Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Título

Herramientas de Búsqueda de Malware en Aplicaciones Windows

Autor: Ing. Caifas Franco

Tutor: Dr. Pedro Hecht

Año 2019
Cohorte 2017

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Caifas Franco

Resumen

El trabajo final de especialización se orientará en la Criptovirología, en los tipos de análisis de malware (estáticos, dinámicos) y en la descripción de algunas de las herramientas empleadas en el análisis de malware en aplicaciones desarrolladas para sistemas operativo Windows. De igual forma se describirán los diferentes métodos que utilizan los antivirus para detectar el malware.

Se describirán un conjunto de herramientas tales como software de virtualización para crear entornos seguros de análisis, analizadores de tráfico para poder ver las conexiones del malware, análisis de procesos para conocer los procesos que son creados en la maquina después de la ejecución del malware, autoruns para comprobar si el malware en cuestión creó alguna entrada en el registro y así crear persistencia en el Sistema Operativo, aplicaciones para controlar los cambios que se realicen en el registro de Windows, editores hexadecimales, aplicaciones que ayudaran a saber si el malware utiliza algún comprensor/empaquetador y depuradores a nivel de aplicación.

Algunas herramientas mencionadas anteriormente están incluidas en la suite Sysinternals Security Utilities de Microsoft y en SysAnalyzer de David Zimmer, las cuales también serán mencionadas en este trabajo. Además, se comentará sobre 4n4lDetector que es una herramienta creada por Germán Sánchez Garcés, que se basa en la extracción de strings “ANSI” y “UNICODE” y en Memory Dumps de los ejecutables.

Palabras Claves: Criptovirología, Virtualización, análisis de malware, herramientas de análisis de malware, Windows, malware, tipos de análisis de malware, antivirus.

Tabla de contenido

INTRODUCCIÓN 7

1. CRIPTOVIROLOGÍA 8

1.1 ¿QUÉ ES UN CRYPTOVIRUS? 10

1.2 ¿QUÉ ES UN SISTEMA CRIPTOGRÁFICO DE "CAJA NEGRA" O “BLACK BOX”? 11

1.3 ¿QUÉ ES UN CANAL SUBLIMINAL Y LA RELACIÓN CON UN ATAQUE CLEPTOGRÁFICO? 12

1.4 POLIMORFISMO 13

2. MÉTODOS DE ESCANEO DE ANTIVIRUS 16

3. ¿IMPORTANCIA DE UN ANÁLISIS DE MALWARE? 21

3.1 TÉCNICAS DE ANÁLISIS DE MALWARE 23

4. HERRAMIENTAS DE ANÁLISIS 23

4.1 HERRAMIENTAS DE ANÁLISIS ESTÁTICO 24

4.1.1 IDENTIFICACIÓN DEL TIPO DE ARCHIVO 24

4.1.2 EXTRACCIÓN DE STRINGS 29

4.1.3 ANÁLISIS DE CÓDIGO 30

4.1.4 ANALIZANDO DEPENDENCIAS 32

4.2 HERRAMIENTAS DE ANÁLISIS DINÁMICO 34

4.2.1 BUSQUEDA DE PROCESOS 34

4.2.2 ANÁLISIS DE CONEXIONES 38

4.2.3 ANÁLISIS DE REGISTRO. 40

4.3 VIRTUALIZACIÓN 41

4.3.1 VIRTUAL BOX 42
4.3.2 VMWARE WORKSTATION 44
4.4 OTRAS HERRAMIENTAS 45
4.4.1 CFF Explorer 45
4.4.2 SYSTEMINFO 45
4.4.3 SSDEEP 46
4.4.4 SYSINSPECTOR 46
4.4.5 SYSANALYZER 47
4.4.6 4N4LDETECTOR 48
4.5 ESCANERES ONLINE 49
4.6 SANDBOX 53
5. CONCLUSIÓN 55
BIBLIOGRAFÍA ESPECIFICA 59
BIBLIOGRAFÍA GENERAL 59
TABLA DE ILUSTRACIONES 63

Prólogo

Quiero agradecer primero que todo a Dios y a mis padres Rene Franco y Ruth Arteaga por haberme apoyado y darme ánimo durante todo momento mientras estudiaba y vivía en otro país. De igual forma agradezco la ayuda de mis hermanas Olga Franco y Jennifer Franco que me brindaron ánimo constantemente para poder cumplir este objetivo propuesto.

Asimismo, quiero dar las gracias por la orientación y apoyo a mi tutor de proyecto y a todas las personas cercanas quienes me han ayudado de una u otra forma a culminarlo.

INTRODUCCIÓN

En el mundo la cantidad de ataques informáticos a organizaciones y personas del común va en aumento año tras año. El análisis de estos malware nos permite documentar el comportamiento y “acciones” de un software/código malicioso, es decir, establecer que hace y como lo hace.

Con el análisis podríamos obtener información sobre las conexiones de red que realiza, las modificaciones que efectúa en el registro, procesos ejecutados y archivos creados en el sistema por parte del software dañino.

Tener conocimiento de los cambios y el comportamiento que presenta el software maligno es conveniente ya que así podremos tomar las medidas adecuadas para la posterior desinfección del sistema operativo, saber el alcance exacto del ataque y tomar las medidas correctivas para prevenir cualquier otro ataque similar.

El análisis de malware es empleado en la auditoria forense para conocer si el programa dañino causo algún perjuicio económico o comprometió información, también es utilizado para crear herramientas de protección propias en caso que la solución de Antivirus o Antimalware que se maneje aun no detecte la amenaza.

Con este trabajo se pretende detallar los métodos de análisis de malware y algunas de las herramientas que son empleadas durante el análisis, y de esta forma sirva como base para quienes quieran profundizar más en el tema y aprender a realizar sus propias investigaciones.

1. CRIPTOVIROLOGÍA

Es un concepto teórico desarrollado por Adam Young y Moti Yung el cual utilizaron y es empleado actualmente para referirse al análisis del software malicioso (malware) que emplea la criptografía, simétrica o asimétrica, para ocultarse y dificultar un posible análisis a través de la ingeniería inversa que hagan los investigadores o en los ataques en los cuales se sirven de la criptografía para causar daño como encriptando o cifrando la información de las víctimas o el acceso completo a su PC, para así chantajear o pedir una recompensa a cambio de la contraseña que permita el acceso nuevamente a sus archivos, PC o simplemente buscan causar daño a la operación y continuidad de una organización o afectar el trabajo de una persona común.

La criptografía se ha utilizado a lo largo de la historia como una herramienta defensiva ayudando a la protección de posibles ataques contra la integridad, autenticación o confidencialidad de la información, pero en un nuevo escenario los desarrolladores de software dañino la están empleando para fortalecer, mejorar y desarrollar nuevos ataques más sofisticados mejorando la capacidad de anonimato del atacante, mejorar la capacidad de extorsión y dificultando posibles estudios o análisis a través de Ingeniería Inversa.

Young y M. Yung señalan que “La criptovirología se extiende más allá de encontrar fallas en el protocolo y vulnerabilidades de diseño. Es una disciplina de ingeniería avanzada que puede usarse para atacar en lugar de defender.” [6]

Uno de los primeros casos que los atacantes emplearon la criptografía asimétrica fueron RANSOM o GPCODE y el más reciente cryptoataque cibernético fue el WannaCrypt, el cual afectó varias empresas a nivel mundial, este tipo de ataques se conocen como Cryptoviral Extorsion.

Imagen 1: Mensaje mostrado por WannaCrypt (xataka.com)

Los ataques de CRYPTOVIRAL EXTORSION a grandes rasgos son los que utilizan la criptografía asimétrica también conocida como de clave pública para cifrar los datos almacenados o bloquear la máquina del usuario para luego pedir un “rescate” a cambio de la contraseña que permita desbloquear la información o la PC de la víctima.

Para este tipo de ataque como ya se mencionó se emplea un cryptovirus que utiliza un sistema criptográfico híbrido para encriptar los datos de la maquina mientras estos son eliminados o sobrescritos en el proceso.

Por lo general el desarrollador del virus utiliza un generador de bits aleatorio (TRBG) para generar una clave simétrica y un vector de inicialización al azar, posteriormente el virus cifra los datos de la maquina con la clave simétrica y el

vector de inicialización, por ejemplo, utilizando el modo de encadenamiento de bloques de cifrado (CBC).
El virus concatena el vector de inicialización con la llave simétrica y cifra la cadena resultante con la llave pública del desarrollador, por ejemplo, usando RSA-OAEP, el cual es un esquema de cifrado de llaves públicas estandarizado.

El virus le avisa a la víctima del ataque, por lo general a través de un cuadro de texto o dialogo, que sus datos han sido encriptados y notificándole sus demandas a cambio de que pueda recuperarlos, si la persona perjudicada cumple con dicha demanda que por lo general es dinero (Bitcoin) el autor del virus le envía la llave privada o contraseña que solo el posee y de esta forma el afectado pueda recuperar sus datos. Un ejemplo del mensaje puede ser visto en la Imagen 1.

1.1 ¿QUÉ ES UN CRYPTOVIRUS?

Es un virus informático que contiene y utiliza una clave pública, la cual generalmente pertenece al creador del virus, un ejemplo es el Ransomware. Los cryptovirus pueden utilizar web pública para comunicarse o quedar a la “escucha” de alguna acción que le envíen.

Un ejemplo es el que fue descubierto el pasado mes de diciembre del 2018 en el cual un virus se mantenía a la escucha e ingresaba a una cuenta de Twitter en busca de instrucciones, para lo cual el autor del virus enviaba comandos ocultos en los metadatos de una imagen que posteaba (meme “What If I Told You”) en dicha cuenta. Utilizaba palabras como */print, /clip y /procesos* para imprimir/capturar la pantalla, copiar el portapapeles o listar los procesos de la maquina infectada respectivamente. Esta técnica de ocultar texto en una imagen es conocida como estenografía.

Los cryptotroyanos o cryptogusanos es lo mismo que un cryptovirus, pero con caballos de Troya (troyanos) y gusanos. Un virus que utilice clave simétrica no

sería un cryptovirus, como el caso de los virus polimórficos que en su gran mayoría emplean una clave simétrica.

1.2 ¿QUÉ ES UN SISTEMA CRIPTOGRÁFICO DE "CAJA NEGRA" O "BLACK BOX"?

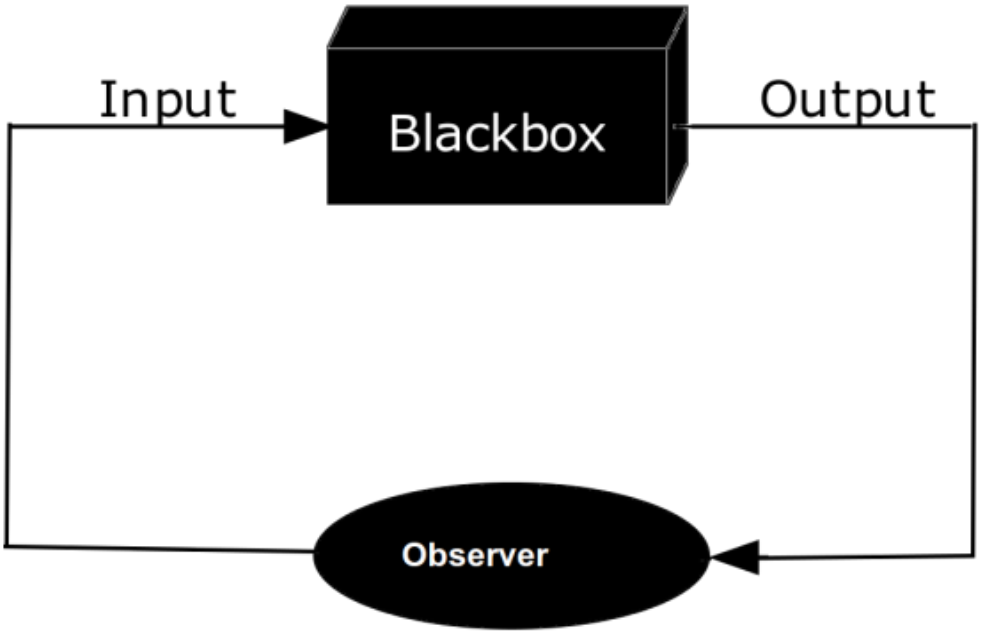


Imagen 2: Ejemplo de un Cryptosistema de caja negra (http://informatica.blogs.uoc.edu)

Un cryptosistema de caja negra es el que se implementa y no puede ser analizado ya que no se tiene acceso o bien sea al código fuente o a los circuitos instalados, por lo tanto, son utilizados sin verificar la exactitud de su implementación y su verdadera funcionalidad puede diferir.

