un congelamiento extraño de la pantalla y no se sabe a qué se debe.

14.1. Información volátil

Lo primero que se debe de obtener es la fecha y hora del sistema, como hemos dicho anteriormente, primero se debe establecer una línea temporal de los hechos durante la recopilación de evidencias, etc. Para extraer la fecha y hora del sistema utilizaremos PowerShell, se trata de una interfaz de consola segura integrada en el mismo Windows.

Figura 17: Captura del comando para extraer la fecha y la hora del sistema (Fuente: propia).

Se debe comparar la fecha obtenida con el tiempo universal coordinado (UTC) para comprobar si la fecha del sistema es correcta o no, en este caso si es correcta.

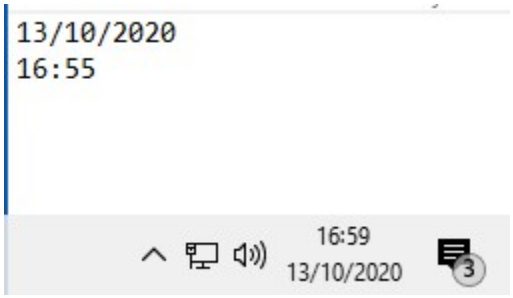


Figura 18: Fecha y hora del inicio del análisis (Fuente: propia).

Una vez extraída la fecha hay que tener presente que los sistemas FAT almacenan valores del tiempo en local del ordenador en cambio los sistemas NTFS los almacenan en formato UTC. Esto significa que dependiendo de la zona horaria donde vivas los FAT tendrán distinto valor en cambio los NTFS no se ven afectado por los cambios.

14.1.1. Volcado de memoria

Esta fase se podría tratar de la más crítica de toda la extracción de información volátil. Un error en el volcado de memoria se podría perder toda pista del ataque y no poder seguir con el proceso de análisis forense. En la memoria se almacena la mayoría de la información necesaria para este proceso por lo que en ella podemos encontrar si hay algún proceso o instrucción extraña que no pertoque.

Para este proceso tenemos que tener en cuenta que hay 2 tipos de memoria: la memoria física y la memoria virtual. La memoria física se refiere a los chips como la memoria RAM y los dispositivos de almacenamiento como los discos duros. En cambio, la memoria virtual se trata de un espacio de memoria creado por el sistema operativo para poder utilizar más memoria que la "físicamente" posible. La memoria virtual normalmente corresponde al fichero de paginación pagefile.sys. La memoria virtual se crea combinando RAM con el espacio del disco duro, eso hace que se puedan ejecutar programas grandes mucho más rápido sin la necesidad de ocupar toda la memoria RAM incluso cuando la memoria

RAM no es suficiente.

Para efectuar el volcado de memoria utilizaremos la aplicación recomendada en este caso Dumplt.

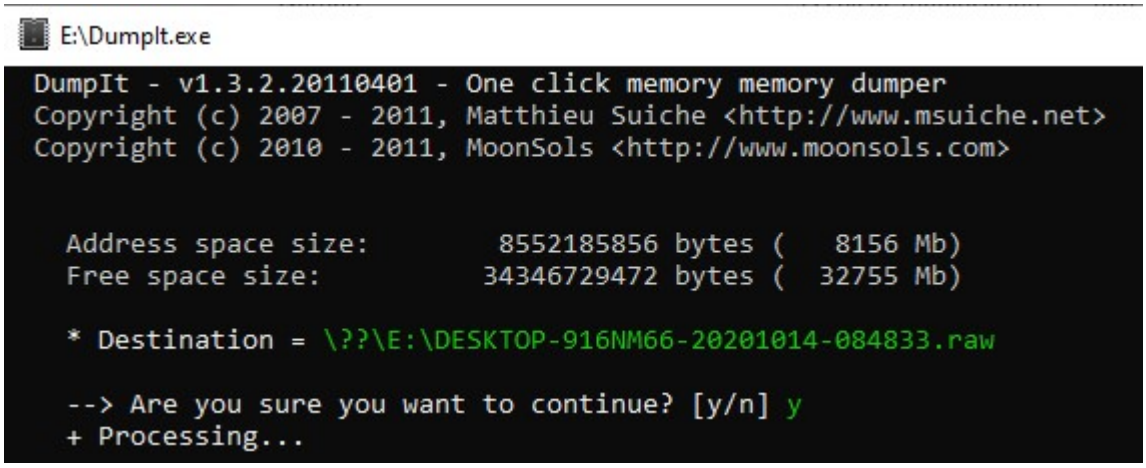


Figura 19: Programa Dumplt para extraer la memoria RAM (Fuente: propia).

Una vez tenemos la imagen del volcado de memoria hemos de guardar su hash para poder realizar comprobaciones a posteriori de que no ha habido ninguna modificación de la imagen, yo extraeré el hash SHA-256. Hay otros tipos de hashes como el MD5, SHA-1... que pese al grado de facilidad de su extracción presenta problemas de colisiones, puede ser que ficheros que son diferentes tengan el mismo MD5 y en estos casos no nos podemos permitir que surja un error así. Para extraer el hash utilizaremos una aplicación llamada HashMyFiles.

Figura 20: Pantalla principal de la aplicación HashMyFiles (Fuente: propia).

Como hemos dicho anteriormente también debemos extraer la memoria virtual que se encontrara en el fichero de paginación pagefile.sys. Para ello como obtendremos una imagen completa del sistema posteriormente ya se incluirá en ella.

14.1.2. Procesos en ejecución

Para obtener los procesos que se están ejecutando en este mismo instante utilizaremos la herramienta PSList para volcar los procesos en un fichero de txt.

```
C:\Users\campe\Downloads\PSTools>pslist64.exe

PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for DESKTOP-916NM66:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   2    0     60     2:23:34.359     1:28:53.678
System                4   8 117 3392    196     0:01:39.843     1:28:53.678
Registry             92   8   4    0   3744     0:00:00.843     1:29:00.701
smss                352  11   2   53   1064     0:00:00.234     1:28:53.558
csrss               476  13  11  503   1720     0:00:01.000     1:28:49.076
csrss               552  13  14  494   1912     0:00:26.781     1:28:48.370
wininit             572  13   1  159   1316     0:00:00.156     1:28:48.362
winlogon            616  13   6  278   2840     0:00:00.375     1:28:48.310
services            692   9   9  648   5052     0:00:05.078     1:28:47.845
lsass               708   9  11 1502   8568     0:00:06.328     1:28:47.549
svchost             824   8   1   54    808     0:00:00.000     1:28:46.030
svchost             844   8  13 1233  10928     0:00:06.625     1:28:45.947
fontdrvhost         864   8   5   32   1264     0:00:00.046     1:28:45.918
fontdrvhost         872   8   5   32   6668     0:00:00.671     1:28:45.918
svchost             956   8  16 1251   8040     0:00:16.140     1:28:45.231
svchost            1008   8   4  253   2188     0:00:01.031     1:28:45.022
dwm                 392  13  16 1054  53156     0:01:41.500     1:28:44.416
svchost            1004   8   1  211   2128     0:00:00.156     1:28:43.765
svchost            1072   8   3  109   1224     0:00:00.031     1:28:43.483
svchost            1080   8   1  146   1776     0:00:00.203     1:28:43.481
svchost            1208   8   2  224   2300     0:00:00.109     1:28:43.280
svchost            1244   8   5  383   5588     0:00:01.937     1:28:43.223
svchost            1264   8   6  249   3276     0:00:00.406     1:28:43.172
svchost            1312   8   9  310   3156     0:00:01.187     1:28:42.939
svchost            1336   8   7  393  14004     0:00:00.625     1:28:42.864
svchost            1396   8   5  220   2620     0:00:04.218     1:28:42.546
svchost            1404   8   3  183   1292     0:00:00.046     1:28:42.546
svchost            1416   8   8  173   2040     0:00:00.234     1:28:42.543
svchost            1496   8   4  136   3952     0:00:00.281     1:28:42.388
svchost            1532   8   2  169   1784     0:00:00.062     1:28:42.366
svchost            1540   8   6  223   2080     0:00:00.453     1:28:42.360
svchost            1584   8   2  168   1664     0:00:00.109     1:28:42.229
svchost            1592   8   6  151   1720     0:00:00.312     1:28:42.229
```

Figura 21: Aplicación PSList (Fuente: propia).

Como siempre, extraemos el hash del archivo para asegurar que no ha habido ninguna modificación a posteriori.

14.1.3. Servicios en ejecución

Con los servicios podemos obtener información sobre aplicaciones que se han instalado o procesos recurrentes.

```
C:\Users\campe\Downloads\PSTools>PSservice64.exe

PsService v2.25 - Service information and configuration utility
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: AJRouter
DISPLAY_NAME: Servicio de enrutador de AllJoyn
Enruta los mensajes AllJoyn de los clientes AllJoyn locales. Si este servicio se interrumpe, los clientes AllJoyn que no teng
an sus propios enrutadores integrados no podrán ejecutarse.
        TYPE               : 20 WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
                             (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms

SERVICE_NAME: ALG
DISPLAY_NAME: Servicio de puerta de enlace de nivel de aplicación
Proporciona compatibilidad entre los complementos de protocolo de terceros y la Conexión compartida a Internet
        TYPE               : 10 WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
                             (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms

SERVICE_NAME: AppIDSvc
DISPLAY_NAME: Identidad de aplicación
Determina y comprueba la identidad de una aplicación. Si se deshabilita este servicio, no se aplicará AppLocker.
        GROUP              : ProfSvc_Group
        TYPE               : 20 WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
                             (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms
```

Figura 22: Terminal ejecutando la aplicación PSService que muestra los servicios en ejecución (Fuente: propia).

14.1.4. Usuarios que han iniciado sesión y listado de usuarios

En los sistemas de mando y control es posible que mediante un movimiento lateral se hayan conseguido crear usuarios con privilegio sin que la víctima se haya enterado y así poder controlar y utilizar fraudulentamente el PC. Por eso miraremos una lista de usuarios que se han loggeado recientemente en el PC y la lista de usuarios creados. Para ello utilizaremos la aplicación PSLoggedOn.

```
C:\Users\campe\Downloads\PSTools>PSLoggedon.exe

PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     17/10/2020 11:27:33        DESKTOP-916NM66\campe

No one is logged on via resource shares.
```

Figura 23: Lista de usuarios logueados (Fuente: propia).

14.1.5. Red

Debemos de comprobar si hay alguna comunicación extraña que nos de pistas sobre el ataque, para ello extraeremos los datos de nuestro equipo mediante el comando ipconfig.

```
C:\Users\campe\Downloads\PSTools>ipconfig /all

Configuración IP de Windows

   Nombre de host. . . . . . . . . . : DESKTOP-916NM66
   Sufijo DNS principal  . . . . . . :
   Tipo de nodo. . . . . . . . . . . : híbrido
   Enrutamiento IP habilitado. . . . : no
   Proxy WINS habilitado . . . . . . : no
   Lista de búsqueda de sufijos DNS: localdomain

Adaptador de Ethernet Ethernet0:

   Sufijo DNS específico para la conexión. . : localdomain
   Descripción . . . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Dirección física. . . . . . . . . . . . . : 00-0C-29-53-10-B3
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::451a:d12b:aab6:a374%14(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.19.128(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : sábado, 17 de octubre de 2020 11:27:21
   La concesión expira . . . . . . . . . . . : sábado, 17 de octubre de 2020 12:42:22
   Puerta de enlace predeterminada . . . . . : 192.168.19.2
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.19.254
   IAID DHCPv6 . . . . . . . . . . . . . . . : 100666409
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-27-0F-8E-AB-00-0C-29-53-10-B3
   Servidores DNS. . . . . . . . . . . . . . : 192.168.19.2
   Servidor WINS principal . . . . . . . . . : 192.168.19.2
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

Figura 24: Configuración de la red de nuestro ordenador infectado (Fuente: propia).

14.1.6. Conexiones Establecidas

Debemos de comprobar si hay alguna actividad oculta en las conexiones de red para ver si el malware que ha atacado al equipo está comunicándose con el atacante o nos han insertado una puerta trasera que está inactiva esperando a una comunicación.

Para ello utilizaremos NetBIOS (*Network Basic Input/Output System*) es una especificación de interfaz para acceso a servicios red, es decir, se trata de una capa de software desarrollado para enlazar en un sistema operativo de red con hardware específico. Normalmente funciona sobre TCP/IP, con esto comprobaremos que otros equipos están dentro del radio de acción y si se han buscado otros objetivos para expandir el malware.

También cuenta con una tabla de ficheros transferidos por este protocolo, con esto podremos comprobar si ha habido un esparcimiento de la amenaza por otro el sistema.

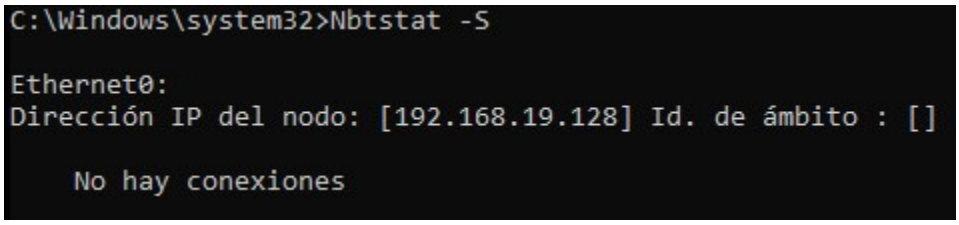


Figura 25: Conexiones establecidas (Fuente: propia).

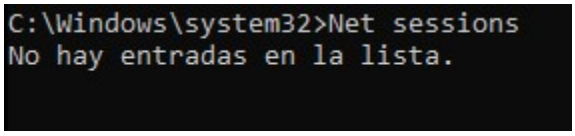


Figura 26: Sesiones establecidas (Fuente: propia).

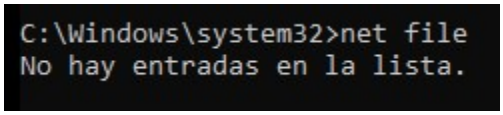


Figura 27: Ficheros transferidos (Fuente: propia).

14.1.7. Conexiones activas y puertos activos

Buscaremos puertos que estén escuchando y que sean extraños ya que podrían ser un acceso remoto.Para obtener el listado de conexiones activas utilizaremos el comando netstat.