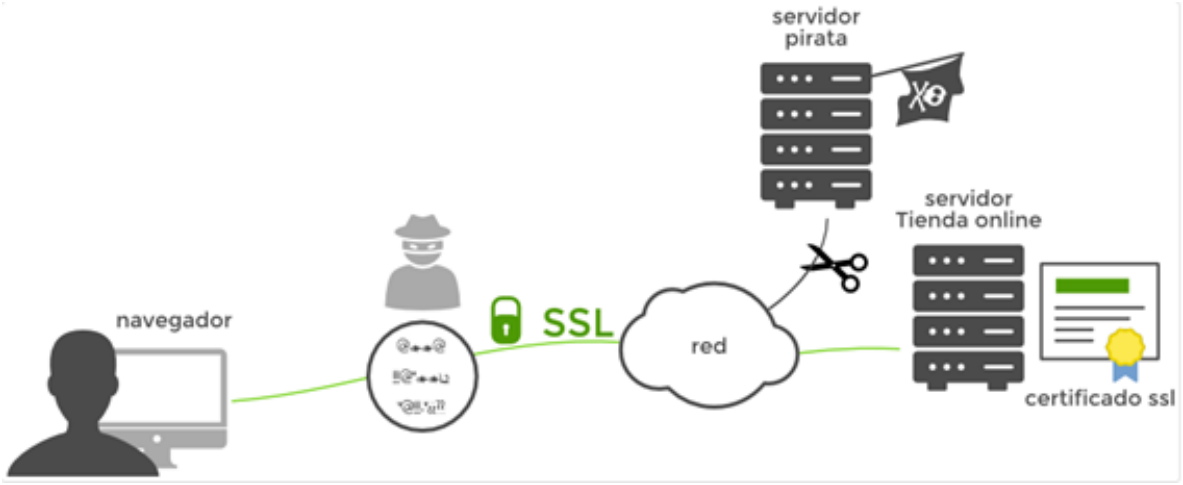


Imagen 3: Ejemplo de implementación de SSL (cosmomedia.es)

La mayoría de los usos de la criptografía son cryptosistema de caja negra, como por ejemplo la implementación de SSL para conexiones seguras (Secure Sockets Layer) utilizadas en su mayoría en las páginas web de compras online o páginas de transacciones electrónicas, las cuales no son verificadas por el usuario, las tarjetas inteligentes como la de los hoteles o las que se dan en las empresas para controlar el ingreso es otro ejemplo común que es utilizado todos los días.

En palabras más específicas un sistema criptográfico de caja negra es un dispositivo o sistema en el cual se puede observar sus entradas y sus salidas sin lograr ver las funcionalidades internas.

1.3 ¿QUÉ ES UN CANAL SUBLIMINAL Y LA RELACIÓN CON UN ATAQUE CLEPTOGRÁFICO?

Un canal subliminal es un canal en el cual se puede enviar o transmitir información desde un cryptosistema de forma encubierta, por lo general los atacantes se aseguran que los canales subliminales se utilicen solo en sistemas criptográficos de caja negra ya que son fáciles de descubrir cuando el código es examinado por los criptógrafos.

Un primer intento fue realizado en 1993 por el profesor de Ingeniería de Seguridad en el Laboratorio de Computación de la Universidad de Cambridge Ross Anderson, el cual desarrollo una puerta trasera en la generación de claves RSA. Con el tiempo su propuesta no prosperó ya que se descubrió que se trataba de una puerta trasera simétrica y cualquiera que la descubriera podía utilizarla, además, se podía detectar a partir de la salida de la caja negra criptográfica.

Tres años después, 1996, los investigadores A. Young y Moti Yung presentaron su propuesta de una puerta trasera para obtener la clave privada en la generación de una clave RSA, la principal diferencia es que era una puerta trasera asimétrica y el único que conocía la contraseña era el atacante.

A este tipo de ataques los investigadores (Young y Yung) lo denominaron **ataque cleptográfico**, que no es más que la modificación de un sistema criptográfico de manera imperceptible en el cual no se distingue la salida de un sistema infectado de uno no infectado.

El atacante aprovecha el canal subliminal y la criptografía asimétrica para sacar la información necesaria y recuperar la clave privada y proteger el canal solo para su uso respectivamente. Solo con ingeniería inversa y un análisis profundo de la caja negra es posible descubrir este tipo de ataque, pero el investigador no podrá nunca hacer uso del canal.

En palabras de A. Young y Moti Yung “un ataque cleptográfico es una puerta trasera asimétrica que solo puede usar el diseñador que realiza el ataque[1].”[7]

1.4 POLIMORFISMO

[1] Traducido del ingles: In other words, a kleptographic attack is an asymmetric backdoor that can only be used by the designer that carries out the attack

Es un virus que produce copias distintas de sí mismo empleando un código polimórfico, es decir, se modifica a sí mismo manteniendo su funcionalidad en cada ejecución para dificultar la detección por parte de los antivirus los cuales identifican coincidencias en cadenas y crean una firma, esta es almacenada en la Base de Datos del Antivirus. En el escaneo de un archivo el antivirus busca los patrones o coincidencias en cada archivo que sea escaneado. Si encuentra una coincidencia salta la alerta.

Los virus polimórficos fueron de los primeros tipos de malware que coloco en aprietos a las compañías de antivirus ya que encriptaba y cambiaba parte de su código. Este tipo de malware funciona de tal forma que encripta su código por medio de una clave y utiliza una operación reversible como puede ser un XOR con clave aleatoria para el desencriptado, el cual ocurre en el tiempo de ejecución y la clave para desencriptar el ejecutable es distinta cada vez que se ejecuta.

En el código del malware siempre queda una parte sin mutar ya sea porque sea una función esencial para el correcto funcionamiento y esos sectores son los más vulnerables por lo tanto son los más aprovechados por los programas de protección para colocar las firmas, de igual forma también emplean la heurística para detectar acciones sospechosas en la ejecución y notificar al usuario, ya que el código cambia, pero no la funcionalidad.

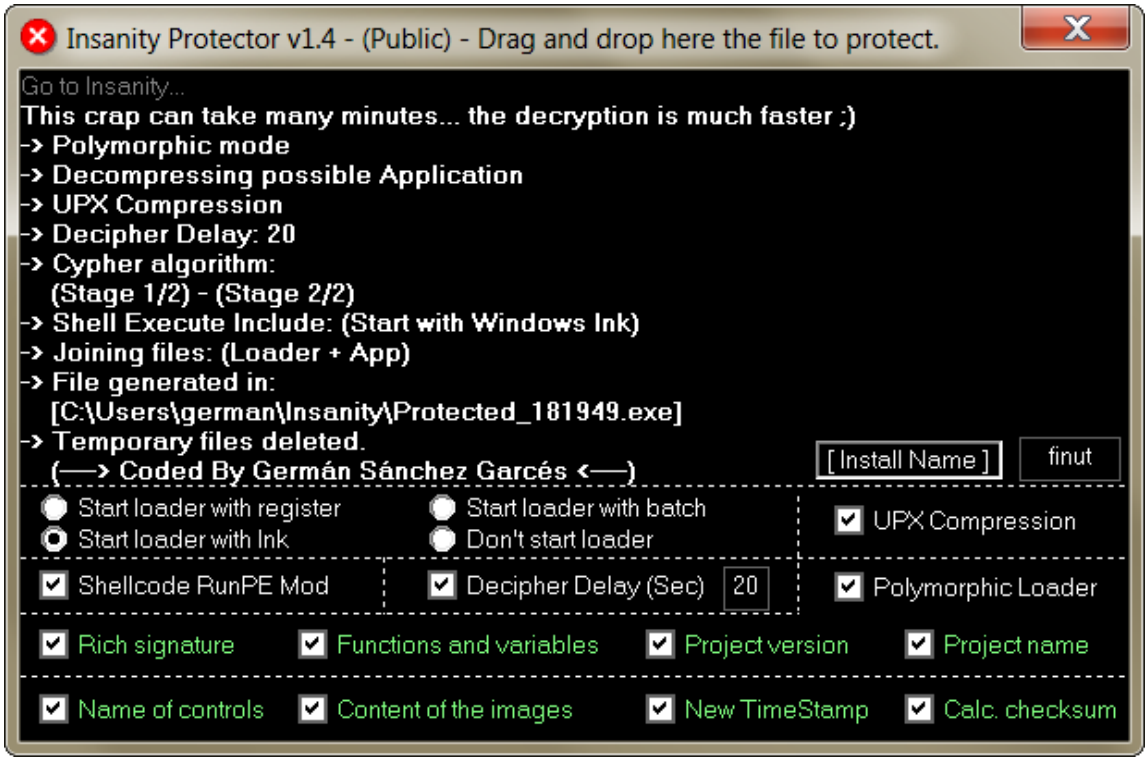


Imagen 4: Crypter Poliformico (enelpc.com)

Existen programas para la creación de malware con código polimórfico que varían las secuencias de sus instrucciones, insertando en la rutina o al momento del descifrado código basura, insertando diferentes funciones o partes de código que cumplan la misma función con el objetivo de confundir a los antivirus ya que el código no sería igual, obligando de esta forma a que los antivirus tengan que evolucionar, ya que el código basura y los métodos alternativos que use el programador no alteraría la función principal ni corrompería el archivo potencialmente dañino.

ONE HALF es ejemplo de uno de los primeros virus polimórfico, el cual cifraba el disco duro por partes cada vez que se iniciaba la maquina huésped y el usuario no notaba nada hasta que se cifraba la mitad del Disco ya que es cuando les mostraba el mensaje:

```
Dis is one half.
 Press any key to continue ...
 Did you leave the room?
```

Este virus solo encriptaba los archivos con extensiones .EXE y .COM y chequeaba los archivos antes de infectarlos en busca de las cadenas de texto “SCAN, CLEAN, FINDVIRU, GUARD, NOD, VSAFE, o MSAV” que son empleadas por los antivirus.

Una vez infectada la maquina el usuario podía usar su PC con normalidad, si intentaba eliminarlo podría perder su información ya que la misma quedaba encriptada. Esto debido a que el virus almacena la clave de cifrado como la información sobre la ubicación y la extensión del área cifrada dentro de su código.

2. MÉTODOS DE ESCANEO DE ANTIVIRUS

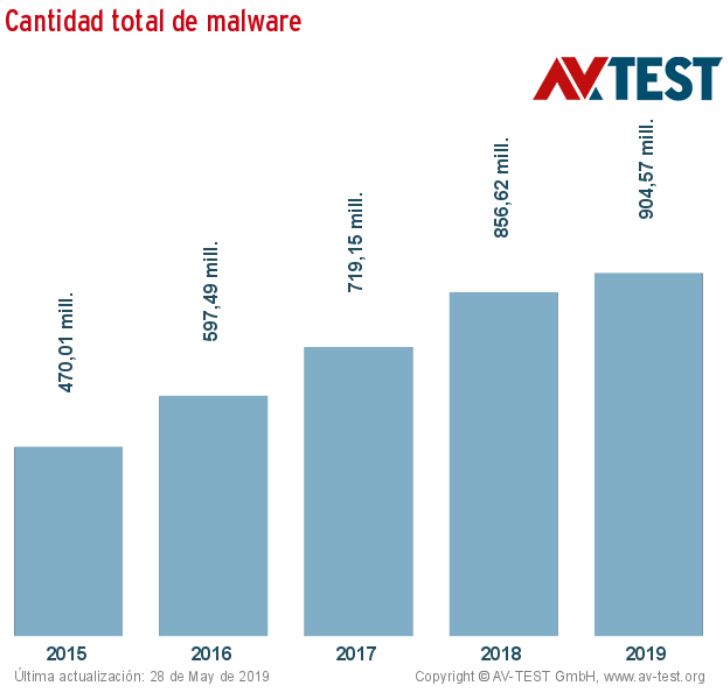


Imagen 5: Métricas del total de malware desde el 2015 (av-test.org)

Día a día la cantidad de virus informáticos va en constante aumento y propagándose con mayor rapidez gracias a internet, debido a esto es importante proteger la información y el software instalado lo mejor posible y una de las herramientas empleadas para este fin es el Antivirus. El cual es un software de

protección que tiene como función principal proteger el sistema ante posibles ataques de malware.

El servicio fundamental de un antivirus es la prevención y la detección de un virus informático o el accionar del mismo, para detenerlo y de esta forma disminuir el porcentaje de daño causado en la máquina. Actualmente los antivirus se basan en la prevención de posibles virus informáticos con una opción de protección en tiempo real.

De igual forma hay algunos antivirus tienen funciones para actuar como una solución antimalware que resguardan los datos contra gusanos, troyanos, ransomware, rootkit entre otros programas dañinos. Adicionalmente cuentan con otras opciones como anti spam, firewall, protección de archivos, protección de contraseñas, protección de compras online y operaciones bancarias, protegen tu privacidad mientras navegas, y otras funciones más dependiendo del Antivirus.

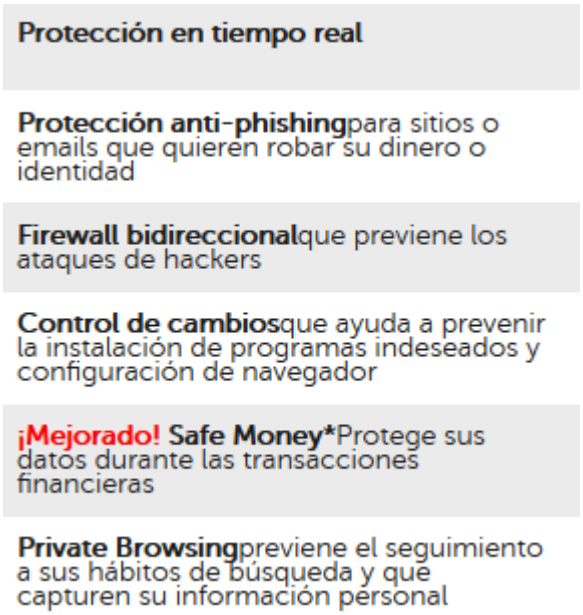


Imagen 6: Funciones adicionales de Kaspersky AV para el Hogar (kaspersky.com)

El software de protección cuenta con dos métodos de detección de virus informáticos: **el reactivo**, en el cual se debe conocer el malware para que sea

detectado, consiste en un método basado en firmas donde el fabricante del antivirus emplea una base de datos para determinar si un archivo es una amenaza o no. El funcionamiento es sencillo, el antivirus compara el archivo contra su base de datos y si encuentra una coincidencia alerta al usuario informando que es dañino.