```
C:\Windows\system32>netstat -an | findstr /i "state listening established"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    192.168.19.128:139     0.0.0.0:0              LISTENING
  TCP    192.168.19.128:50086   192.168.1.41:445       ESTABLISHED
  TCP    192.168.19.128:50183   40.67.251.132:443      ESTABLISHED
  TCP    192.168.19.128:51011   52.184.217.37:443      ESTABLISHED
  TCP    192.168.19.128:51017   52.184.213.21:443      ESTABLISHED
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:7680              [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49669             [::]:0                 LISTENING
```

Figura 28: Conexiones activas y puertos activos (Fuente: propia).

14.1.8. Contenido de la caché DNS

El protocolo DNS (*Domain Name System*) permite asociar direcciones IP con nombres de dominio ya que éstos últimos son más sencillos de recordar. En la caché DNS se puede visualizar dicha asociación con respecto a los dominios a los que se ha accedido desde el equipo. Para extraer dicha información utilizaremos el comando ipconfig.

```
C:\Windows\system32>ipconfig /displaydns

Configuración IP de Windows

    smtp.gmail.com
    ----------------------------------------
    Nombre de registro  . : smtp.gmail.com
    Tipo de registro  . . : 1
    Período de vida . . . : 5
    Longitud de datos . . : 4
    Sección . . . . . . . : respuesta
    Un registro (host). . : 74.125.133.108
```

Figura 29: Terminal que muestra el caché DNS (Fuente: propia).

14.1.9. ARP caché

La tabla ARP se encarga de almacenar la relación entre la dirección física (MAC) y la dirección lógica (IP) de todos los equipos con el que se haya comunicado este ordenador.

Se trata de una información muy volátil y si no ha habido comunicación en mucho tiempo no queda rastro de la misma.

```
C:\Windows\system32>arp -a

Interfaz: 192.168.19.128 --- 0xe
  Dirección de Internet          Dirección física      Tipo
  192.168.19.2          00-50-56-f0-6a-c5     dinámico
  192.168.19.254        00-50-56-e4-ef-7d     dinámico
  192.168.19.255        ff-ff-ff-ff-ff-ff     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

Figura 30: Tabla de dirección física y lógica de todos los equipos que se ha comunicado el ordenador (Fuente: propia).

14.1.10. Tráfico de red

Conviene capturar el tráfico de la red durante un lapso de tiempo para ver si el malware ha generado tráfico o conexiones con el servidor CC etc.

14.1.11. Registros de Windows

El registro de Windows es donde se guarda la información sobre configuraciones y ajustes básicos del sistema operativo. También almacena y centraliza datos sobre programas, dispositivos, usuarios y hardware.

Todo lo que está configurado en el equipo tiene una entrada de registro asociada. Cuando se instala un programa nuevo, este se añade al registro de Windows un nuevo set de instrucciones y archivos además de información adicional, es decir, todo lo que pasa en el ordenador queda registrado dentro de los registros de Windows. El registro está compuesto por distintos valores de registro (instrucciones).

Para hacer este análisis utilizaremos Autoruns de Sysinternals, este nos muestra información como las aplicaciones que se ejecutan al inicio de arrancar el SO, tareas que ya están programadas etc.

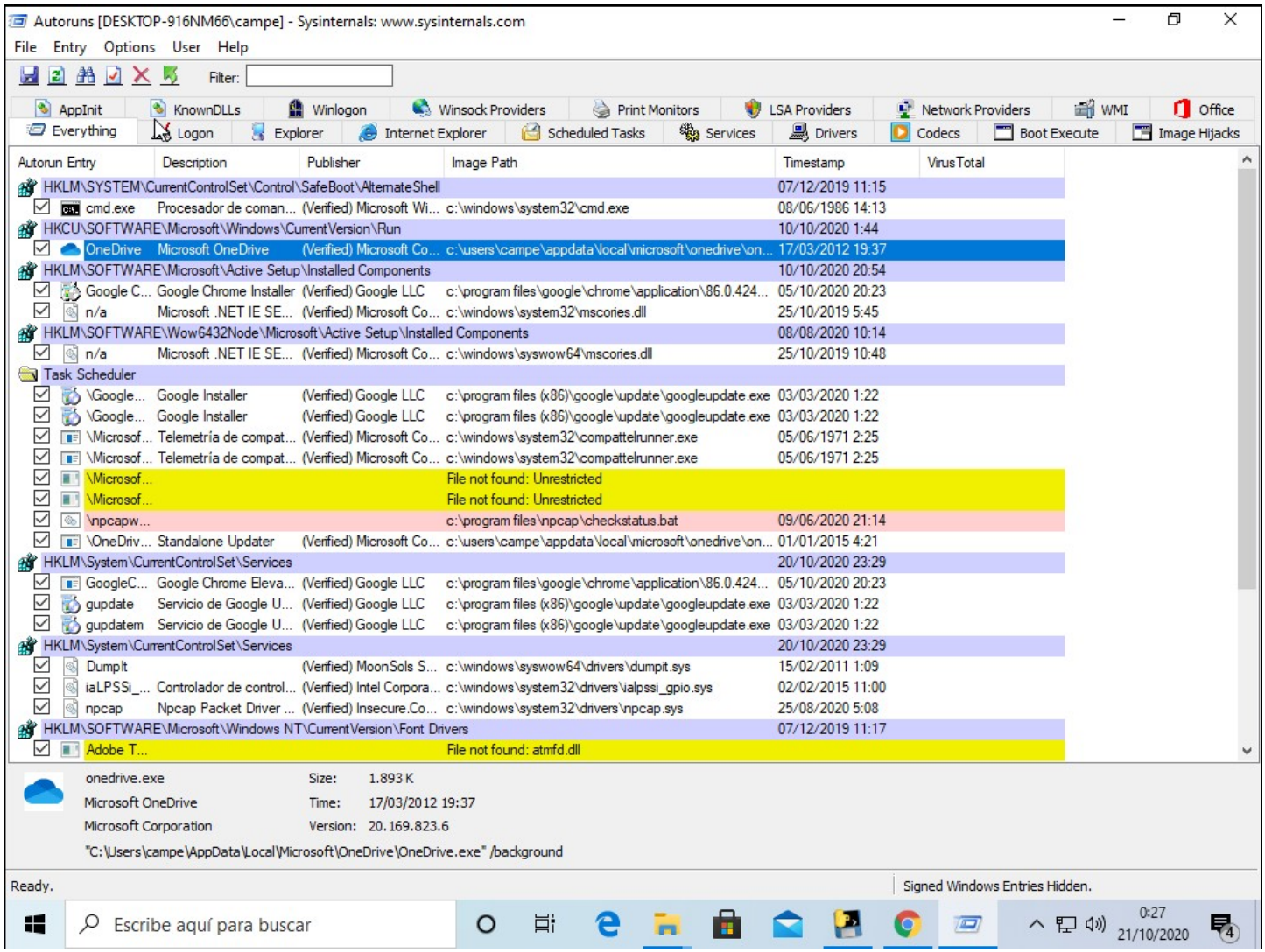


Figura 31: Pantalla principal de autoruns (Fuente: propia).

14.1.12. Asociaciones de ficheros con depuradores

En el registro de Windows hay una serie de entradas gracias a las cuales se puede indicar al SO que abra un programa listo para ser depurado. Existe malware que utiliza estas entradas para poder ejecutarse automáticamente sin que la víctima lo sepa, para comprobar si ha sido el caso vamos a exportar la entrada de registro correspondiente.

Dicha entrada se encuentra en `Equipo\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\NT\CurrentVersion\Image\File\Execution\Options`

14.1.13. MUICache

Cada vez que un usuario ejecuta por primera vez un programa se almacena en el registro una entrada que guarda el nombre del programa, para comprobar si ha habido alguna ejecución de un programa malicioso exportaremos el registro.

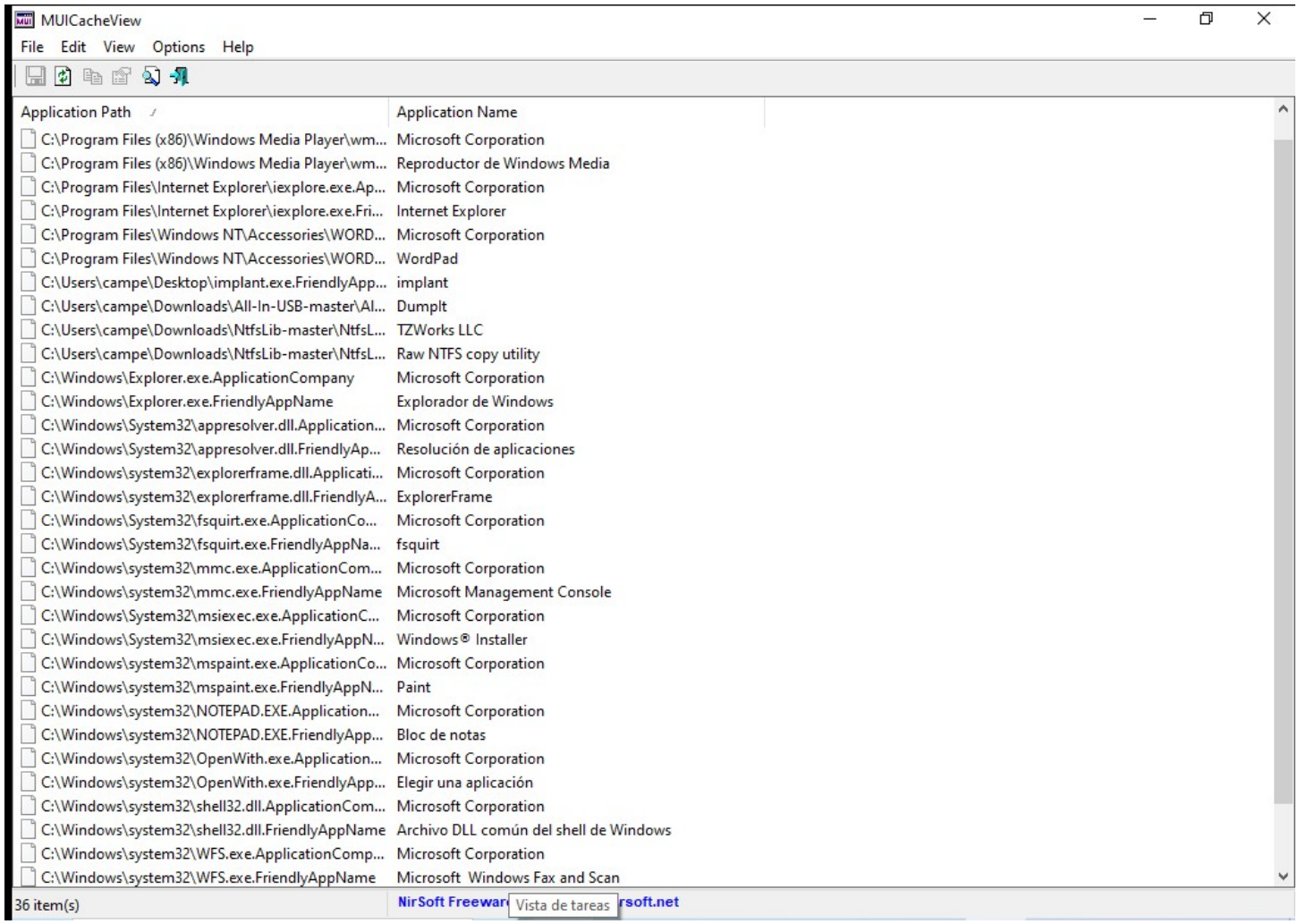


Figura 32: Programas registrados en la MUICache (Fuente: propia).

14.1.14. Ficheros abiertos recientemente

En los registros también se guarda una entrada llamada RecentDocs donde almacena el listado de ficheros abiertos recientemente.