En este tipo de método es importante que el antivirus este siempre actualizado para contar con protección de los últimos códigos dañinos que se vayan detectando, ya que cada vez que aparezca algún nuevo malware el laboratorio de la compañía analiza una muestra y le crea una nueva firma en su Base de datos.

El contra del método reactivo es que, si un malware no ha sido analizado por la compañía antivirus o no esta actualizado el antimalware, la protección no es eficaz. Como solución a estos inconvenientes las compañías se valen de una segunda forma de detección para mantener a sus usuarios lo más seguro posible, el método **proactivo o Heurística**.

Este método consiste en reglas basadas en el análisis o estudio del comportamiento del malware e ir colocando un puntaje a cada acción que haga en el sistema, por ejemplo, si se carga al inicio, modifica el registro, etc., si supera un valor X es catalogado como una posible amenaza. En la imagen 7 se puede apreciar claramente las diferencias y la forma de detección entre ambos métodos (reactivo y proactivo).

Imagen 7: Métodos de detección de los AV (welivesecurity.com)

La heurística dependiendo del Antivirus se puede configurar por rigurosidad, entre mayor sea la misma es más probable que se detecte un falso positivo, los cuales son comportamientos de un programa legítimo que tiene funciones de alguno dañino como abrir todos los archivos de un PC o escribir en los mismos, los cuales son propios de herramientas como los antivirus, y son detectados por el software antimalware instalado. En palabras simples, es la identificación de archivos inofensivos como maliciosos.

Ejemplos de falsos positivos como los de McAfee y Sophos en el cual luego de una actualización de su Base de Datos, las maquinas que lo tenían instalado les aparecía la pantalla azul de Windows, les andaba la maquina lenta o quedaba colgada, es decir, dejaba de funcionar correctamente el SO. Esto debido a que dicha actualización detectaba por error un componente de Windows como una amenaza y lo eliminaba o enviaba a cuarentena dependiendo de la configuración.

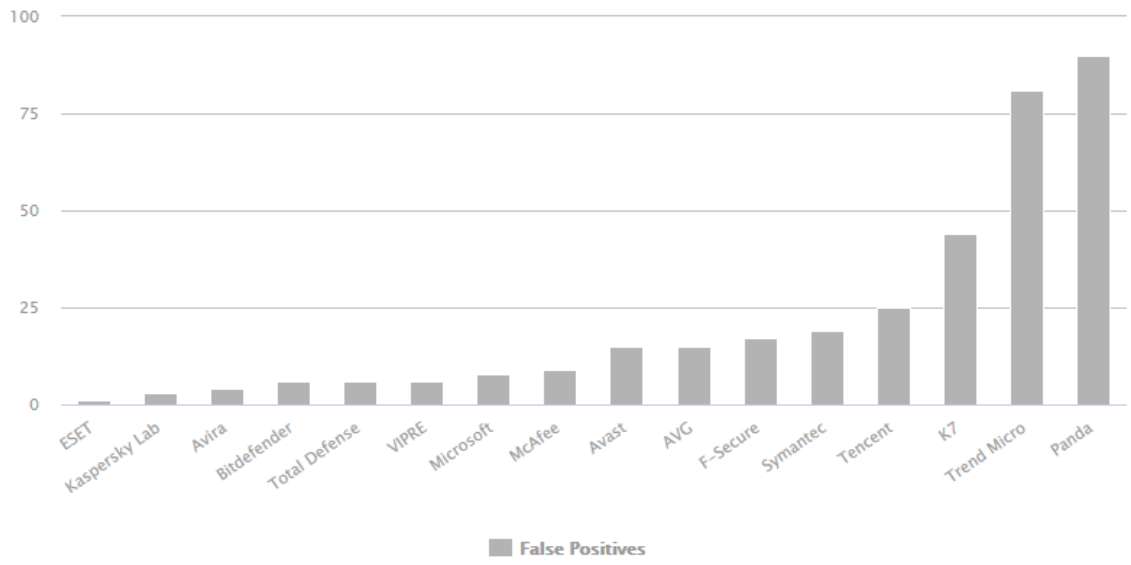


Imagen 8: Malware Protection Test March 2019 - Falses Positives (av-comparatives.org)

Cabe aclarar que los falsos positivos no solo ocurren por la heurística sino también por una firma mal colocada por parte de los analistas de las compañías de Antivirus. En la imagen 7 se aprecia un Test que realizado por la compañía

independiente AV-COMPARATIVES en el mes de marzo de 2019 en el cual Trend Micro y Panda son los antivirus con más falsos positivos y el que menos presenta es ESET (Nod32). Análisis completo en https://www.av-comparatives.org/tests/malware-protection-test-march-2019/.

Imagen 9: Análisis de AV-TEST – Febrero 2019 (av-test.org)

Las mejores soluciones de antivirus a la fecha para Windows 10 son Kaspersky, McAfee, Avast, Symantec y Bitdefender según un estudio realizado

en Febrero del 2019 por el reconocido Instituto de Seguridad IT AV-Test, el cual es independiente y se dedica analizar las diferentes soluciones de Antivirus del mercado basados en tres (3) factores como lo son la protección contra amenazas, rendimiento del ordenador con el Antivirus instalado y la usabilidad, es decir, la sencillez con la que el usuario final lo pueda utilizar y la cantidad de falsos positivos que detecta.

El estudio completo lo pueden ver en su web https://www.av-test.org/es/antivirus/empresas-windows-client/, en la cual también pueden encontrar análisis para otros sistemas operativos como Android y MacOS y son divididos por pruebas para usuarios privados o para empresas.

Imagen 10: Antivirus analizados por AV-TEST – Febrero 2019 (av-test.org)

3. ¿IMPORTANCIA DE UN ANÁLISIS DE MALWARE?

El malware es cualquier software malicioso empleado para causar un perjuicio como bien sea robar información confidencial o valiosa de una

organización o persona, contraseñas, causar mal funcionamiento del sistema, realizar alguna modificación en el equipo sin conocimiento del usuario, evitar que los usuarios accedan a los dispositivos o tomar el control absoluto de la máquina.

Estos programas dañinos tratan de acceder de forma inadvertida por el usuario y por lo general infectan computadores, dispositivos móviles, servidores o una red informática. Algunos tipos de malware de los más conocidos son spyware, adware, phishing, virus, troyanos, gusanos, rootkits, ransomware, Keylogger, entre otros.

El malware es propagado generalmente en forma de enlace o archivo adjunto por correos electrónicos, software fraudulento (warez), páginas webs legitimas vulnerables, USB/CD, redes sociales e Ingeniería Social.

A raíz del aumento constante del malware en la actualidad y la necesidad de saber que daño causa, saber el objetivo o finalidad con que ha sido infectada o intentado infectar una organización o persona se realizan estudios o análisis minuciosos al software dañino enviado para observar las modificaciones o alteraciones que realizó en el sistema y si se realizó alguna conexión de red por parte de este para recibir instrucciones del C&C (centro de control) o enviar información a X destino. Teniendo esta información de antemano se pueden tomar las medidas necesarias para la total desinfección y prevención ante una posible nueva amenaza.

Con un análisis detallado del software malicioso se busca entender cómo funciona, cómo identificarlo y cómo eliminarlo. Uno de los objetivos del análisis suele ser proporcionar la información necesaria para responder a una intrusión. [1]

3.1 TÉCNICAS DE ANÁLISIS DE MALWARE

Existen dos tipos de análisis de malware: estático y dinámico. **En el análisis estático** se busca recopilar la mayor cantidad de información posible sobre el malware en cuestión, se buscan Strings que den pistas sobre qué tipo de malware puede ser, se examina el código con algún desensamblador y depurador de código del mercado, se revisa si esta empaquetado o comprimido, las dependencias entre otras herramientas que den alguna información útil sobre el malware. Toda esta información es recopilada por software específico sin que el software malicioso sea ejecutado, es decir, la PC donde se esté analizando la muestra o el laboratorio no es infectado.

El análisis dinámico a diferencia del estático implica ejecutar el malware, por lo general en un entorno controlado, como un laboratorio virtualizado, para que el Sistema Operativo no sufra ningún tipo de daño y de esta forma poder analizar la actividad del ejecutable dañino y los cambios que produce en la maquina mientras está en ejecución y con ayuda de herramientas especializadas ver las conexiones entrantes y salientes posiblemente del C&C (Comand and Control) los procesos que ejecuta y conocer las posibles alteraciones y modificaciones que realiza el software malicioso en el registro, como el autoarranque, y en el sistema operativo como la eliminación de archivos vitales para el correcto funcionamiento del SO.

4. HERRAMIENTAS DE ANÁLISIS

En la actualidad existen diversas aplicaciones que pueden ser empleadas para analizar un malware en Sistemas Operativos Windows, todo depende del tipo de análisis, estático o dinámico, que se vaya a realizar para escoger los programas informáticos adecuados. Es recomendable implementar los dos tipos de análisis para obtener mejores resultados durante el análisis del archivo.

Una de la suite más conocidas para Windows, la cual posee diversas herramientas que pueden ser utilizadas para analizar software potencialmente dañino es la desarrollada por Mark Russinovich y Bryce Cogswell nombrada Sysinternals[2] , la cual fue adquirida por Microsoft tiempo después.

Las herramientas descritas a continuación se discriminarán según el tipo de análisis. También se mencionarán otras herramientas útiles a la hora de analizar un malware, páginas online de análisis y sandbox, el cual crea una especie de entorno separado del Sistema Operativo principal, es decir, puede ser utilizado para ejecutar software sin que los cambios que produzca en el SO sean permanentes.

4.1 HERRAMIENTAS DE ANÁLISIS ESTÁTICO

A continuación, se describirán algunas de las aplicaciones que pueden ser utilizadas para ejecutar un análisis estático y obtener la mayor información posible de la muestra sin ejecutarla. En este tipo de análisis se busca identificar el archivo, extraer las Strings, determinar las dependencias y analizar el código de la muestra.

4.1.1 IDENTIFICACIÓN DEL TIPO DE ARCHIVO

En esta fase se intenta obtener la mayor información para poder identificar el archivo como: sus hashes, el lenguaje de programación en que fue desarrollado, la firma del archivo (File Signature) para identificar si es un ejecutable, imagen, documento, PDF, etc., si el ejecutable esta comprimido, entre otra información que sea de utilidad.

[2] Sitio Web: https://docs.microsoft.com/en-us/sysinternals/

4.1.1.1 A) Winvi

WinVi[3] es un editor gratuito para Windows, el cual es utilizado como un editor hexadecimal que puede soportar archivos de gran peso ya que utiliza memoria virtual.

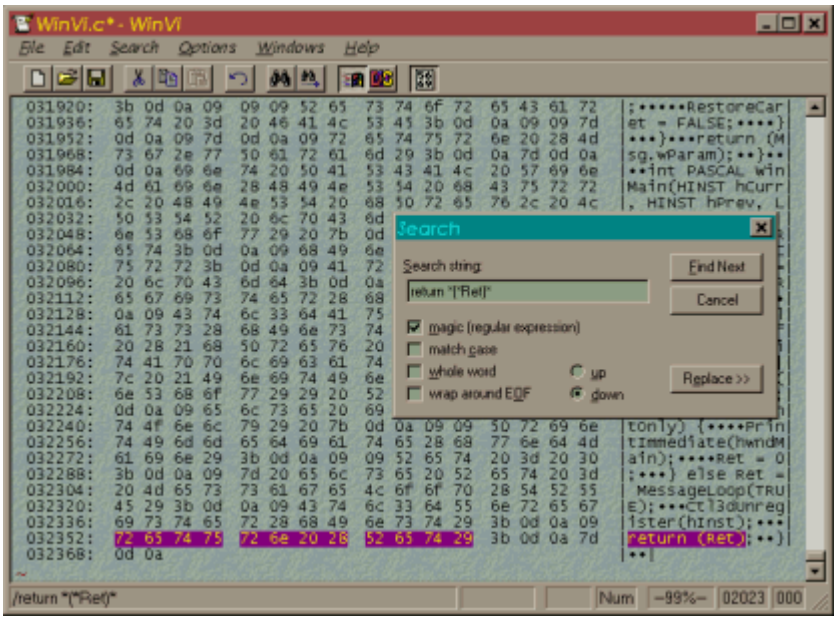


Imagen 11:Pantallazo del programa Winvi (winvi.de)

Esta herramienta nos permite analizar la firma del archivo de la muestra, ayudándonos a identificar el tipo de archivo que vendría siendo: .EXE, .JPG, .DOCX. PDF. RAR, etc.

Por ejemplo, la firma de archivo de un ejecutable de Windows es MZ, cuyo valor hexadecimal es 4D 5A, en la página web https://www.garykessler.net/library/file_sigs.html, la cual es actualizada constantemente, se puede encontrar información con la mayoría de firmas de archivos existentes.

[3] Sitio Web: http://www.winvi.de/es/

Sabiendo la extensión del archivo es posible averiguar o intuir con que programa puede ser ejecutado el archivo. Igualmente, al ver el código de forma hexadecimal se puede conocer si el mismo viene empaquetado o comprimido e investigar como descomprimirlo para que el archivo pueda ser analizado.

4.1.1.2 B) Exeinfo PE

EXEINFO PE[4] es un analizador de ficheros que al igual que WinVi ayuda a identificar la firma del archivo de una forma más sencilla. Además, indica si el archivo esta comprimido o empaquetado y brinda el comando para descomprimir el archivo o la página web del software empleado para comprimirlo y así obtener más información sobre la herramienta utilizada.

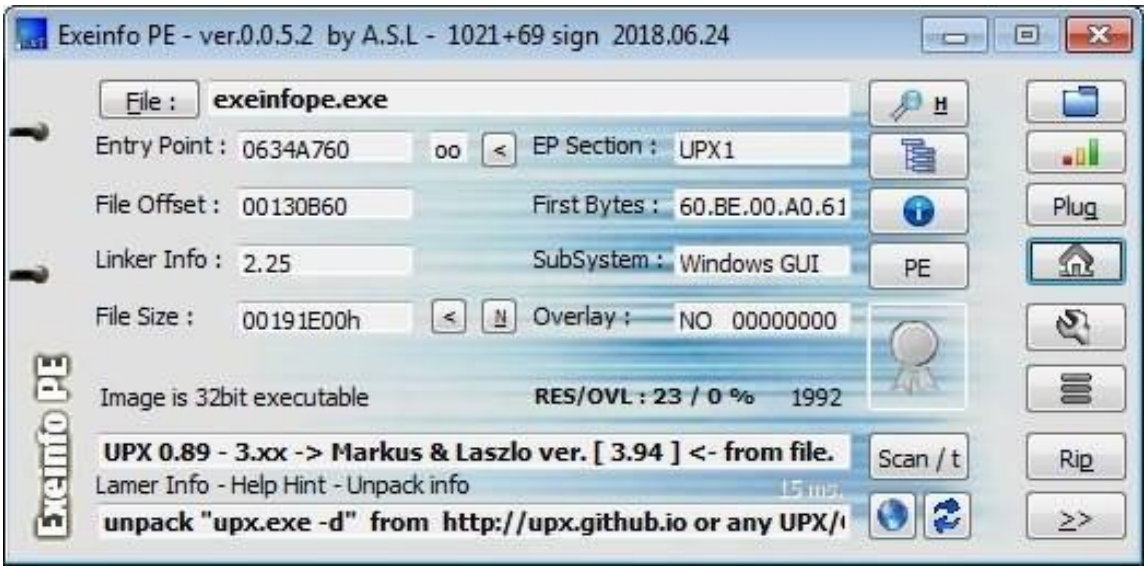


Imagen 12:Pantallazo de Exeinfo (download.cnet.com)

Por lo general se utiliza el compresor de ejecutables UPX para comprimir los ejecutables, ya sea para reducir el tamaño del archivo o para ofuscarlo y pase inadvertido ante los Antivirus. Los compresores son utilizados de forma legítima

[4] Sitio Web: http://www.exeinfo.xn.pl/

por los desarrolladores para reducir el tamaño de su software y ofuscar su código fuente para dificultar su copia o robo.

4.1.1.3 C) FileAlyzer

FileAlyzer[5] es una herramienta de la compañía safer-networking, la misma creadora de Spy&Bot que es un programa el cual funciona desde hace tiempo y funciona de forma gratuita y pago, sirve para eliminar algunos malware, Spyware y Adware. FileAlyzer es una herramienta que permite analizar archivos y capturar metadatos del mismo, brindando información como la fecha de creación, fecha de modificación, fecha de ultimo acceso, lenguaje de programación, compatibilidad con las versiones de Windows, volcado hexadecimal, cabecera PE, y los hashes del ejecutable.

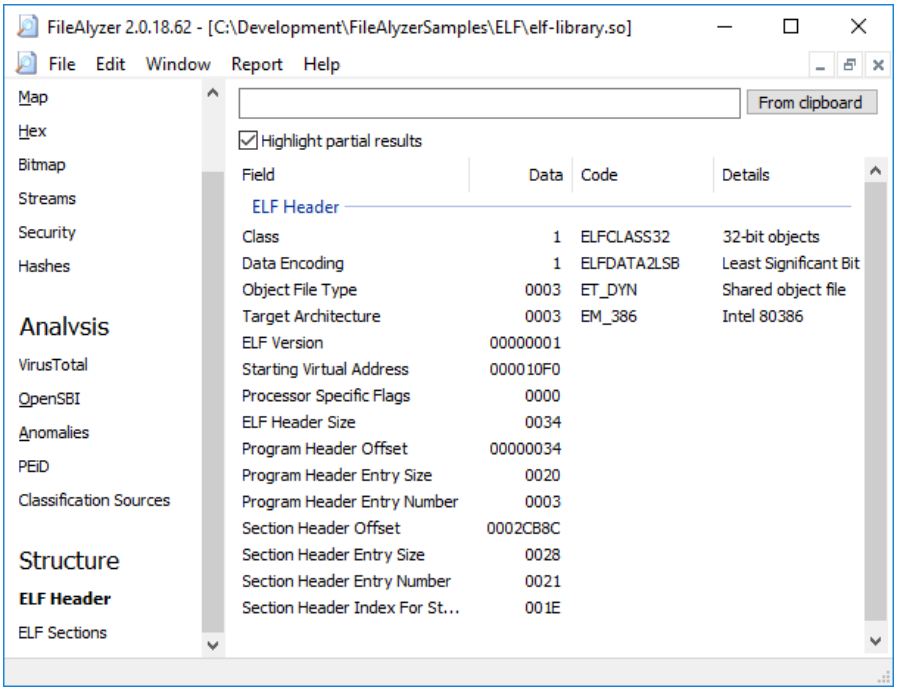


Imagen 13: Pantallazo de FileAlyzer (safer-networking.org)

[5] Sitio web: https://www.safer-networking.org/products/filealyzer/

FileAlyzer te muestra los hashes más comunes como MD5 y SHA-1 si así lo deseas, pero te permite obtener una gran variedad de hashes del archivo analizado en caso tal que lo necesites. Los hashes funcionan como identificación del binario y sirven para diferenciarlos de otros archivos o buscarlo en páginas de análisis por si ya ha sido analizado previamente.

Una vez obtenido el Hash del ejecutable puedes ingresar a páginas como https://www.virustotal.com/#/home/search en el cual colocas el hash y te muestra si el archivo ha sido subido antes y la cantidad de detecciones que obtuvo por parte de los Antivirus.

4.1.1.4 D) RGD Packer Detector

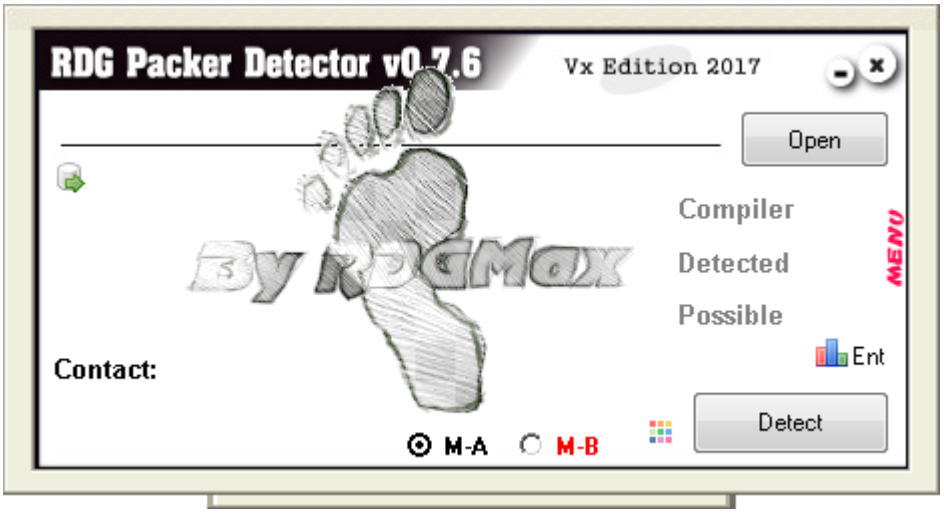


Imagen 14: Pantallazo RGD Packer (rdgsoft.net)

RGD PACKER DETECTOR[6] es un software especializado gratuito capaz de detectar si un archivo ejecutable esta comprimido o encriptado. Su autor lo define como: "… detector de packers, Cryptors, Compiladores, Packers Scrambler, Joiners, Installers." [2]

[6] Sitio Web: http://www.rdgsoft.net/

Además, permite la multi-deteccion de packers, ya que en algunas ocasiones son utilizados varios para reducir el peso del ejecutable lo más posible, evadir algunas firmas de antivirus y dificultar la tarea del análisis.

4.1.2 EXTRACCIÓN DE STRINGS

En esta etapa del análisis se extraen cadenas de texto del archivo examinado en busca de texto plano o legible que no esté ofuscado y aporten información útil como URL, emails, mensajes de error, nombres de archivos, mensajes que pueda mostrar el ejecutable, etc.

4.1.2.1 A) BinText

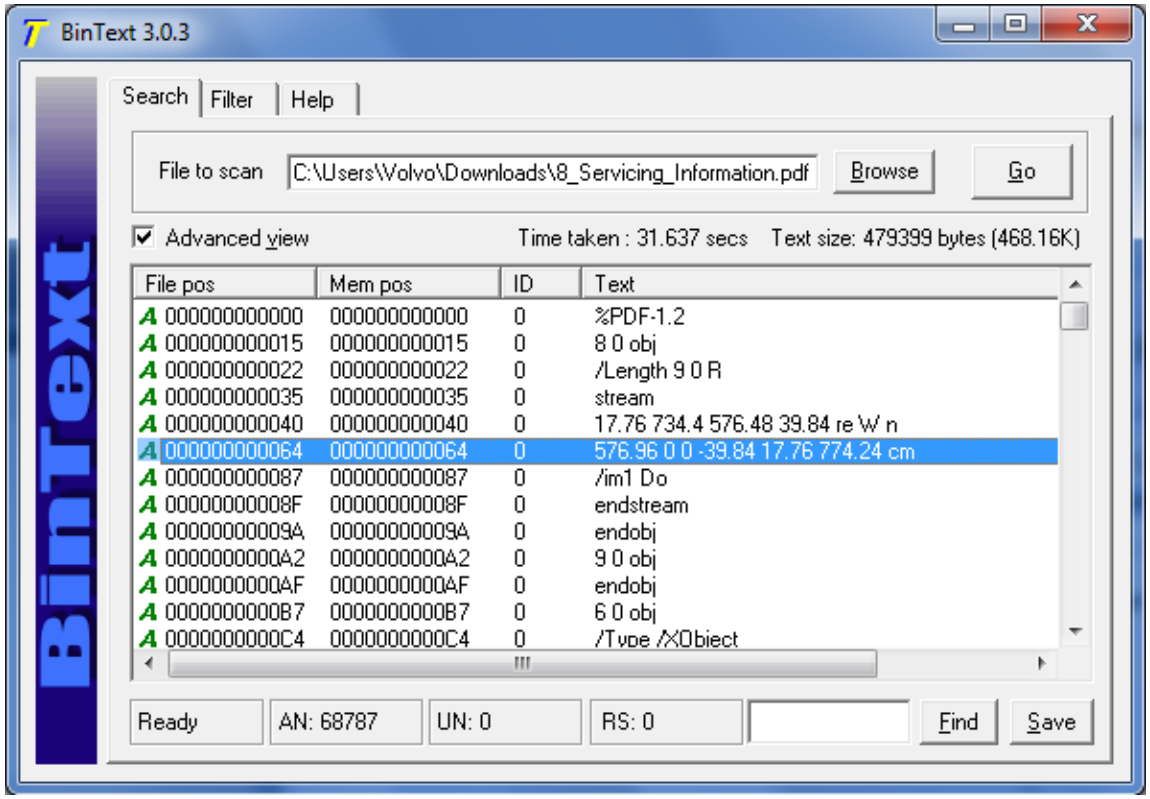


Imagen 15: Pantallazo BinText (bintext.soft32)

BinText[7] es una aplicación gratuita de McAfee, utilizada para realizar búsqueda de cadenas de texto en archivos ejecutables. Es capaz de encontrar texto ASCII, Unicode y cadenas de Recursos. Posee un filtrado que ayuda a excluir de la búsqueda texto no deseado y exportar lo encontrado a un archivo .TXT.

Otra aplicación similar es Strings[8] la cual está incluida en la suite Sysinternals de Microsoft, y al igual que BinText también realiza búsqueda de cadenas de texto UNICODE o ASCII con una longitud mínima de tres (3) caracteres. A diferencia de BinText se ejecuta mediante consola de comando (cmd).

Las cadenas de texto también pueden ser vistas en editores hexadecimales, bien sea WinVi, HXD, entre otros o en descompiladores como OllyDbg e IDA Pro.

4.1.3 ANÁLISIS DE CÓDIGO

En esta fase se emplean herramientas que permiten ver el código ensamblador cuando no se tiene el código fuente del archivo malicioso. Estos programas también son utilizados para desencriptar o descomprimir archivos que tengan esta medida de protección, como UPX o Themida el cual era bastante empleado en un principio para ofuscar el código del ejecutable y saltar la detección de los Antivirus.