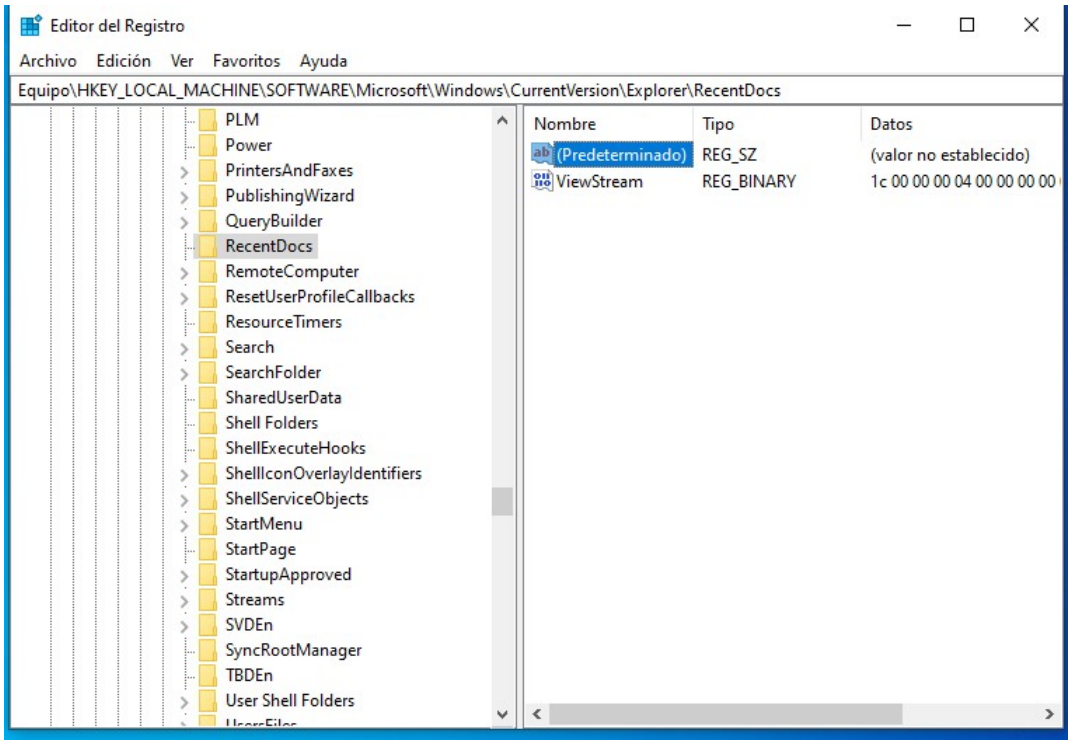


Figura 33: Menu del Editor de Registro con los ficheros reciente (Fuente: propia).

14.1.15. Contraseñas

Otra cosa que debemos de comprobar en un análisis forense son los diferentes nombres de usuario y las contraseñas almacenadas de esto. Existen multitud de contraseñas que pueden estar almacenadas y comprometidas por culpa del ataque. Contraseñas tales como banca online, correo electrónico, servicios de compra-venta, etc. Podemos utilizar programas como WebBrowserPassView o Network Password Recovery.

Como esta máquina virtual se ha creado desde cero no extraeremos ninguna información.

14.1.16. Árbol de directorios y ficheros

Puede resultar interesante conocer el árbol de directorios y ficheros con el fin de poder comprobar la existencia de ficheros sospechosos. Para esto extraeremos tres listados de ficheros mediante los tiempos MAC (Modificación, Acceso, Creación).

```
C:\Users\campe>dir /t:c /a /s /o:d c:\ > "C:\Users\campe\ListadoFicherosPorFechaDeCreacion-%date:~-4,4%%date:~-10,2%%date:~-7
,2%_%time:~3,2%%time:~6,2%.txt"

C:\Users\campe>dir /t:w /a /s /o:d c:\ > "C:\Users\campe\ListadoFicherosPorFechaDeModificacion-%date:~-4,4%%date:~-10,2%%date
:~-7,2%_%time:~3,2%%time:~6,2%.txt"

C:\Users\campe>dir /t:a /a /s /o:d c:\ > "C:\Users\campe\ListadoFicherosPorUltimoAcceso-%date:~-4,4%%date:~-10,2%%date:~-7,2%
_%time:~3,2%%time:~6,2%.txt"
```

Figura 34: Extracción de los ficheros por consola mediante los tiempos MAC (Fuente: propia).

14.2. Información no volátil

Una vez hemos recopilado toda la información volátil necesaria ahora vamos a trabajar en el disco duro. Para ello vamos a tomar una imagen forense del equipo y así hacemos una copia exacta de toda la información de este por si trabajando se puede corromper y así todos los estudios se hacen sobre el disco copiado y no directamente sobre el equipo que está corrompido.

14.2.1. Copia disco duro

Dependiendo de qué proceso y del tiempo que deseas invertir hay tres tipos de volcado de disco disponibles.

- Crear una copia bit stream de disco a imagen: se trata del método más habitual y más rápido. Este es el método que utilizaremos en este análisis forense, este método permite realizar tantas copias como sea necesario de una manera fácil y sencilla.
- Crear una copia bit stream de disco a disco: en este método también se pueden realizar tantas copias como discos dispongamos, como clonamos directamente a un disco conlleva mayor fiabilidad y rapidez.

  Para este tipo de copiado hay que tener en cuenta que tipo de hardware utilizaremos, si un (SSD) Solid State Drive o un disco magnético ya que los SSD no funcionan de la misma manera que estos. El comando TRIM de los discos SSD puede ser un quebradero de cabeza para los novatos en análisis forense, es posible que no conozcan ni de su existencia, se trata de un comando implementado por los fabricantes para alargar la vida útil y el rendimiento de los discos SSD. Este comando permite informar que celdas ya no están en uso al controlador y notifica al recolector de basura que borre electrónicamente el contenido de esas celdas para evitar que se esté guardando una información que no va a ser utilizada para así evitar un desgaste innecesario de las celdas. Este proceso de eliminación de información es automático siempre y cuando el comando TRIM este activado lo que significa que si algún usuario quiere borrar un fichero para eliminar su rastro del análisis y el comando TRIM está en funcionamiento la evidencia desaparecerá para siempre y no quedará rastro de su borrado. Este comando TRIM puede ser desactivado, pero se trata de una función que se desconoce ya que todo el proceso que desencadena corre en segundo plano para evitar que el usuario vea o intente tocar cosas que no sabe lo que son. Solo nos daríamos cuenta de la modificación del disco a la hora de sacar el hash y compararlo con el original.
- Creación de una copia de datos dispersos de una carpeta o archivo: este tipo de copia es la menos recomendable si quieres hacer un análisis forense extenso ya que no sabes la procedencia del ataque ni que tipo es, se realiza una copia selectiva de los ficheros que interesan investigar. Se trata de una técnica muy específica a esos casos y no es necesario volcar todo el disco.

Como hemos dicho antes nosotros utilizaremos la primera opción. Para ello conectaremos un disco duro externo extraíble donde copiaremos la imagen y tenemos nuestro programa de copia. Existen varios software de pago y libres como por ejemplo EnCase.

Utilizaremos la aplicación FTK Imager, en su interfaz gráfica encontraremos una opción para poder crear una imagen del disco y almacenarla como evidencia.

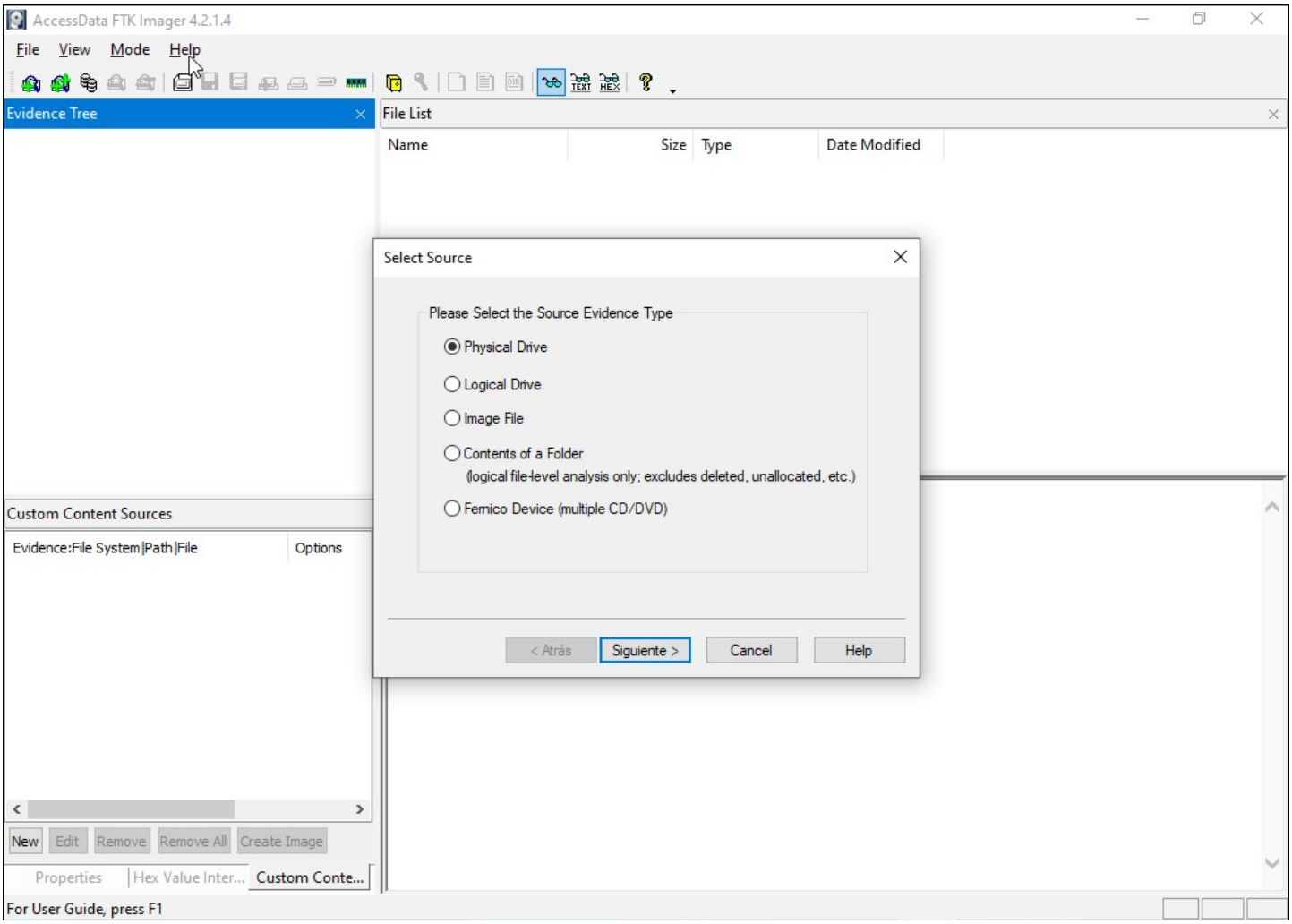


Figura 35: Programa FTK Imager para hacer una copia bit a bit del disco duro (Fuente: propia).

Escogeremos la partición para la creación de la máquina virtual.

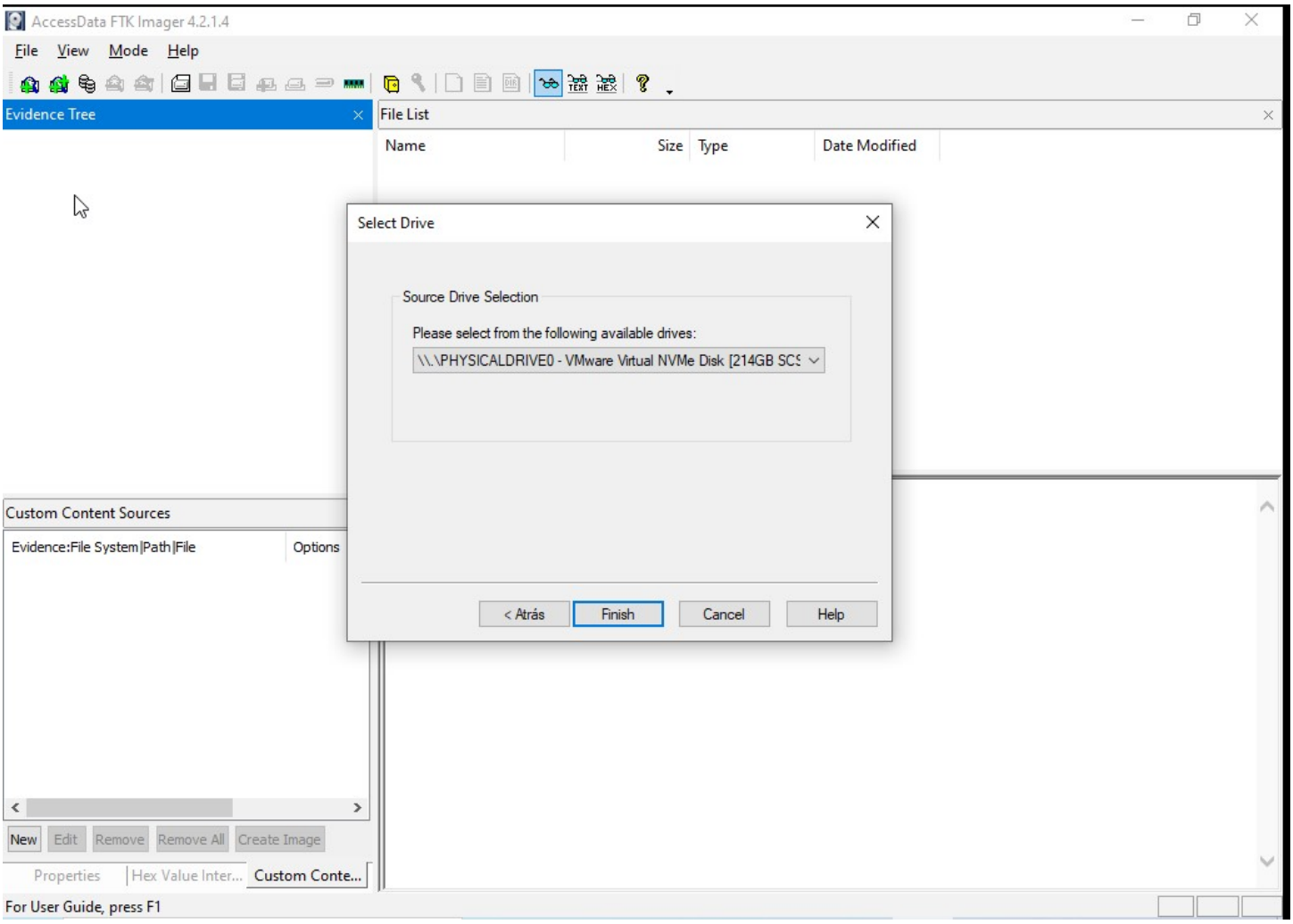


Figura 36: Programa FTK Imager para hacer una copia bit a bit del disco duro (Fuente: propia).

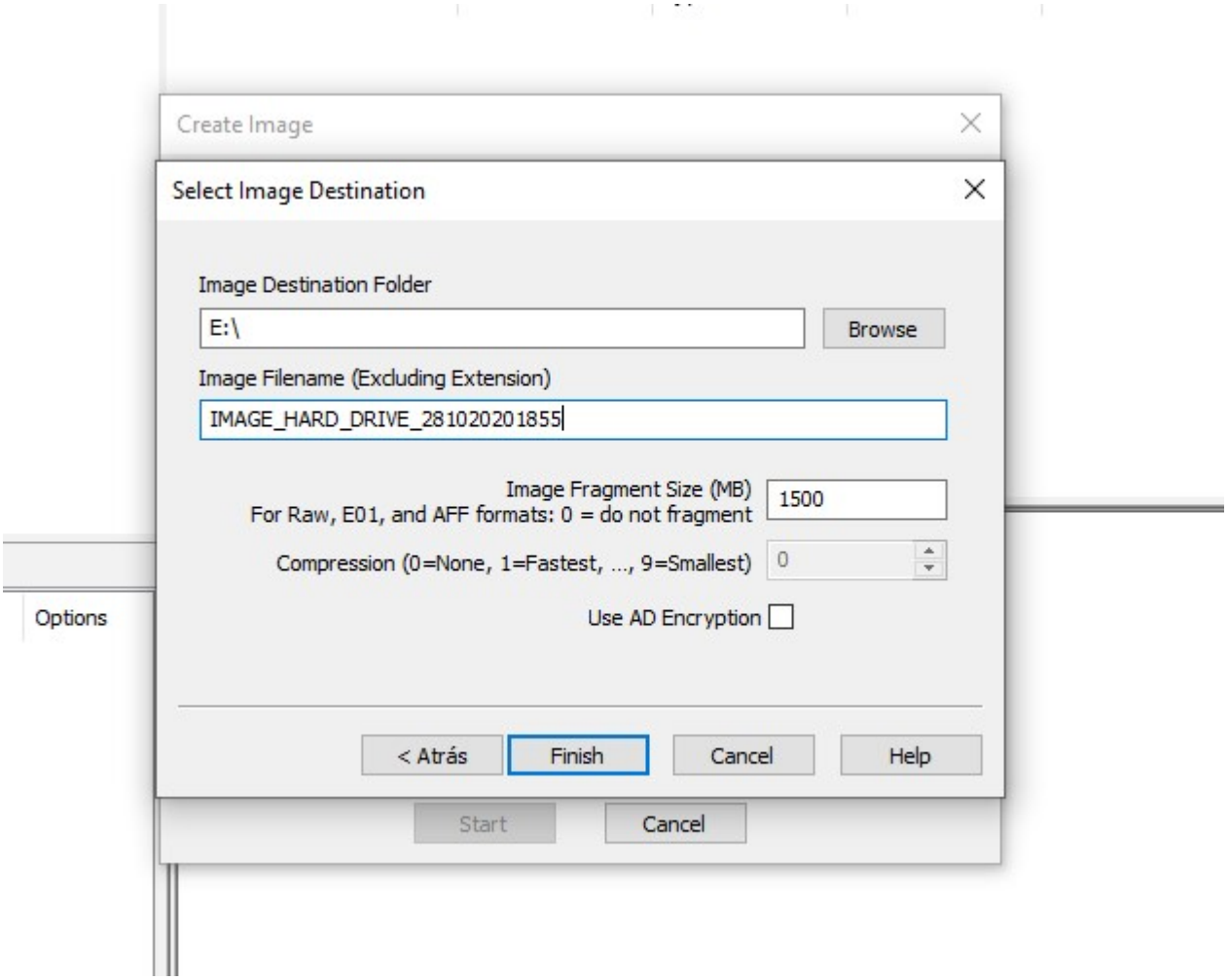


Figura 37: Escogemos el nombre de la imagen y donde estará destinada (Fuente: propia).

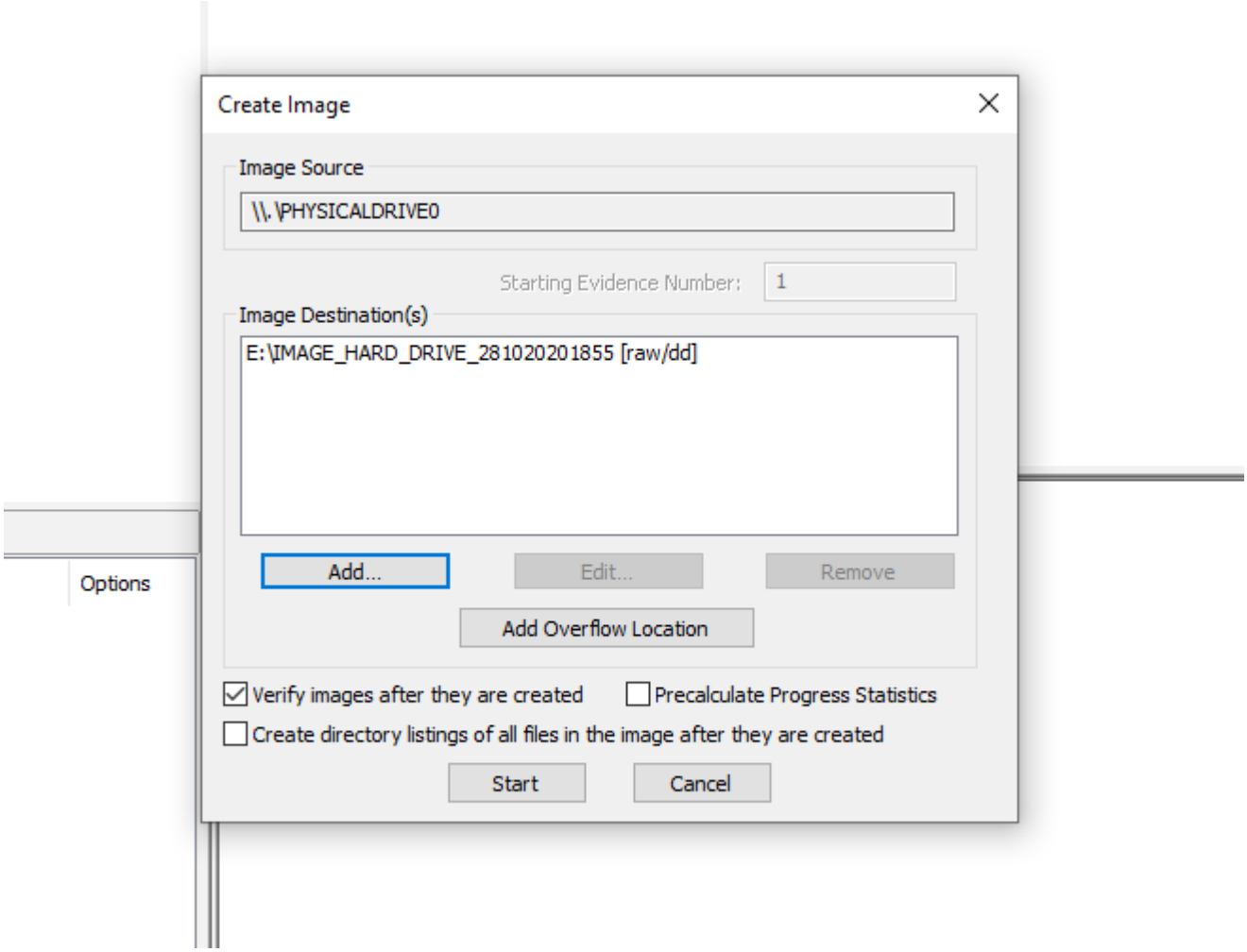


Figura 38: Añadimos la imagen a copiar (Fuente: propia).

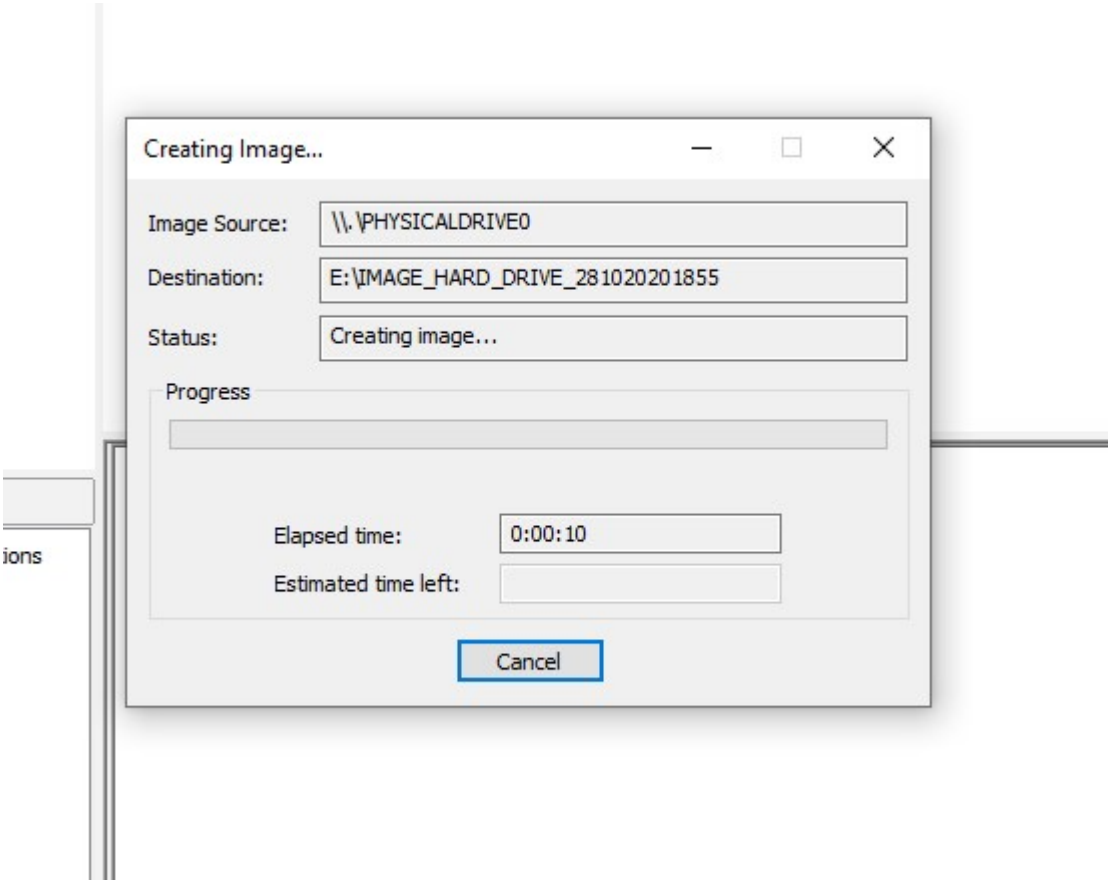


Figura 39: Se copia la imagen bit a bit (Fuente: propia).