Este tipo de herramienta informática también es empleado para hacer ingeniería inversa de un ejecutable, es decir, obtener información de cómo interactúa el archivo, su función y operación. Es recomendable tener algún

[7] Sitio web: https://www.mcafee.com/es/downloads/free-tools/bintext.aspx
[8] Sitio web: https://docs.microsoft.com/es-mx/sysinternals/downloads/strings

conocimiento básico para darle un mejor funcionamiento a este tipo de programas.

4.1.3.1 A) OllyDbg

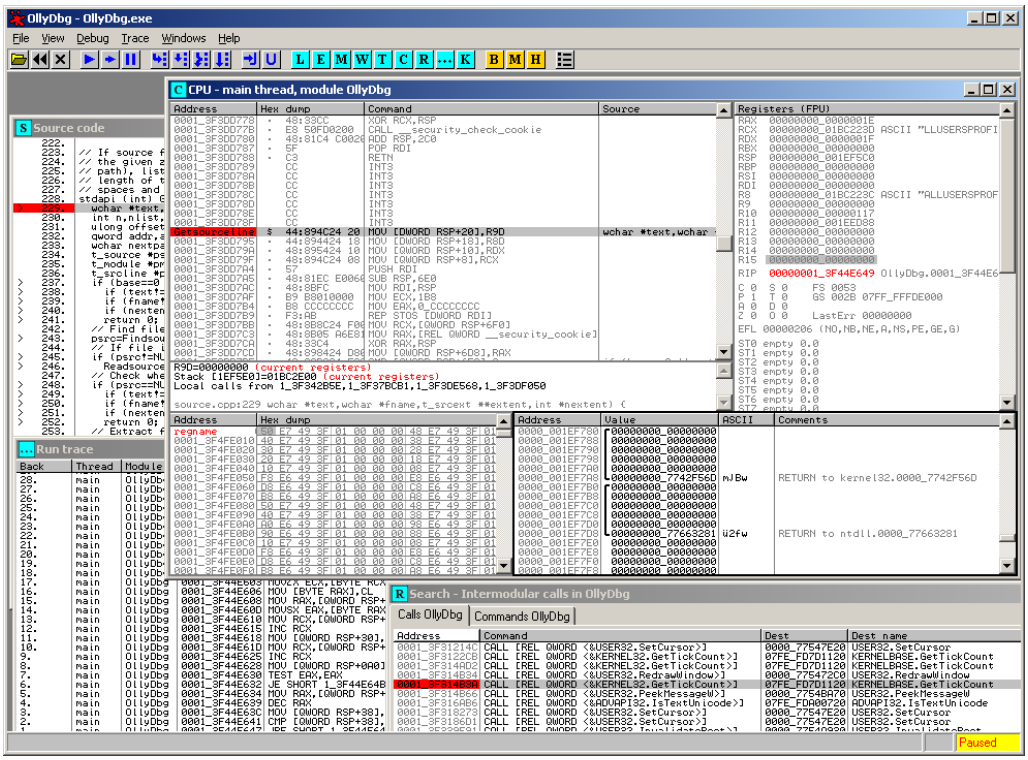


Imagen 16: Pantallazo de OllyDbg (ollydbg.de)

OllyDbg[9] es un depurador que funciona en Sistemas Operativos Windows de 32 Bits. Permite rastrear registros, mostrar las dependencias del ejecutable, reconocer procedimientos, bucles, llamadas API, buscar rutinas de archivos objetos y bibliotecas, muestra la pila, la cabecera PE, edición hexadecimal, soporta complementos de terceros entre muchas funciones más.

[9] Sitio web: http://www.ollydbg.de/

4.1.3.2 B) IDA Pro

IDA Pro[10] al igual que OllyDbd es un depurador y desamblador de archivos binarios y ambos pueden ser empleados para realizar análisis de malware estático y dinámico, se diferencian en que IDA soporta una gran variedad de archivos ejecutables para diversos Sistemas Operativos (SO) y procesadores.

Una ventaja adicional de IDA es que tiene soporte para sistemas de 64 bits y es funcional en sistemas operativos Windows, Linux y MAC OS. Se puede considerar a IDA Pro como una de las herramientas más utilizadas para el análisis de malware por su gran facilidad de uso y la gran cantidad de plugins, SO y procesadores soportados.

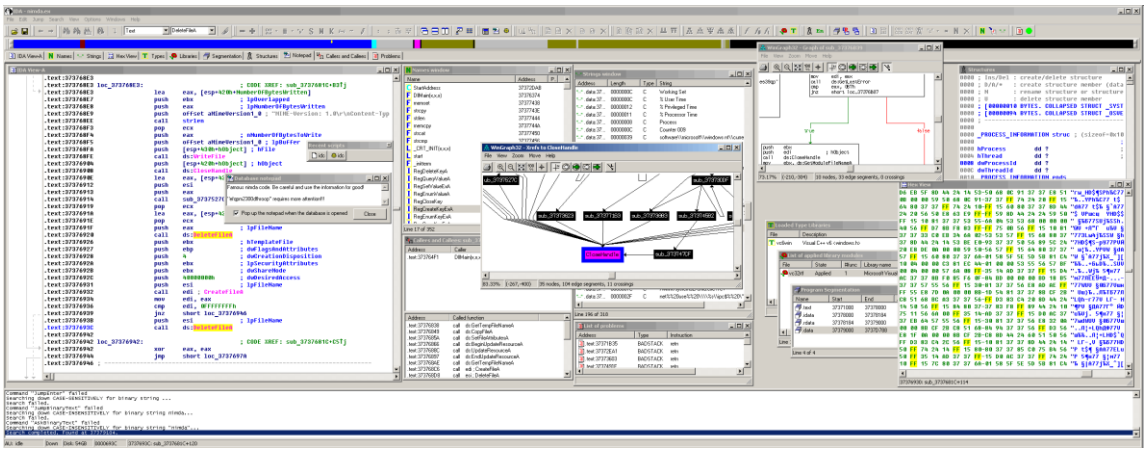


Imagen 17: Pantallazo de IDA PRO (hex-rays.com)

4.1.4 ANALIZANDO DEPENDENCIAS

Con el análisis de dependencias se busca determinar las funciones y librerías (DLL) de las depende o recurre el archivo para ir teniendo alguna claridad sobre su finalidad.

[10] Sitio web: https://www.hex-rays.com/products/ida/

Los .DLL (Dynamic Link Library) son librerías de enlace dinámico las cuales son cargadas a medida que son requeridas por el software e incluso el Sistema Operativo otorgándole así cierta funcionalidad dependiendo de la librería que emplea.

Algunas librerías conocidas que son utilizadas por los programadores de malware son Ntdll.dll, WSock32.dll, Ws2_32.dll, KERNELL32.dll y User32.dll. Estas DLL son empleadas para acceder y modificar la memoria o archivos y crear procesos, acceder a la red, manipular procesos y registrar o administrar servicios.

Las DLL empleadas se puede ver también con algún programa que vuelque Hexadecimalmente el ejecutable solo es buscar la extensión (.DLL).

4.1.4.1 A) Dependency Walker

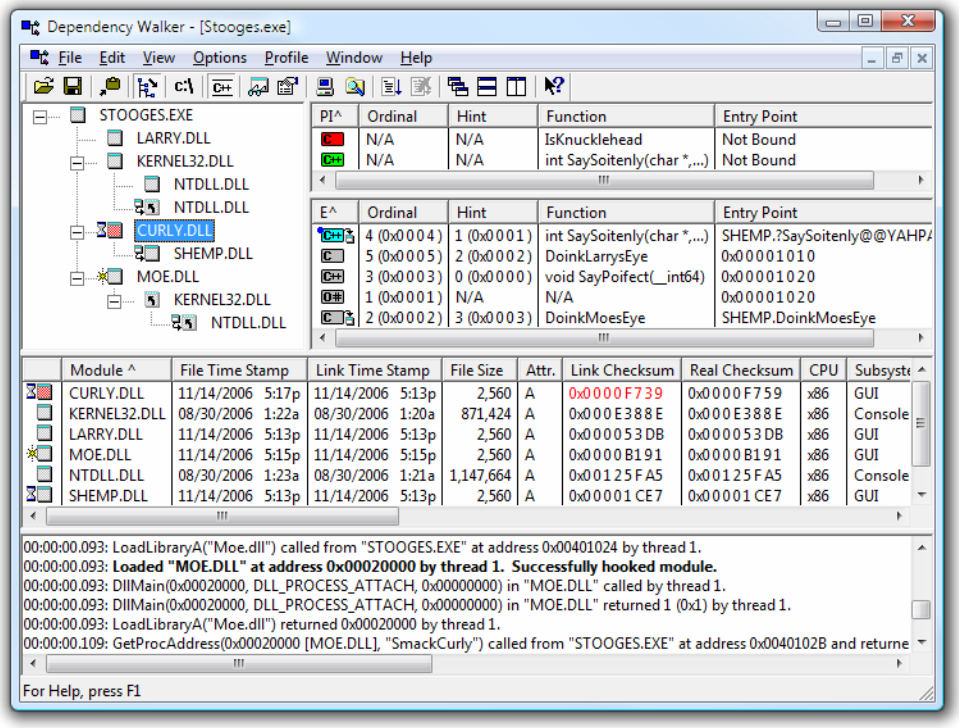


Imagen 18: Pantallazo de Dependency Walker (dependencywalker.com)

Dependency Walker [11]es una aplicación gratis que funciona en Windows de 32 y 64 bits que escanea cualquier modulo, exe, dll, ocx, sys, etc., y crea un diagrama de dependencia del binario analizado, es decir, las librerías que utiliza o invoca en el Sistema. Con las dependencias del archivo se puede ir haciendo una idea del comportamiento del malware dependiendo de las funciones de la API de Windows y las DLL que emplee.

Otra herramienta que tiene la misma función es PE Explorer Dependency Scanner, aunque este si es una utilidad paga y solo funcional con archivos .EXE. Las dependencias de los archivos también se pueden observar en los desambladores/depuradores mencionados anteriormente.

4.2 HERRAMIENTAS DE ANÁLISIS DINÁMICO

En este apartado se detallarán algunas de las herramientas que pueden ser empleadas para realizar una investigación de un archivo mediante un análisis dinámico. Cabe resaltar que en este tipo de análisis la muestra es ejecutada y se recomienda hacerlo en un entorno controlado como en máquinas virtuales de las cuales se hablará en la sección de Otras Herramientas.

Las fases de este tipo de análisis son buscar los procesos del sistema que sean iniciados por la muestra después de su ejecución, examinar el registro para observar si ejecuta algún cambio y realizar un análisis de red o tráfico para ver las conexiones, entrantes o salientes, que hace posterior a su ejecución.

4.2.1 BUSQUEDA DE PROCESOS

En esta fase del análisis se visualizan los procesos actuales del sistema y se observa si se crea o elimina algún proceso después de ejecutar el ejecutable

[11] Sitio web: http://www.dependencywalker.com/

analizado. Así mismo se podrá observar si algún proceso se esconde en otro proceso existente lo cual es una de las técnicas de camuflaje más implementadas por el malware.

4.2.1.1 Process Explorer[12]

Esta herramienta incluida en la suite Sysinternals permite conocer los procesos que se están ejecutando en el sistema. Dependiendo de un color muestra el estado, nuevo, eliminado, suspendido, empaquetado, entre otros, de un proceso.

Por otro lado, permite verificar la legitimidad de la firma del software del ejecutable del proceso, mostrar la clave del registro con el cual va a iniciarse automáticamente con el sistema en caso tal que tenga esta opción el archivo, los privilegios de usuarios con que se ejecuta, el análisis de virus total, el directorio donde se encuentra, si se ejecuta tras un proceso padre, terminar procesos, entre otras funcionalidades que brinda.

Imagen 19: Process Explorer en ejecución (download.cnet.com)

[12] Sitio web: https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer

4.2.1.2 Process Monitor[13]

Es una herramienta solo para Sistemas operativos Windows la cual hace parte de la suite Sysinternals que permite monitorear y filtrar en tiempo real la actividad en el sistema de archivos, el registro, la actividad de las DLL y los procesos que están ejecutándose en el momento.

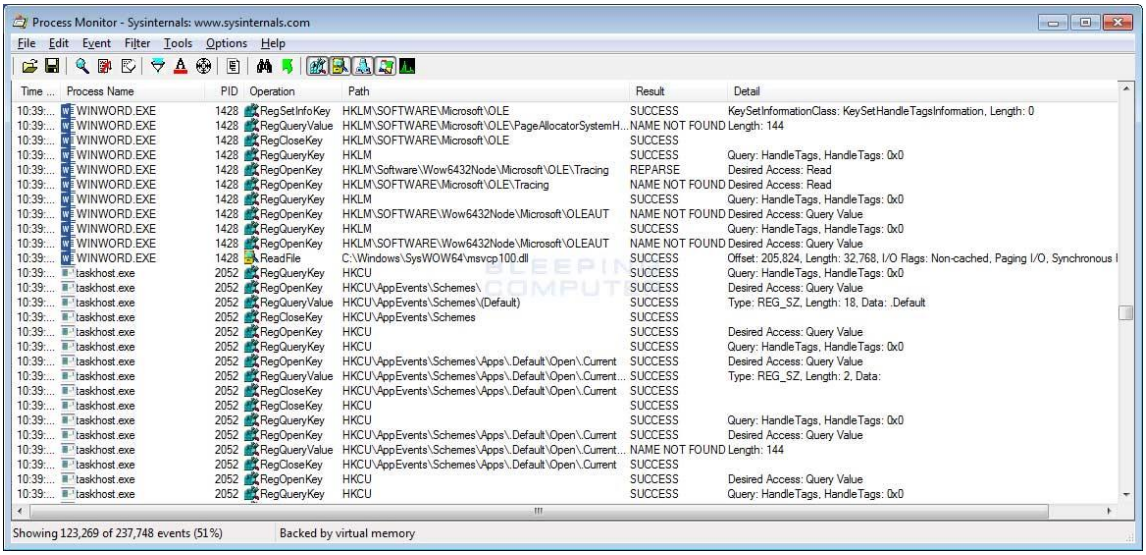


Imagen 20: Process Monitor en ejecución (bleepingcomputer.com)

Los filtros no son destructivos, por lo tanto, cuando se aplique alguno la información restante no se perderá y pueden ser configurables para cualquier campo de datos. Esta herramienta también conocida como procmon de igual forma muestra la actividad de la red, pero es recomendable utilizar otro software un mucho más completo y especializado para este fin.

4.2.1.3 C) Autoruns[14]

Esta herramienta la cual al igual que todas las mencionadas para búsqueda de procesos también pertenece a la suite Sysinternals de Microsoft

[13] Sitio web: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon
[14] Sitio web: https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

permite ver que programas están configurados para ejecutarse automáticamente con el sistema operativo. Además, permite guardar un escaneo y compararlo con uno actual en busca de diferencias.

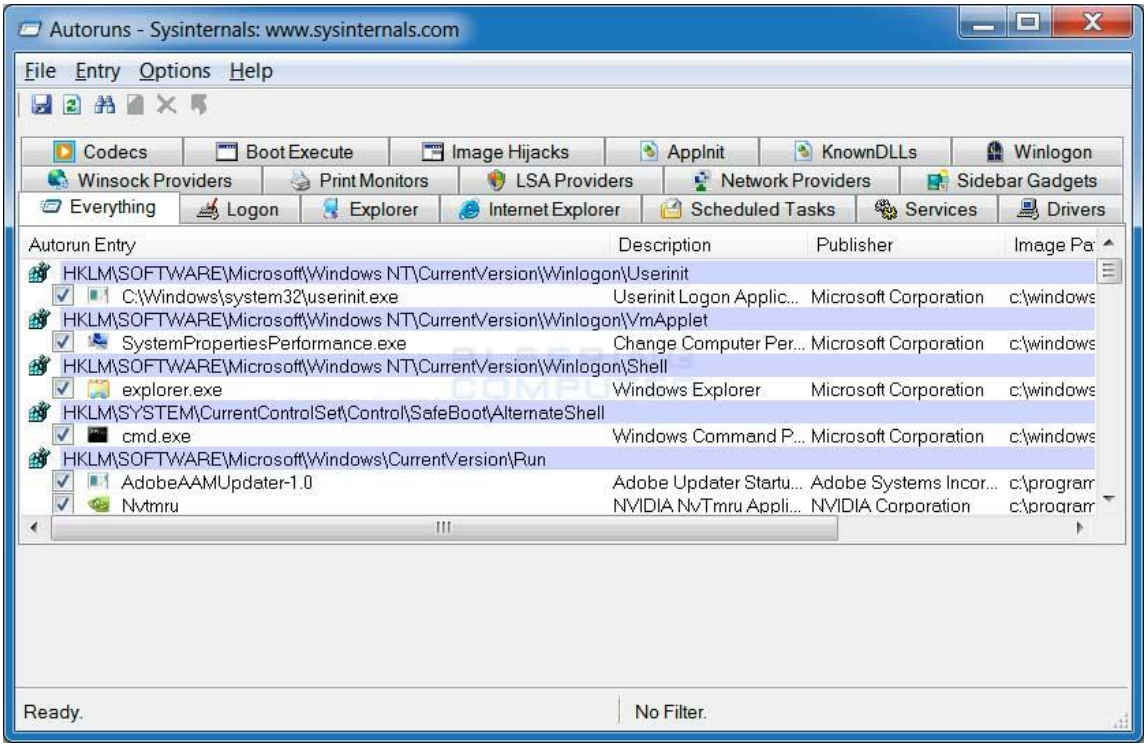


Imagen 21: Pantallazo de autoruns (bleepingcomputer.com)

Mark Russinovich, quien es el desarrollador de autoruns, menciona que "Autoruns informa extensiones de shell Explorer, barras de herramientas, objetos de ayuda del navegador, notificaciones de Winlogon, servicios de inicio automático y mucho más[15]"[3].

También muestra las claves y ubicaciones de registro y los archivos de las aplicaciones y en el paquete de descarga incluye una versión que funciona mediante línea de comando llamada Autorunsc.

[15] Traducción del ingles: Autoruns reports Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more.

4.2.2 ANÁLISIS DE CONEXIONES

En esta etapa del análisis se pretende observar si se realiza algún tipo de conexión por parte del malware, bien sea entrante o saliente y así descubrir las direcciones IP o URL a las cuales intenta acceder en busca de ordenes/instrucciones, envío de información, descarga de otros archivos, actualizaciones, etc.

4.2.2.1 A) TCPview[16]

Herramienta que pertenece y puede ser descargada de la suite Sysinternals la cual permite ver las conexiones TCP y UDP del sistema y el estado de las mismas. Este programa también permite ver las direcciones locales, remotas y el nombre del proceso que realiza o realizó la conexión.

TCPview permite cerrar conexiones desde su interfaz y es empleado en el análisis de malware para ver las conexiones. Al igual que Autoruns el paquete de descarga incluye Tcpvcon la cual es una versión que funciona desde la línea de comandos.

A) Wireshark[17]

Es el analizador de protocolo de red más consumido por los investigadores, es de código abierto y al igual que TCPview captura el tráfico de red y permite analizarlo, posee muchas funciones y filtros lo cual lo convierte en una de las herramientas más utilizadas y completa de su tipo.

Es un programa multiplataforma ya que se ejecuta en varias Sistemas Operativos incluyendo Windows, Linux, Mac, entre otros, además permite el

[16] Sitio web: https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
[17] Sitio web: https://www.wireshark.org/

análisis de varios protocolos. En resumidas cuentas, “Wireshark proporciona visualización, análisis de flujo de paquetes y análisis en profundidad de paquetes individuales”[18][4].

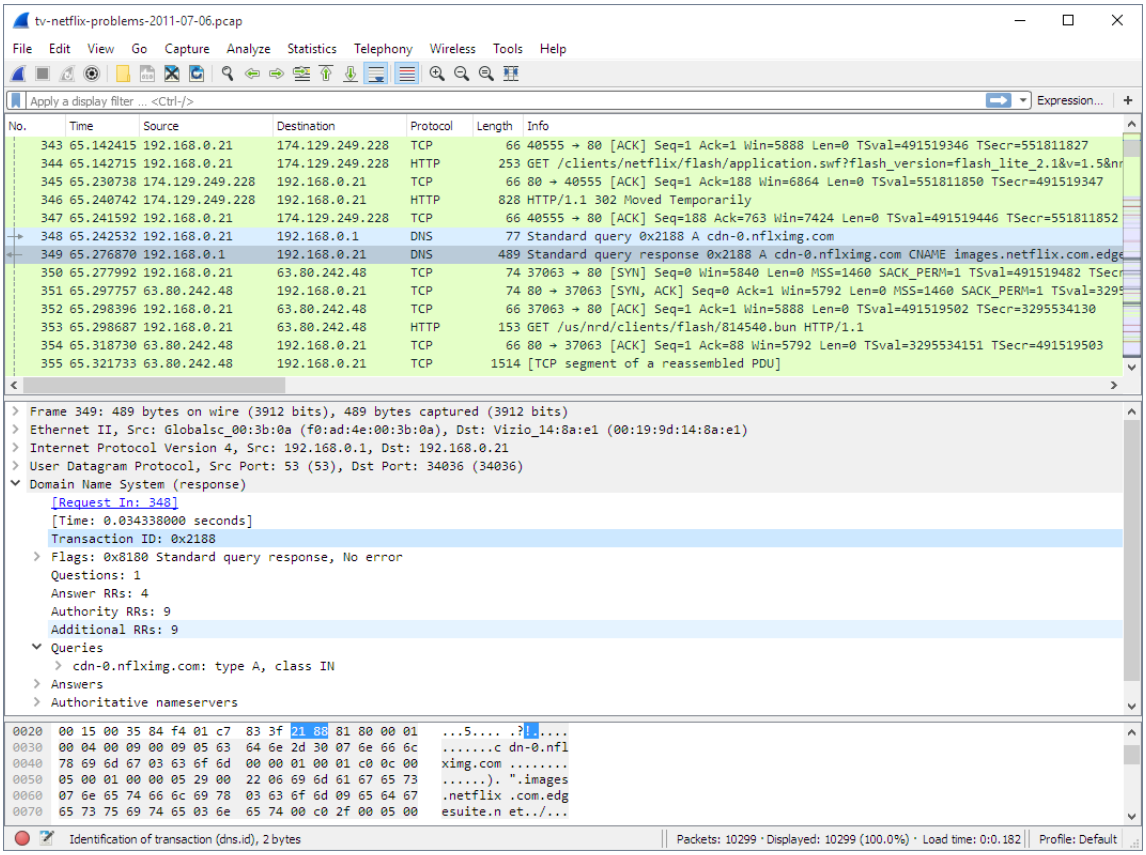


Imagen 22: Pantallazo de Wireshark (wireshark.org)

B) FakeNet[19]

Es una herramienta que emula un servidor remoto empleado por el malware para que este siga ejecutándose y poder observar su actividad de red.

Además entre otras funcionalidades soporta los protocolos DNS, HTTP y SSL, extensiones de Python para agregar nuevos protocolos y permite la

[18] Traduccion del ingles: Wireshark provides visualization, packet-stream analysis, and in-depth analysis of individual packets.
[19] Sitio web: https://practicalmalwareanalysis.com/fakenet/

creación de archivos de captura de paquetes (.pcap) para que sean analizados posteriormente.

La última actualización de esta herramienta fue el 29 de mayo del 2013, es funcional en Windows Vista / 7 pero algunas funciones se desactivan y es completamente funcional en WinXP Service Pack 3, por lo cual el equipo de FireEye (Mandiant) desarrolló su propia herramienta basada en FakeNet llamada FakeNet-NG[20], la cual soporta las últimas versiones de Windows y Linux.

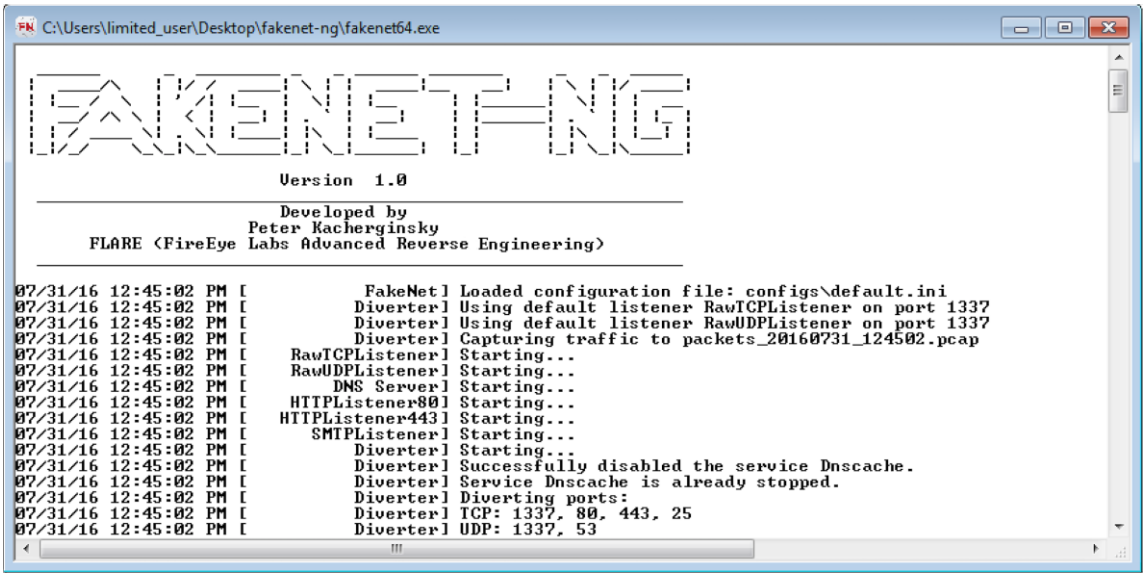


Imagen 23: Pantallazo de Fakenet (fireeye.com)

4.2.3 ANÁLISIS DE REGISTRO.

En esta etapa del análisis se busca identificar los cambios que realiza el malware en el registro del sistema operativo, como la creación de alguna clave para garantizar su persistencia en la máquina e iniciar cada vez que esta sea encendida o reiniciada, lo cual es realizado por la mayoría de los malware para ejecutarse cada vez que se encienda la PC de la víctima.