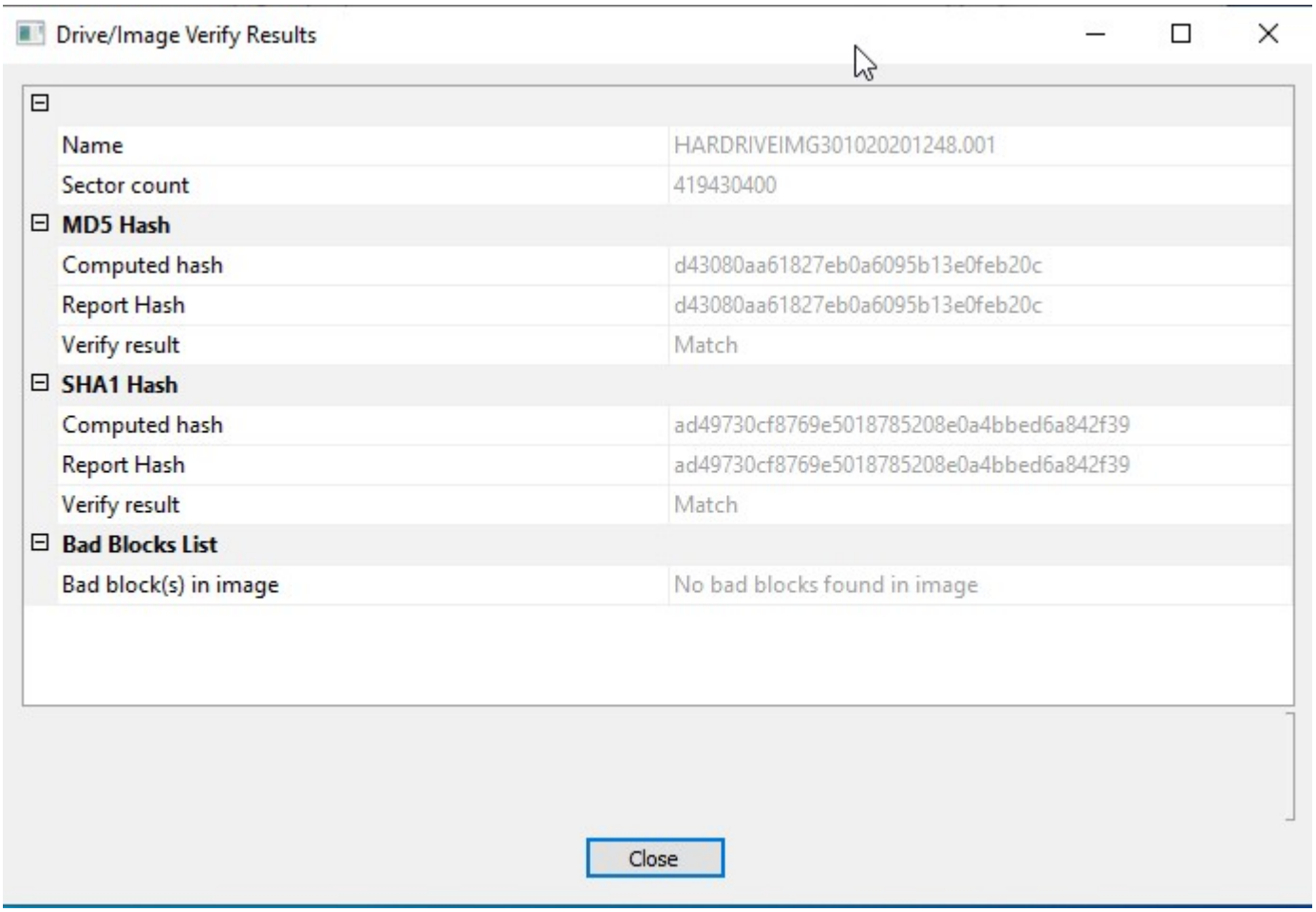


Figura 40: Se comparan los dos hashes (original y copia) (Fuente: propia).

El mismo programa ya te da la opción de calcular si es el mismo valor hash que el disco original como se puede ver en la siguiente captura.

Una vez tenemos una copia bit a bit de nuestra imagen es el momento de desconectar el disco duro del dispositivo y trabajar solamente con la imagen, en nuestro caso cargaremos esta imagen en un laboratorio seguro para evitar una infección en nuestro sistema principal. Con esta imagen podremos empezar a investigar ese disco duro sin perder datos en el original. Como nosotros trabajamos con una máquina virtual, crearemos una nueva cargando el contenido del disco duro a investigar. Cabe destacar que en nuestro caso podríamos cargar una snapshot antigua en caso de una perdida de datos por un error en la investigación, pero he querido intentar acercarme a un caso real lo más posible y "simular" lo que sería añadir un disco duro infectado en un entorno seguro y aislado.

14.2.2. Master Boot Record (MBR)

El MBR o master boot record es el primer sector físico de un dispositivo de almacenamiento de datos, se utiliza para iniciar los PC. Posee un tamaño de 512 bytes y almacena información general del sistema a iniciar, como se inicia este sistema, que tipo de particiones hay, que tamaño tiene esas particiones.

El MBR se puede encontrar en casi todos los medios de almacenamiento externo y, obviamente, en los discos duros internos de nuestro ordenador. Siempre consta de al menos cuatro componentes:

- Programa de inicio (bootloader).
- Soporte de datos, firma de disco.
- Tabla de particiones maestra.
- MBR o firma de arranque

El programa de inicio se encuentra en los primeros 446 bytes del MBR. El software se activa cuando se arranca el PC e inicia el proceso de arranque a nivel operativo. Esto pone en funcionamiento una rutina más extensa con pasos de procesamiento estandarizados que culmina con el SO listo para el uso del usuario.

Aunque en este análisis no es el caso, existen malwares como el famoso ransomware Petya que su ataque principal reside en el MBR del ordenador de la víctima. Este obliga al equipo a reiniciarse y simula una pantalla de aviso de Windows donde dice que el disco ha sido dañado y se está reparando cuando en realidad lo que está haciendo es encriptar los datos. Un ataque a la MBR puede ser muy peligroso ya que puede incluso evitar que se encienda el dispositivo lo que podría suponer una pérdida total de toda la información volátil, los registros etc.

Para asegurarnos de que nuestro atacante no reside en la MBR o si hay alguna partición oculta en el disco duro, la exportaremos con la herramienta MBRutil para más tarde investigarlo.

14.2.3. Master File Table

La Master File Table es una tabla que almacena información relevante de todos los ficheros y carpetas de una unidad o disco. Hay al menos una entrada en la MFT para cada archivo en un volumen del sistema de archivos NTFS incluida la MFT en sí.

La tabla de archivos maestra asigna una cierta cantidad de espacio para cada registro de archivo. Los atributos de un archivo se escriben en el espacio asignado de la MFT. Contiene información del archivo, nombre, tamaño, fecha, hora, o permisos. Para extraer la MFT utilizaremos el programa Mft2csv.

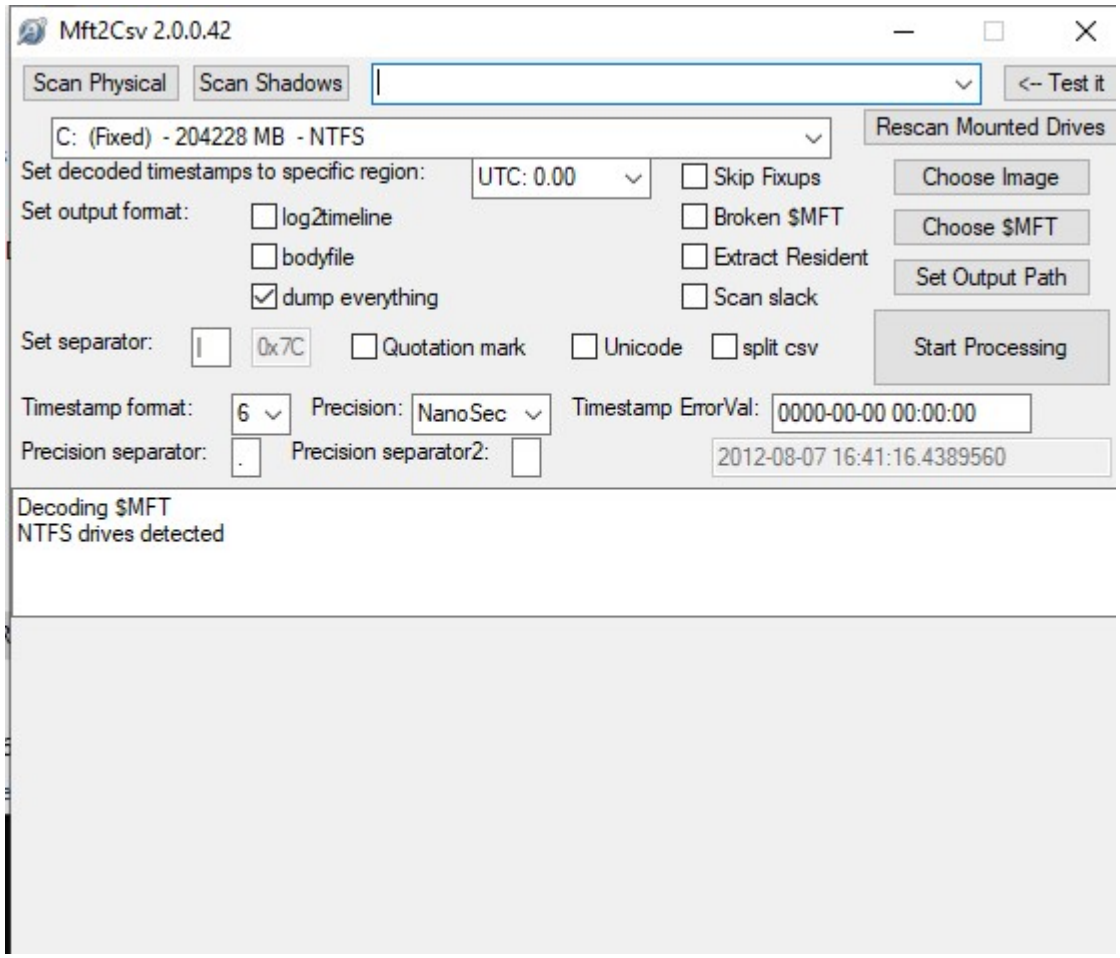


Figura 41: Pantalla principal del programa Mft2csv (Fuente: propia).

14.2.4. Información del sistema

El propio SO nos puede dar diferente información interesante acerca del hardware, software, actualizaciones o tiempos de actividad. Para ello utilizaremos la herramienta systeminfo:

```
E:\>systeminfo > "InformacionDelSistema-%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Figura 42: Comando para extraer la información del sismtema (Fuente: propia).

En el fichero encontraremos esto:

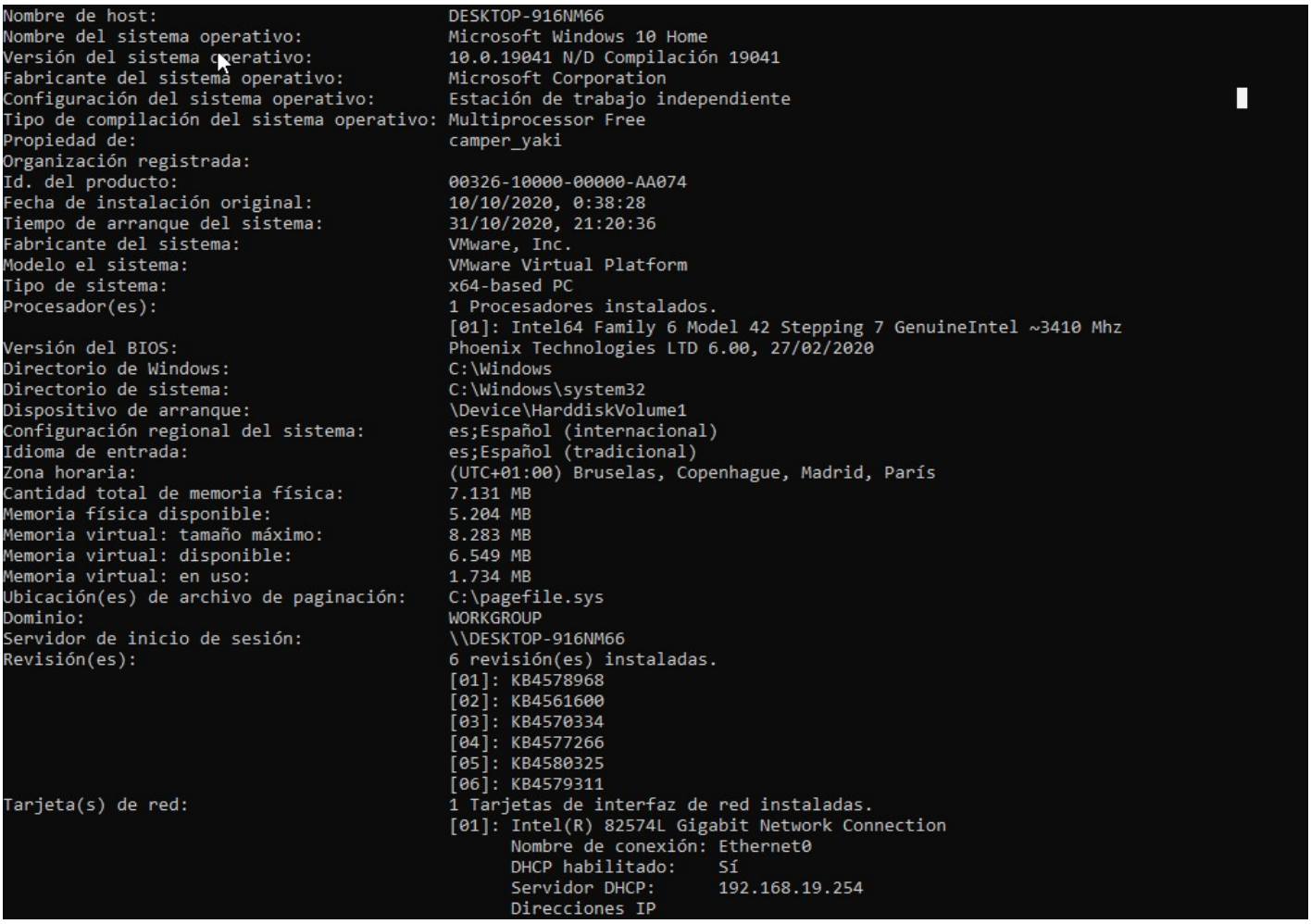


Figura 43: Información del ordenador infectado (Fuente: propia).

14.2.5. Tareas Programadas

En algunos casos la intrusión con un backdoor o un malware puede crear una tarea programada para asegurarse que su aplicación va a estar ejecutándose en todo momento. Por ello vamos a revisar las tareas programadas mediante el comando schtasks.

```
Carpeta: \
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== ==============
OneDrive Standalone Update Task-S-1-5-21 01/11/2020 19:37:14    Listo

Carpeta: \Agent Activation Runtime
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== ==============
S-1-5-21-3203403749-2385085536-422303527 N/A                    Deshabilitado

Carpeta: \Microsoft
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== ==============
Información: no hay tareas programadas disponibles actualmente para el nivel de acceso.

Carpeta: \Microsoft\OneCore
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== ==============
Información: no hay tareas programadas disponibles actualmente para el nivel de acceso.

Carpeta: \Microsoft\Windows
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== ==============
Información: no hay tareas programadas disponibles actualmente para el nivel de acceso.

Carpeta: \Microsoft\Windows\.NET Framework
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== ==============
.NET Framework NGEN v4.0.30319           N/A                    Listo
.NET Framework NGEN v4.0.30319 64        N/A                    Listo
.NET Framework NGEN v4.0.30319 64 Critic N/A                    Deshabilitado
.NET Framework NGEN v4.0.30319 Critical  N/A                    Deshabilitado

Carpeta: \Microsoft\Windows\Active Directory Rights Management Services Client
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== ==============
AD RMS Rights Policy Template Management N/A                    Deshabilitado
AD RMS Rights Policy Template Management N/A                    Listo

Carpeta: \Microsoft\Windows\AppID
Nombre de tarea                          Hora próxima ejecución Estado
======================================== ====================== ==============
PolicyConverter                          N/A                    Deshabilitado
VerifiedPublisherCertStoreCheck          N/A                    Deshabilitado
```

Figura 44: Tareas programas en el ordenador infectado (Fuente: propia).

14.2.6. Variables de entorno

Una variable de entorno se trata de una variable dinámica que puede afectar al comportamiento de los procesos en ejecución de un ordenador.

Ejemplos como %USERPROFILE% son una variable de entorno, es decir una cadena de texto que sistemas operativos como Windows, Linux o Mac utilizan para almacenar valores que pueden variar de un equipo a otro. Normalmente en estos valores hacen referencia a archivos, directorios y funciones comunes del sistema cuya ruta concreta puede variar. El ejemplo USERPROFILE es simple, aun sin saber el nombre del usuario le estás diciendo que quieres acceder al usuario entonces dependiendo de que ordenador o que usuario estas logeado el valor de esa variable cambiara.

```
C:\Users\campe\Desktop>path > "VariablesDeEntorno-%date:~-4,4%%date:~
-10,2%%date:~-7,2%_%time:~0,2%%time:~3,2%%time:~6,2%.txt"
```

Figura 45: Comando para guardar las variables de entorno en un fichero .txt (Fuente: propia).

14.2.7. Logs del sistema

Los logs son ficheros de texto que almacenan información relevante como conexiones remotas, eventos del sistema, etc. Existen varios que son de gran interés forense y que deben de ser recopilados.

14.2.8. Windows Event Logs

Dentro de los logs de eventos de Windows hay 3 que tienen especial importancia:

- AppEvent.evt(x): registra los sucesos relativos a aplicaciones.
- SysEvent.evt(x): registra los sucesos relativos al sistema.
- SecEvent.evt(x): registra los sucesos relativos a la seguridad.

Para exportarlos utilizaremos la función wevtutil que viene incorporada en Windows.

14.2.9. Carpeta prefetch

En esta carpeta se almacenan los programas que se abren habitualmente y es utilizada por el sistema operativo para cargarlos en memoria con una mayor rapidez. Cada programa utilizado habitualmente tiene asociado un fichero con extensión PF que almacena todo tipo de información del ejecutable, tal como su nombre, el número de veces que se ha ejecutado, librerías, etc.

Para ello utilizaremos una herramienta llamada WinPrefetchView.

14.2.10. Ficheros hosts

Si sospechamos de actividades de malware debemos de sopesar que la víctima ha ejecutado algún fichero que posiblemente no esté firmado, por ello para acotar la búsqueda de los archivos ejecutables que pueden contener un malware podemos buscar ejecutables no firmados mediante el uso de Sigcheck que viene dentro de la carpeta de utilidades de SysInternals.

Consultar este fichero ayuda a aclarar si el malware modifica el fichero hosts con el fin de impedir que el usuario pueda acceder a ciertas páginas web, principalmente aquellas destinadas a la seguridad del ordenador.

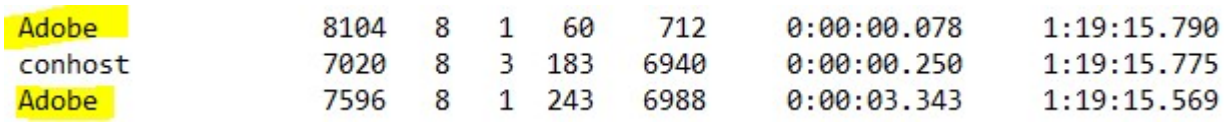
```
C:\Users\campe>type c:\windows\system32\drivers\etc\hosts > "Fichero
Hosts-%date:~6,4%%date:~3,2%%date:~0,2%-%time:~0,2%%time:~3,2%.txt"
```

Figura 46: Comando para guardar el nombre de los ficheros hosts en un archivo .txt (Fuente: propia)

15. Informe del ataque

Una vez tenemos todas las pruebas extraídas, conservadas e identificadas es hora de empezar a extraer información de todas ellas, para resumirlo solo plasmare las evidencias significativas encontradas e intentaremos extraer que tipo de ataque ha sido y cuando se produjo.

El día 25/10/2020 el usuario del ordenador investigado noto un extraño comportamiento cuando este se le bloqueaba varias veces durante el día y percibía errores de escritura como duplicación de letras o acentos aleatorios. Una vez consciente de esto procedió a llamar para el análisis forense. El usuario nos dijo que ese día no había descargado nada extraño, sino que había seguido su rutina de siempre.
Una vez analizado todo el contenido del ordenador encontramos las siguientes evidencias.



Adobe	8104	8	1	60	712	0:00:00.078	1:19:15.790
conhost	7020	8	3	183	6940	0:00:00.250	1:19:15.775
Adobe	7596	8	1	243	6988	0:00:03.343	1:19:15.569

Figura 47: Proceso “Adobe” no reconocido dentro del fichero de servicios en ejecución (Fuente: propia).

Investigado los servicios de ejecución encontramos un proceso extraño repetido dos veces.

En un principio se pensaba que se trataba del proceso de Adobe Photoshop, pero este aparecía en esta misma lista por lo tanto nos hizo sospechar que podría ser causa de un malware que intenta emular un proceso de Adobe para evitar hacer saltar las alarmas del usuario.

Una vez encontrado una posibilidad de la existencia de un malware en el equipo comencé a explorar que tipo de ataque se ha producido.
En la caché de DNS encontré una conexión extraña.

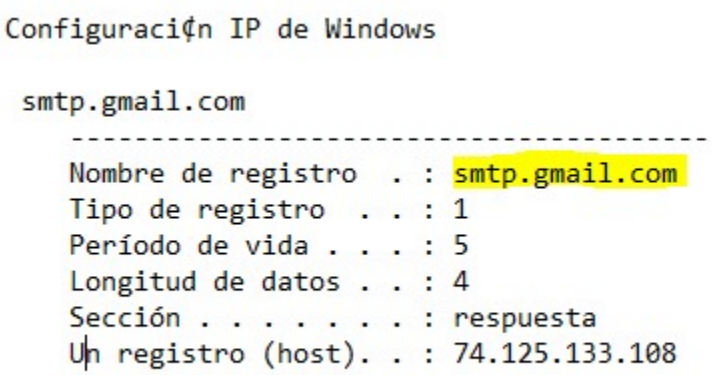
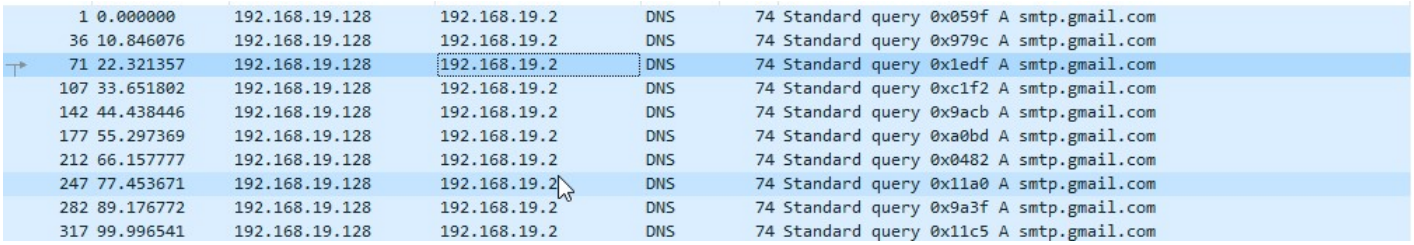


Figura 48: Imagen de la cache DNS con la información al dominio Gmail (Fuente: propia).

Como se puede ver en la figura 48 el sistema se estaba comunicando con una dirección de Gmail enviando respuestas por lo tanto es posible que se tratase de un ataque CC donde toda la información y las instrucciones se devuelven a un Gmail indicado, para corroborar mi hipótesis comencé a interceptar el tráfico de red del ordenador infectado.



1	0.000000	192.168.19.128	192.168.19.2	DNS	74	Standard query 0x059f A smtp.gmail.com
36	10.846076	192.168.19.128	192.168.19.2	DNS	74	Standard query 0x979c A smtp.gmail.com
71	22.321357	192.168.19.128	192.168.19.2	DNS	74	Standard query 0x1edf A smtp.gmail.com
107	33.651802	192.168.19.128	192.168.19.2	DNS	74	Standard query 0xc1f2 A smtp.gmail.com
142	44.438446	192.168.19.128	192.168.19.2	DNS	74	Standard query 0x9acb A smtp.gmail.com
177	55.297369	192.168.19.128	192.168.19.2	DNS	74	Standard query 0xa0bd A smtp.gmail.com
212	66.157777	192.168.19.128	192.168.19.2	DNS	74	Standard query 0x0482 A smtp.gmail.com
247	77.453671	192.168.19.128	192.168.19.2	DNS	74	Standard query 0x11a0 A smtp.gmail.com
282	89.176772	192.168.19.128	192.168.19.2	DNS	74	Standard query 0x9a3f A smtp.gmail.com
317	99.996541	192.168.19.128	192.168.19.2	DNS	74	Standard query 0x11c5 A smtp.gmail.com

Figura 49: Comprobación del tráfico entre el ordenador infectado y el dominio Gmail (Fuente: propia).

La figura 49 muestra el tráfico de red del ordenador infectado hacia una cuenta de Gmail, esto fue la extracción de una hora de tráfico, el host enviaba una petición al pc infectado y este le respondía con una query con los datos o la información específica.

Una vez hecho el descubrimiento el tipo de ataque estaba claro, se trata de un ataque backdoor con CC en un Gmail, por lo que podemos ver en la figura el atacante ha estado tiempo actuando y la filtración de datos ha sido muy grande. A partir de extraer el tráfico desconectamos el equipo de la red para evitar que el atacante se quede con más activos importantes para el usuario.

Una vez sabemos que ataque ha sido y los daños que ha causado investigamos como se ha producido este ataque, donde estaba la vulnerabilidad. Podemos notificar que el usuario no tenía activado su Windows por lo tanto no tenía las últimas actualizaciones ni las medidas defensivas necesarias para proteger dichos activos.

Probablemente el usuario aun tenga el exploit ejecutable almacenado en el ordenador por lo tanto vamos a investigar los archivos creados para ver si alguno de ellos nos puede indicar que malware es o que archivo ejecutable es. El primer indicio lo encontramos explorando los archivos creados, dentro de una carpeta temporal de Windows se han creado unos archivos que llaman la atención.