[20] Sitio web: https://www.fireeye.com/services/freeware/fakenet-ng.html

4.2.3.1 A) Regshot[21]

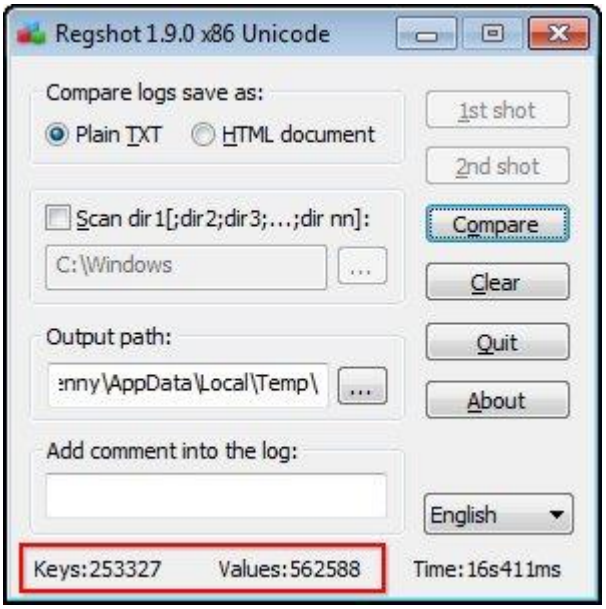


Imagen 24Pantallazo de Regshot (howtogeek.com)

Es una utilidad gratuita que permite realizar una instantánea del registro del sistema antes y después de realizar alguna acción en el Sistema Operativo, para luego ser comparadas y así poder observar los cambios que se realizaron en el sistema durante su ejecución. El informe de la herramienta puede ser guardado en formato TXT y HTML.

Otro programa similar a Regshot es Active Registry Monitor (ARM), el cual puede ser descargado de https://www.devicelock.com/es/arm/

4.3 VIRTUALIZACIÓN

La virtualización es la simulación de un entorno informático o virtual, como puede ser un sistema operativo, dispositivos de almacenamiento, hardware, etc

[21] Descarga: https://sourceforge.net/projects/regshot/

el cual logra trabajar de forma independiente del anfitrión, es decir, de la maquina o Sistema Operativo principal.

Se puede particionar un disco en X cantidad de máquinas virtuales e instalar el SO deseado, los cuales emplearan los recursos de la maquina física por lo cual hay que tener cuidado en la configuración para no extralimitarse y causar mal funcionamiento a la maquina principal.

La autonomía de las máquinas virtuales nos garantiza que nuestro sistema operativo principal y entorno de red no se vean afectado a la hora de analizar un malware, ya que si se desea se puede emplear FakeNet para simular una conexión. Otra de las ventajas es que los discos duros de estas actúan como especie de un contenedor, por lo cual se pueden congelar, respaldar, transportar y copiar.

Se puede guardar el estado de una maquina a través de las instantáneas, permitiendo así que se realice un análisis de malware y si sale algo mal volver al estado anterior de la máquina. Se pueden realizar tantas instantáneas como se deseen.

A continuación, se describirán dos de los programas más conocidos y empleados en el mercado:

4.3.1 VIRTUAL BOX[22]

Es un programa de virtualización perteneciente a la empresa Oracle el cual puede ser ejecutado en Windows, Linux, Mac y Solaris, convirtiéndolo así en una aplicación multiplaforma. Además, es compatible con arquitecturas de X32 - X64 bits y puede ser usado tanto a nivel empresarial como doméstico de forma gratuita.

[22] Sitio web: https://www.virtualbox.org/

Esto quiere decir que puede ejecutar un SO Mac en un SO Windows. Puede instalar tantos Sistemas operativos como desee, la única limitación es el disco duro y la memoria del PC principal ya que se toman los recursos de este.

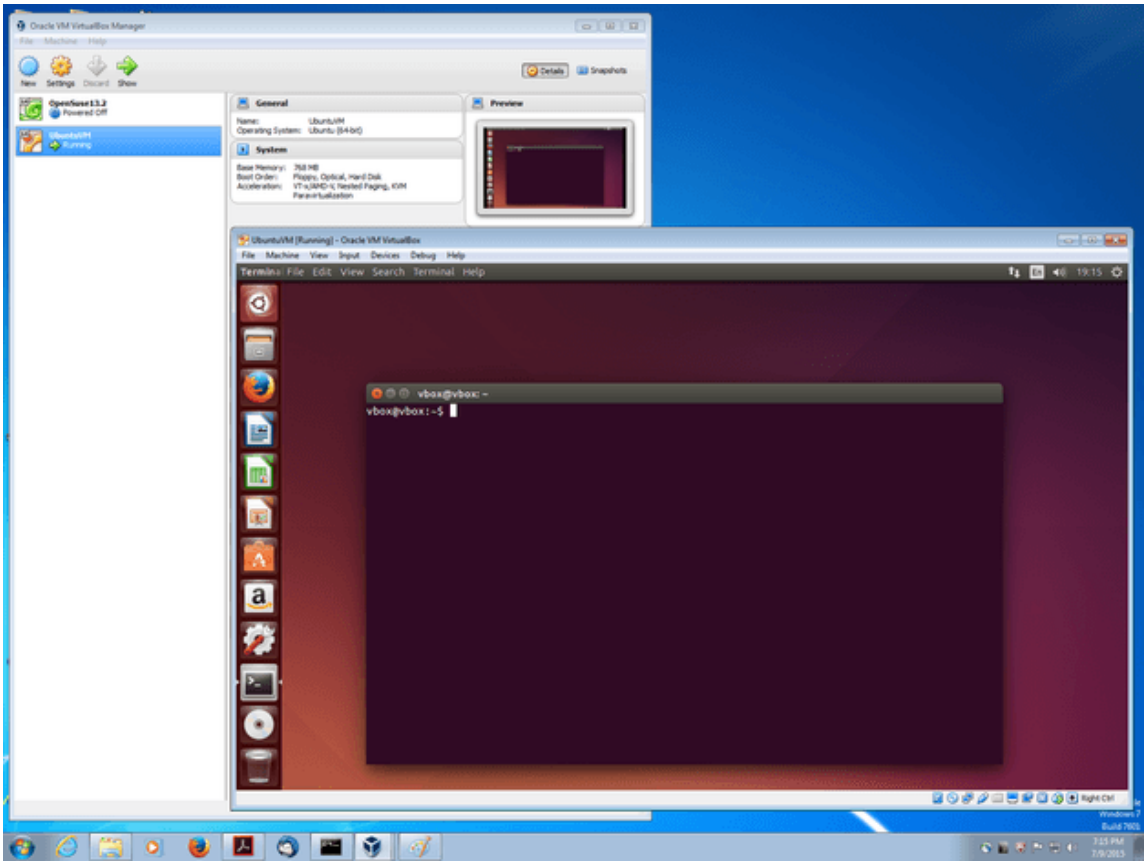


Imagen 25: Virtual en maquina Windows ejecutando Ubuntu (virtualbox.org)

La herramienta posee una documentación completa, donde explican cómo crear una máquina virtual, los sistemas operativos admitidos, toma de instantáneas, clonación, eliminación, importación, exportación de máquinas virtuales y otras características que posee este software, el cual es recomendable leer para aprovechar todas las características que posee. Puede ser leído en https://www.virtualbox.org/manual/ch01.html

4.3.2 VMWARE WORKSTATION[23]

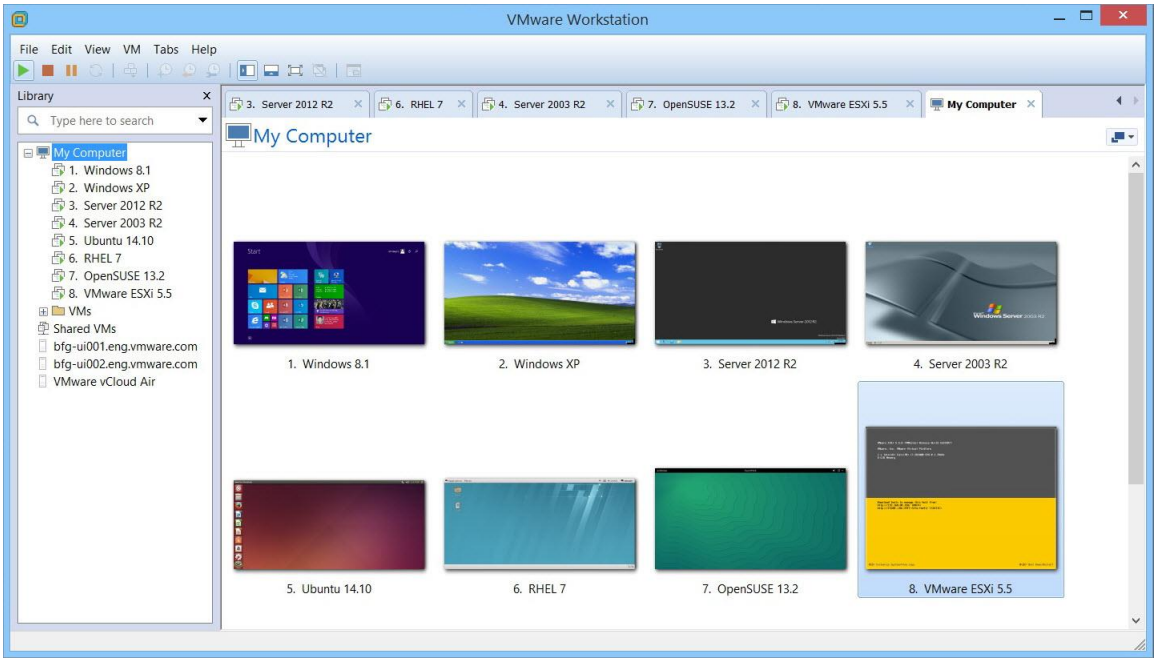


Imagen 26: VMWARE virtualizando varios SO (blogs.vmware.com)

Al igual que Virtual Box es un software de virtualización que permite instalar y ejecutar varios sistemas operativos en una única PC, con la diferencia que este solo funciona en Windows y Linux de 64 Bits.

Workstation Player es la versión gratuita de VMWare Workstation el cual no cuenta con características relevantes como la toma de instantáneas para restaurar el SO a un punto anterior y la clonación de máquinas virtuales.

VMWare posee una extensa y detallada documentación al igual que Virtual Box y si se compra la licencia de su versión PRO obtiene un soporte especializado por si llega a ocurrir algún inconveniente o se presenta alguna duda con la herramienta.

[23] Sitio web: https://www.vmware.com/latam/products/workstation-pro.html

4.4 OTRAS HERRAMIENTAS

En este segmento se describirán otras herramientas que pueden ser de gran ayuda en el análisis de programas dañinos. Algunas de las mencionadas tendrán funcionalidades de programas mencionados anteriormente en este trabajo e incorporan utilidades para el análisis estático y el análisis dinámico del malware.

4.4.1 CFF Explorer

CFF Explorer[24] es un producto desarrollado por NTCore para la inspección de programas PE de 32 y 64 bits, pero además presenta otras funcionalidades que fueron explicadas anteriormente como editor hexadecimal, desensamblador, walker de dependencias, tipo de archivo, visor de procesos, visor de drivers, entre otras características que pueden ser leídas en la web del autor http://www.ntcore.com/exsuite.php.

Asimismo, con este software se puede obtener información del archivo al igual que Filealyzer. Lo que lo diferencia de otros programas es que soporta edición, vista de código y vista de estructuras de .NET. CFF Explorer tiene una versión de pago llamada Cerbero Profiler.

4.4.2 SYSTEMINFO[25]

Comando incluido en Windows por medio del cual podemos obtener información detallada de la PC, como el sistema operativo y la versión del mismo, el fabricante, modelo y tipo del sistema (32, 64 Bits), procesadores instalados,

[24] Sitio web: http://www.ntcore.com/exsuite.php
[25] Sitio web: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo

versión del BIOS, Revisiones instaladas y demás características de seguridad, identificación del producto y propiedades del hardware presente en la máquina.

Esto es útil si queremos hacer una copia exacta de la PC en una máquina virtual y proceder analizar un malware que ataque configuraciones especificas ya que en ocasiones están programados para ser ejecutados solamente bajo ciertas condiciones.

Una herramienta que cuenta con las mismas características de SYSTEMINFO pero que se puede manejar por interfaz gráfica es SIW (System Information for Windows).

4.4.3 SSDEEP[26]

Programa funcional a través de la línea de comandos de Windows capaz de comparar el hash de dos archivos. Con este procedimiento se puede llegar a saber si el malware que se está investigando es similar a alguna muestra anterior o si es parecido y solo presenta algunas pequeñas modificaciones.

Una vez que se obtenga el hash se puede buscar información en línea, como, por ejemplo, en virustotal.com el cual almacena los hashes de archivos que ya han sido subidos para su análisis por otros usuarios o simplemente se puede colocar en el buscador de preferencia en busca de un resultado.

4.4.4 SYSINSPECTOR[27]

Es una herramienta gratuita creada por ESET, los mismos desarrolladores del antivirus Nod32 y otras herramientas al servicio de la seguridad virtual, la cual

[26] Sitio web: https://ssdeep-project.github.io/ssdeep/
[27] Sitio web: https://www.eset.com/ar/soporte/diagnostico-de-pc-gratuito/

realiza un screenshot o instantánea de los procesos en ejecución, registro, conexiones de red y elementos de inicio de los sistemas operativos Windows.