```
 Directorio de c:\Users\campe\AppData\Local\Temp\_MEI38362

25/10/2020  16:31    <DIR>          ..
25/10/2020  16:31    <DIR>          .
25/10/2020  16:31             1.050 Microsoft.VC90.CRT.manifest
25/10/2020  16:31            93.184 _ctypes.pyd
25/10/2020  16:31         1.014.784 _hashlib.pyd
25/10/2020  16:31            48.128 _socket.pyd
25/10/2020  16:31         1.405.952 _ssl.pyd
25/10/2020  16:31            72.704 bz2.pyd
25/10/2020  16:31             1.011 Adobe.exe.manifest
25/10/2020  16:31           225.280 msvcm90.dll
25/10/2020  16:31           570.520 msvcp90.dll
25/10/2020  16:31           653.976 msvcr90.dll
25/10/2020  16:31           138.240 pyexpat.pyd
25/10/2020  16:31         2.631.680 python27.dll
25/10/2020  16:31           110.592 pywintypes27.dll
25/10/2020  16:31            11.776 select.pyd
25/10/2020  16:31           688.640 unicodedata.pyd
25/10/2020  16:31            24.064 win32pipe.pyd
25/10/2020  16:31            25.088 win32wnet.pyd
              17 archivos      7.716.669 bytes
```

Figura 50: Carpeta temporal _MEI3862 que aloja unos archivos potencialmente maliciosos (Fuente: propia).

Se trata de un archivo con el mismo nombre que el proceso, todos creados el mismo día. Podemos ver archivos Python y .dll, suponemos que esta carpeta es la que se crea una vez ejecutado el backdoor por lo tanto nos la guardaremos para luego exportarla a Virustotal (una vez asegurándonos que nuestros archivos están a salvo).

Por último, encontramos un archivo que potencialmente podría ser un archivo malicioso. Este lo encontramos dentro de la carpeta imágenes y por lo que hemos podido comprobar se trataba de un archivo PDF que una vez abierto se ejecutaba un .exe. Hemos hablado con el usuario sobre ello y él nos comentó que intento abrir un archivo PDF pero que no se abrió y lo dejo pasar. Con la información que nos proporciona el usuario y con el archivo encontrado tenemos una clara evidencia de un archivo ejecutable que contenía el malware fue enviado al usuario mediante una técnica Phishing haciéndole creer que se trataba de un archivo PDF. Se trata de una vulnerabilidad de carácter humano, es decir, el usuario ha caído en la trampa del atacante y este ha explotado un riesgo con lo cual este ordenador y todos sus datos se han visto comprometidos desde el 10/10 /2020 a las 17:52 aunque no fue ejecutado hasta el 25/10/2020 a las 16:31, en ese momento la atacante tenía control total de todo el dispositivo.

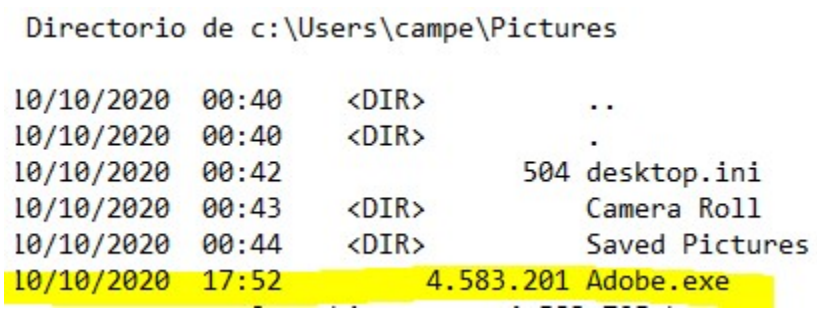


Figura 51: Archivo ejecutable que posiblemente contenga el malware (Fuente: propia).

Una vez recreada la línea temporal seguimos explorando por si queda alguna evidencia o archivo oculto por detectar.

Y así es, en la MFT (Master File Table) encontramos otra vez el archivo Adobe.exe en la carpeta Prefetch, carpeta que se utiliza para los archivos que se ejecutan muy a menudo para así tenerlos accesibles a memoria, es decir, se trata de un archivo que se ejecuta automáticamente sin que el usuario lo sepa. Mirando los Logs de Security hemos encontrado que el 07/11/2020 Windows detecto un intento de aprovecharse de una vulnerabilidad y cerro el evento.

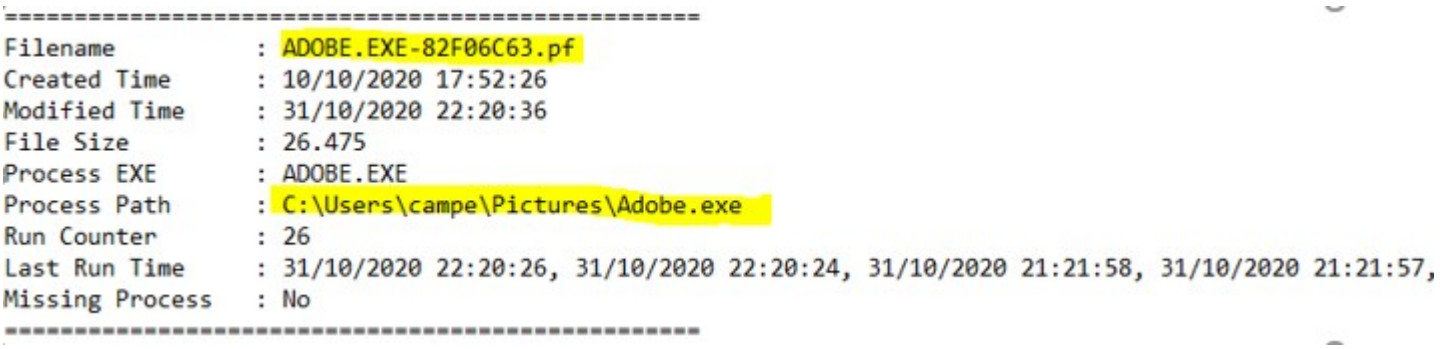


Figura 52: Evidencia encontrada en la carpeta Prefetch (Fuente: propia).

Una vez hemos extraído todas las evidencias y asegurar los datos del usuario vamos a subir los archivos problemáticos a la página web Virustotal para cotejarlo con las bases de datos de los antivirus conocidos y comprobar si se trata de un malware conocido.

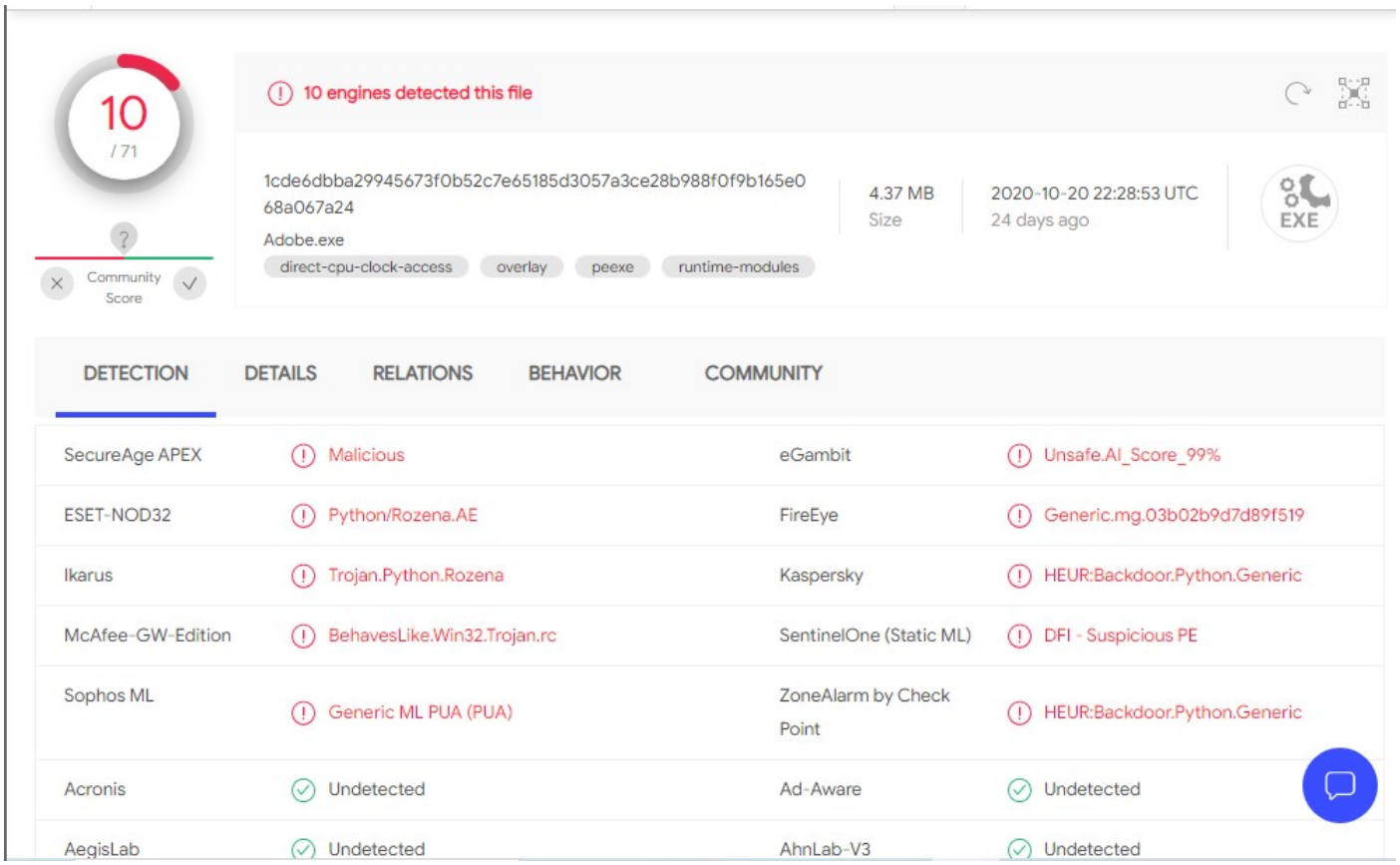


Figura 53: Una vez subido el archivo potencialmente malicioso a Virustotal nos muestra que clase de malware es (Fuente: propia).

Como sospechábamos hemos encontrado un backdoor de Python en el archivo escondido en un PDF. Una vez descubierto esto ya tenemos las pruebas para determinar cuándo fue el ataque y que ataque fue y que archivos se han podido ver comprometidos.

16. Conclusiones

La complejidad de realizar un análisis forense es bastante elevada, la gran facilidad que hemos tenido en este trabajo ha sido la gran cantidad de información y guias oficiales que hay al respecto. Aun habiéndome visto en problemas a la hora de la realización de mi proyecto considero que se han conseguido la mayoría de objetivos especificados:

- He conseguido simular una infección de malware a un ordenador.
- He sido capaz de realizar un analsiis forense paso a paso y poder extraer las pruebas suficientes para poder crear un informe del ataque.
- He aprendido sobre los diferentes malware y peligos que acechan en internet.
- He enseñado como funciona una infección por un malware backdoor.
- He utilizado las herramientas descritas durante el informe para poder extraer la información durante el análisis forense

De cara al futuro me gustaría poder indagar mas en el tema de investigación forense y poder infectar un laboratorio con otros tipos de malware para analizar como atacan al sistema.

17. Bibliografía

Referencias

[dC14] Instituto Nacional de Ciberseguridad. Guía de tomas de evidencias en un entorno windows. https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_toma_evidencias_analisis_forense.pdf, page 9, 2014. Online, accessed 14-jul-2020.

[dE19] Instituto Nacional de Estadística. Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares. http://aiweb.techfak.uni-bielefeld.de/content/bworld-robot-control-software/, 2019. Online, 14-jul-2020.

[For00] Internet Engineering Task Force. Internet Security Glossar.(English). https://tools.ietf.org/html/rfc2828, page 13, 2000. Online, accessed 17-jul-2020.

[For02] Internet Engineering Task Force. Guidelines for Evidence Collection and Archiving.(English). https://www.ietf.org/rfc/rfc3227.txt, 2002. Online, accessed 14-jul-2020.

[Itd17] Itdigitalsecurity. ¿qué hace diferente a un ataque dirigido? https://www.itdigitalsecurity.es/reportajes/2017/08/que-hace-diferente-a-un-ataque-dirigido, 2017. Online, accessed 16-jul-2020.

[Loc34] Edmond Locard. *La police et les méthodes scientifiques. (French)*, pages 8–9. 1934. Online, accessed 14-jul-2020.

[oST13a] National Institute of Standards and Technology. Guide to Malware Incident Prevention and Handling for Desktops and Laptops.(English). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf, page 18, 2013. Online, accessed 18-jul-2020.

[oST13b] National Institute of Standards and Technology. Guide to Malware Incident Prevention and Handling for Desktops and Laptops.(English). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf, page 3, 2013. Online, accessed 17-jul-2020.

[oST15] National Institute of Standards and Technology. Guide to Industrial Control Systems (ICS) Security.(English). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf, page 136, 2015. Online, 17-jul-2020.

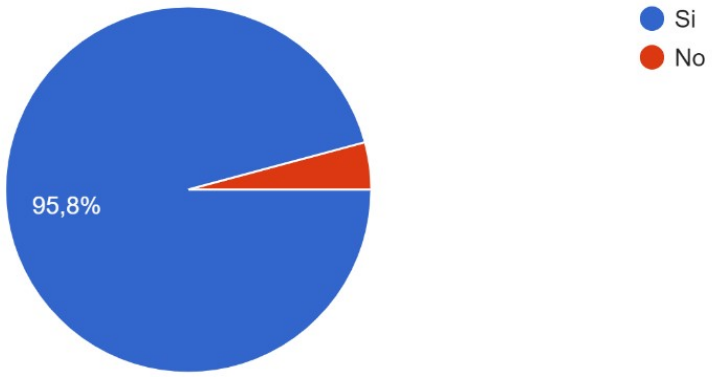
[oST17a] National Institute of Standards and Technology. An Introduction to Information Security. .(English). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, page 24, 2017. Online, accessed 17-jul-2020.

[oST17b] National Institute of Standards and Technology. An Introduction to Information Security.(English). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, page 87, 2017. Online, accessed 17-jul-2020.

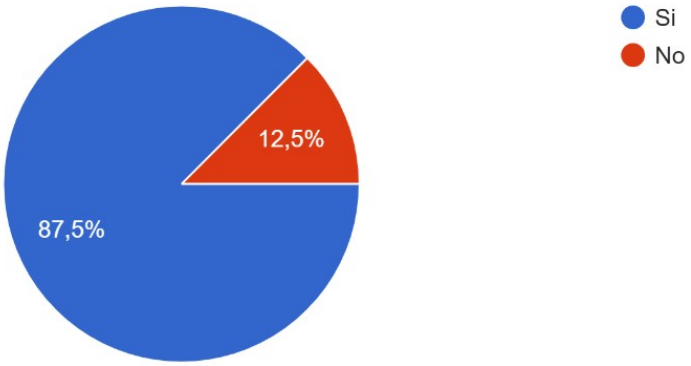
[oST19] National Institute of Standards and Technology. https://www.ine.es/prensa/tich_2019.pdf, 2019. Online, accessed 14-jul-2020.

Apéndice A Encuesta sobre conocimiento de ciberseguridad

¿Sabes lo que es la ciberseguridad?
24 respuestas



¿Alguna vez te has planteado si tu equipo es seguro?
24 respuestas



¿Qué métodos tienes de seguridad?

19 respuestas

Antivirus

El windows Defende

Ninguno, bueno Windows Defender en W10

Antivirus, VPN, complementos de seguridad en Firefox y precaucion.

No se conecta ningún usb o dispositivo que no conozca, no descargar nada que no sepa lo que es, leer todos las clausulas de descargas, mirar urls antes de poner usuario y contraseñas, no te comas las cookies, usuarios anónimos en internet, contraseñas diferentes con aA1!, como última instancia arrancar el ethernet y taladrar el hardware

Windows Defender y yo

password, pin, huella

Windows Defender

Antivirus, sitios importantes con doble autenticacion

Antivirus, firewall , utilizar otro s.o para enviar datos importantes (banco, matrícula de la ub,etc..)

Noscript, mineblock, antivirus,

Ussr antivirus e ir con cuidado

el firewall de windows

Windows Defender y poquito más loquete.

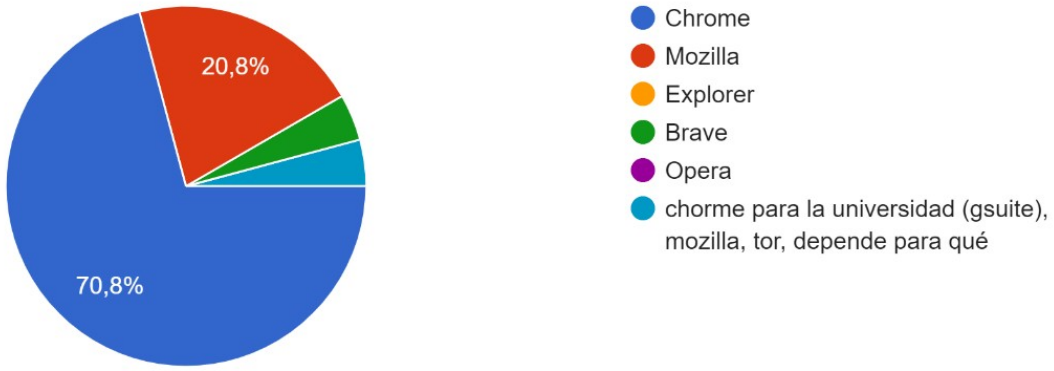
Norton Antivirus

no lo se

Anti-malware/restricciones de acceso de los navegadores web/ el uso de máquinas virtuales para ejecutar programas que no confio.

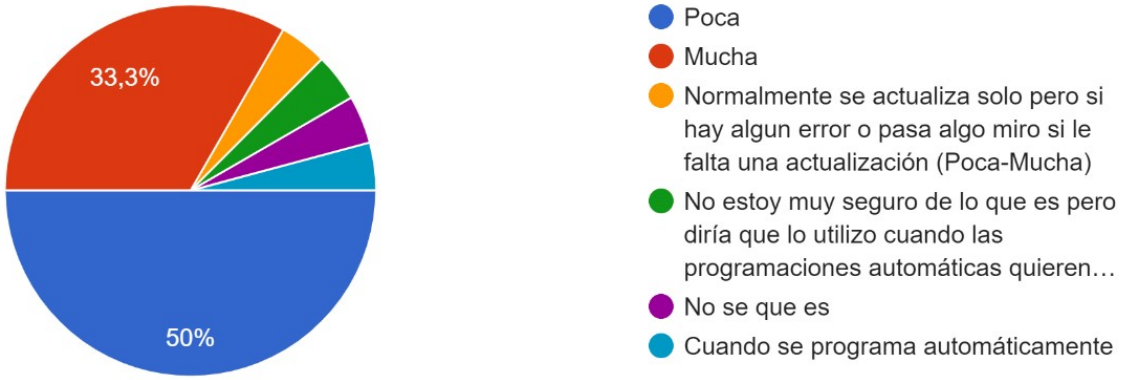
¿Qué navegador web utilizas normalmente?

24 respuestas



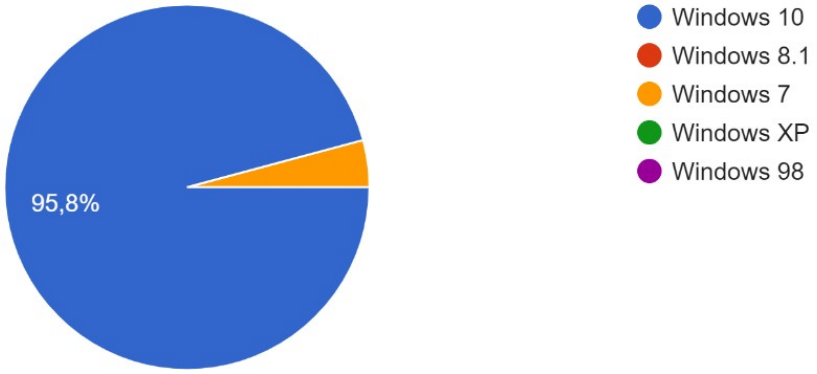
¿Con qué frecuencia utilizas Windows Update?

24 respuestas



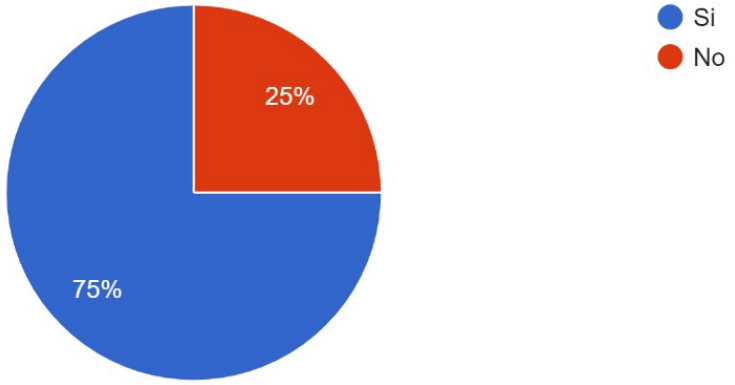
¿Qué versión de Windows está instalada en el equipo que normalmente usas para conectarte a Internet?

24 respuestas



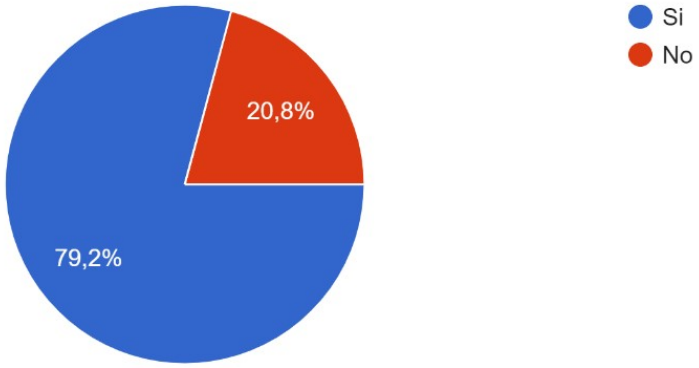
¿Tienes software antivirus instalado en tu ordenador?

24 respuestas

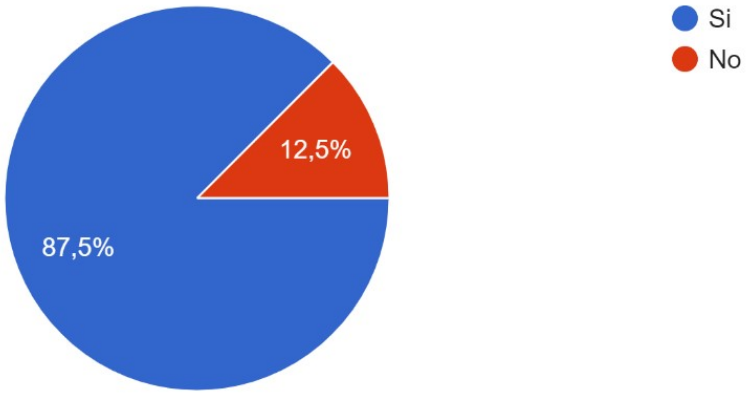


¿Sabes lo que es un malware?

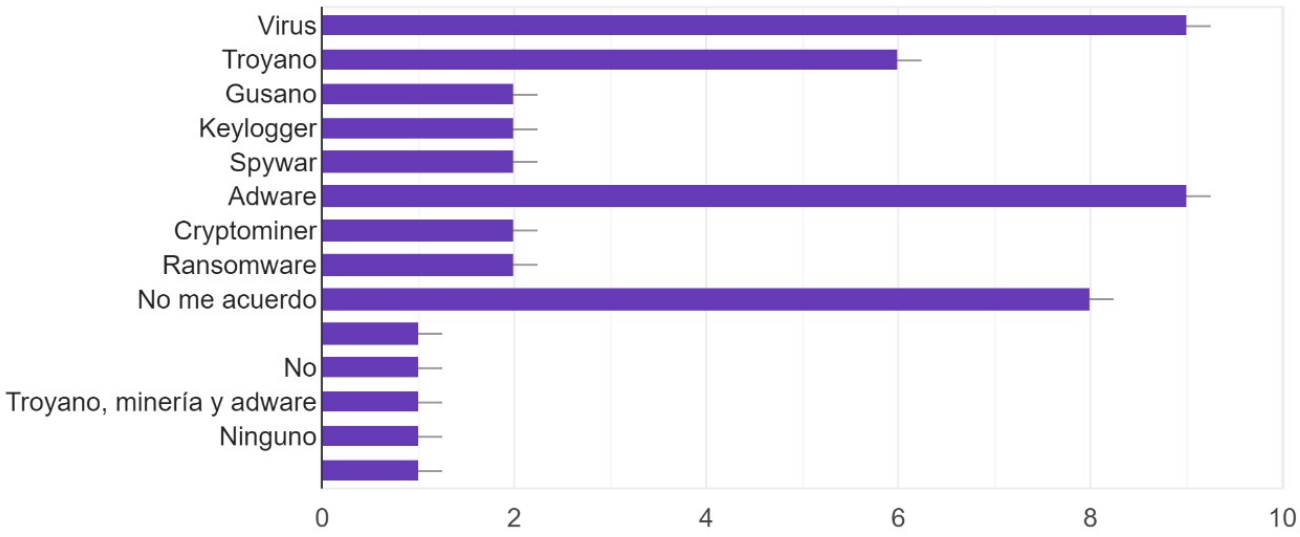
24 respuestas



¿Alguna vez has sido atacado o has descubierto que tenías un "virus" en tu equipo?
24 respuestas

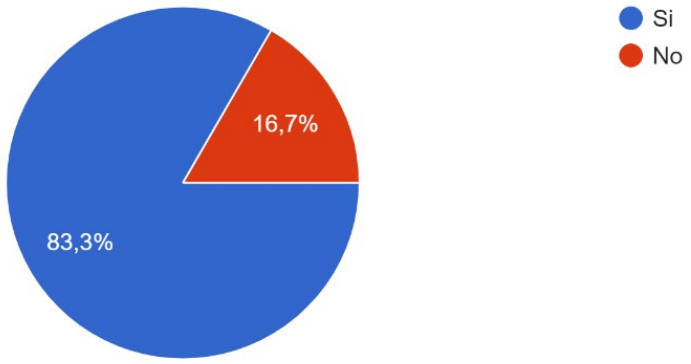


Si es así, ¿qué tipo de virus era?
24 respuestas



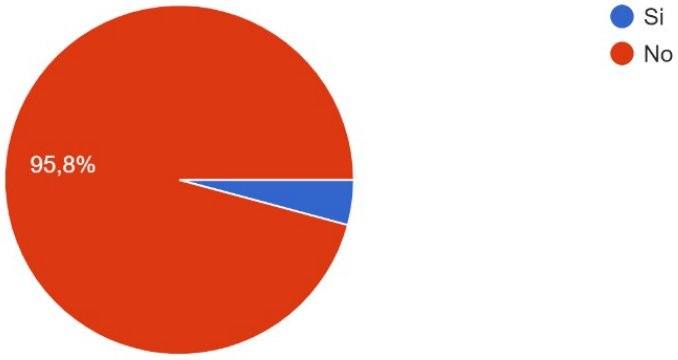
¿Alguna vez has recibido un correo phishing? Es decir un correo de engaño haciéndose pasar por una compañía de confianza para quedarte con tus cr...ciales o insistir en ejecutar un archivo malicioso

24 respuestas



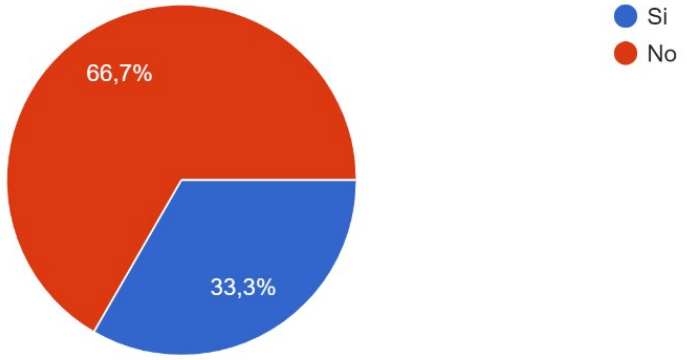
¿Sabes lo que es el INCIBE?

24 respuestas



¿Sabes lo que es el análisis forense de malware?

24 respuestas



¿Sabrías que hacer si el ordenador de empresa/personal está siendo atacado?

24 respuestas