Otras características expuestas por los desarrolladores son:

- Capacidad para generar y guardar un registro detallado que será usado por un técnico o para ser subido a un foro en línea para su discusión. [5]
- Opción para excluir a la información privada o personal de ser guardada en los registros. [5]
- La Tecnología Anti-Steath integrada permite descubrir objetos ocultos (por ejemplo, rootkits) en el MBR, entradas de registros, controladores, servicios y procesos. [5]
- La capacidad para comparar dos registros existentes para facilitarla detección de cambios. [5]
- Las entradas de registros se le asigna un código de color por nivel de riesgo para un fácil filtrado. [5]
- Navegación jerárquica intuitiva de los registros. [5]
- Archivo ejecutable único, rápido y compacto, ideal para las primeras respuestas desde una unidad USB sin instalaciones extensas. [5]

Esta herramienta está disponible para sistemas operativos Windows de 32 y 64 bits y no requiere muchos recursos para su uso. Se encuentra integrada en soluciones de la compañía como ESET NOD32 Antivirus, ESET Internet Security y ESET Smart Security Premium, pero también funciona de forma independiente y se haya en línea para su descarga gratis en https://descargas.eset.es/eset-sysinspector

4.4.5 SYSANALYZER[28]

Es una aplicación realizada por David Zimmer empleada para el análisis de malware. Esta herramienta presenta funciones de análisis estático y análisis dinámico, cabe resaltar que la muestra es ejecutada por sysanalyzer para su análisis, por lo tanto, es recomendable realizarlo en un entorno seguro.

[28] Sitio web: http://sandsprite.com/iDef/SysAnalyzer/

Sysanalyzer recopila, compara e informa el análisis de una muestra de forma automática. Esto es posible ya que el programa hace capturas/ instantáneas durante el tiempo determinado por el usuario antes de iniciar con el estudio de la muestra.

Durante el intervalo de tiempo que se esté ejecutando el análisis este capturará los procesos en ejecución, los DLL cargados en explorer.exe (proceso fundamental del sistema encargado de la parte grafica) e iexplorer.exe (proceso de internet explorer), puertos abiertos y el proceso asociado a este, modificaciones de los archivos, tareas programadas y controladores cargados en el kernel.

Sysanalyzer es compatible en sistemas operativos Windows 2000 hasta Windows 10 ya sean arquitectura de 32 o 64 bits. Puede ser descargado en http://sandsprite.com/iDef/SysAnalyzer/index.html

El proyecto pertenece a IDefense, pero ya no cuenta con soporte por parte de la empresa por lo tanto su autor principal, David Zimmer, ha seguido este proyecto de forma independiente.

4.4.6 4N4LDETECTOR[29]

Es una herramienta creada por Germán Sánchez Garcés, la cual es empleada para el análisis de archivos ejecutables de sistemas operativos Windows la cual funciona mediante la extracción de strings UNICODE y ANSI y si se desea se puede activar también el volcado de memoria.

Posee una lista de las Strings que se quieran extraer del ejecutable y también la opción de analizarlo en Virus Total, que tiene como función analizar

[29] Sitio web: http://www.enelpc.com/p/4n4ldetector.html

URL y archivos que se le suministren, como en este caso, con varios motores de antivirus (más de 60 antivirus) entre los que se encuentran los más populares del mercado.

Esta aplicación permite extraer información sobre: Información de la PE, posibles funciones maliciosas, claves de registros, acceso a los archivos, arquitectura, Anti-VM / Sandbox / Depuración, extractor de URL, lista de IP / Dominios, correos electrónicos y otra serie de funciones que pueden ser vista en la ayuda de la herramienta.

El sitio web del autor es http://www.enelpc.com/, en este también se pueden encontrar otra serie de herramientas desarrolladas por él y tutoriales sobre métodos y herramientas para la evasión de antivirus.

4.5 ESCANERES ONLINE

Existen páginas web gratuitas al servicio de la comunidad que permiten realizar el análisis de archivos en pro de conocer si están infectados o son ejecutables limpios. Este tipo de páginas webs también pueden funcionar como referencias de archivos que ya han sido analizados previamente ya que almacenan los hashes de los archivos.

En este apartado del documento se mencionarán algunas webs que facilitan este servicio de manera online permitiendo el análisis de archivos, PDF, APK e incluso URL que parezcan dudosas.

Las webs descritas a continuación combinan los tipos de análisis estáticos y dinámicos para brindar un mejor servicio y ayudar a identificar la muestra y su comportamiento en caso tal sea un malware.

4.5.1.1 VIRUSTOTAL

Sitios webs como **https://www.virustotal.com** permiten el análisis estático de varios antivirus de archivos y URL de forma Online, una vez culminado el análisis muestra el resultado dividido en las pestañas: detección, detalles, comportamiento y comunidad.

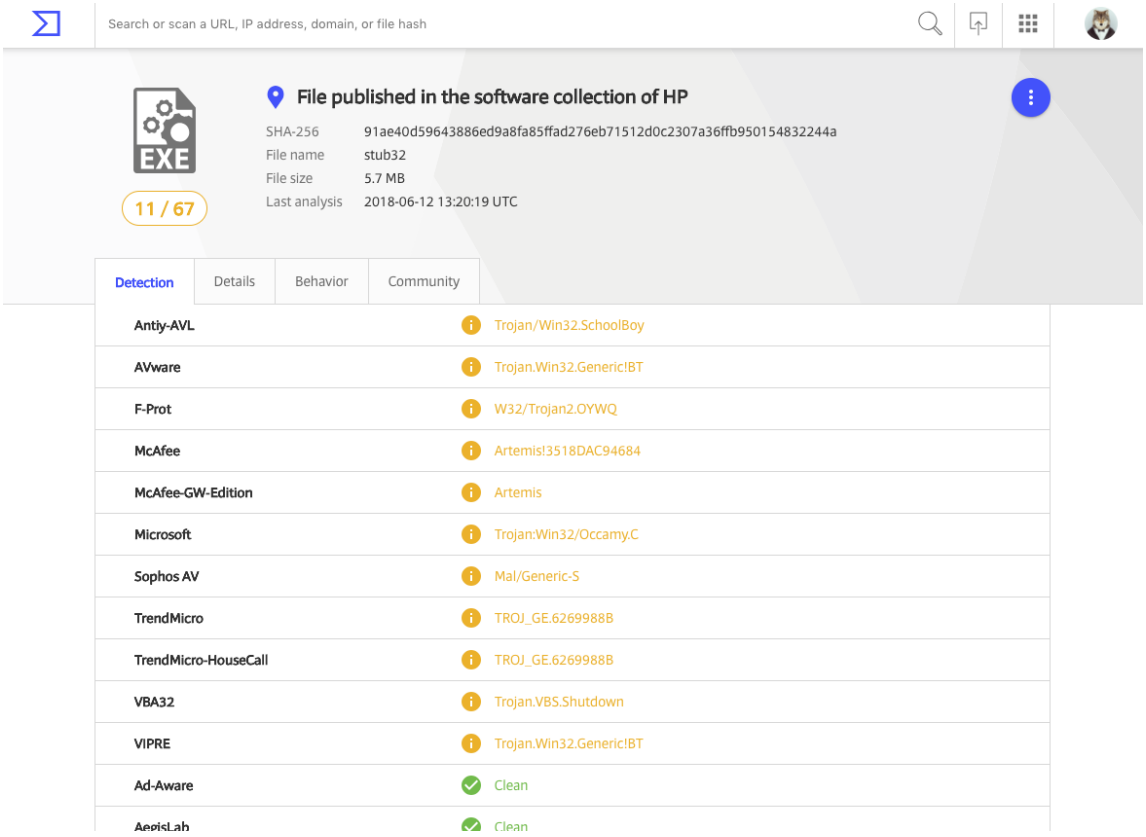


Imagen 27: Página mostrada por Virustotal despues de un análisis (blog.virustotal.com)

La pestaña **"Detección"** cuenta con más de 60 motores de antivirus que a su vez muestran el resultado del escaneo realizado, en los cuales se encuentran los más populares del mercado como Avast, ESET-NOD32, Kaspersky, AVG, McAfee, Symantec, Bitdefender, entre muchos otros.

En la parte de **"Detalles"** se muestra información del archivo como el hash, el tipo y el tamaño del archivo. También muestra la fecha de la primera y

última vez que subieron el archivo para su análisis, el nombre de las secciones que posee el ejecutable y otra serie de información que puede ser útil como referencia en el estudio del archivo dañino.

En la pestaña de **"Comportamiento"** se muestra las acciones del sistema de archivos realizadas por el ejecutable como la creación, lectura, modificación o eliminación y los módulos cargados por el mismo.

Virus total es propiedad del gigante de la internet Google y como es conocido la compañía está comprometida con hacer del Internet un lugar seguro para todos, por lo tanto, además de ayudar a los usuarios a identificar malware, colabora con las compañías de antivirus, ya que, cada muestra que es analizada en esta página web es enviada a dichas empresas, por lo cual si resulta ser un malware las mismas le colocan una firma que se verá reflejada en la próxima actualización de su base de datos.

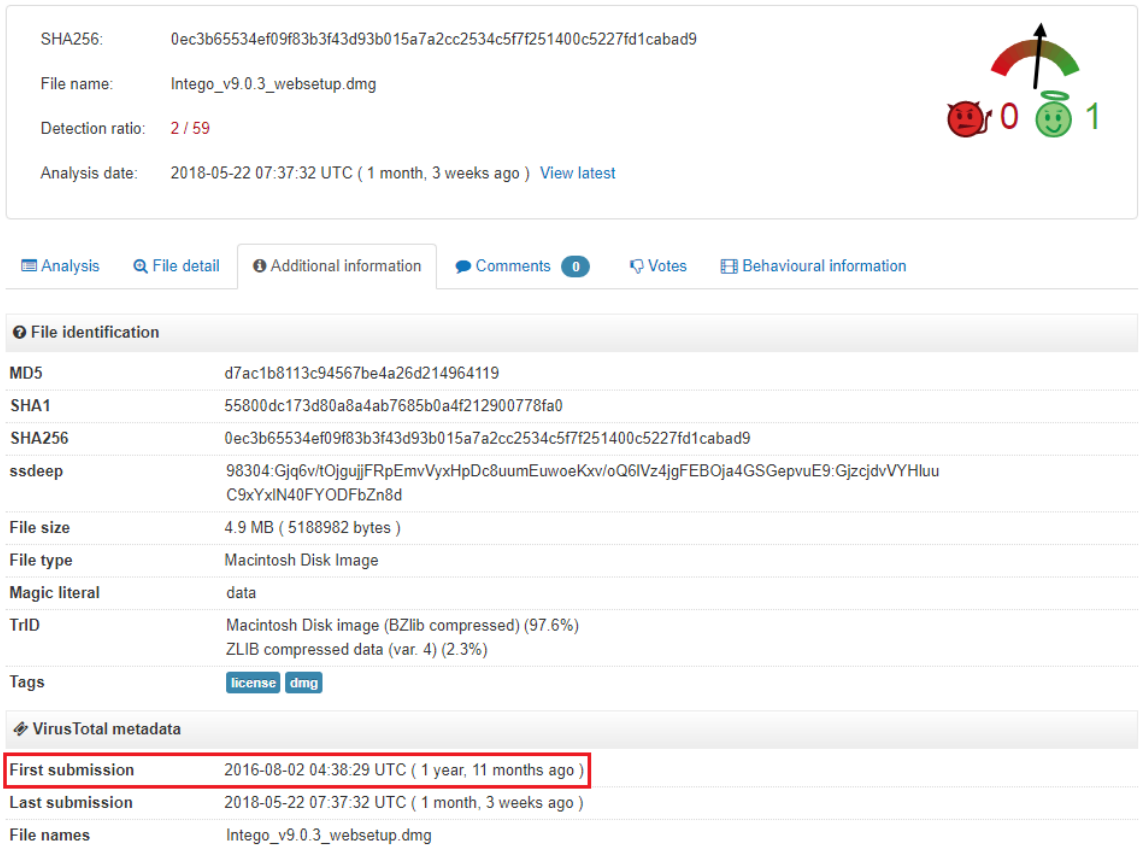
Páginas webs como http://www.virscan.org/language/en/ y https://virusscan.jotti.org/ con 37 y 16 motores de antivirus respectivamente solo permiten el análisis de ejecutables y en su resultado solo muestran los resultados arrojados por los diferentes antivirus con los que cuenta cada una de estos sitios.

4.5.1.2 HYBRID ANALYSIS

La página web https://www.hybrid-analysis.com/ desarrollada por Hybrid Analysis[30] al igual que la web anterior presta un servicio de análisis de malware automatizado gratuito. Este sitio emplea Falcon Sandbox de back-end para el análisis, el cual es de su propiedad. VxStream Sandbox es la versión de pago de la compañía.

[30] Sitio web: https://www.payload-security.com/

Hybrid-Analysis.com además de realizar el estudio de archivos ejecutables, permite el análisis de otros tipos de archivos como PDF, APK, Office, EML con un tamaño máximo de 100 MB.



SHA256:	0ec3b65534ef09f83b3f43d93b015a7a2cc2534c5f7f251400c5227fd1cabad9
File name:	Intego_v9.0.3_websetup.dmg
Detection ratio:	2 / 59
Analysis date:	2018-05-22 07:37:32 UTC (1 month, 3 weeks ago) View latest

File identification

MD5	d7ac1b8113c94567be4a26d214964119
SHA1	55800dc173d80a8a4ab7685b0a4f212900778fa0
SHA256	0ec3b65534ef09f83b3f43d93b015a7a2cc2534c5f7f251400c5227fd1cabad9
ssdeep	98304:Gjq6v/tOjgujjFRpEmvVyxHpDc8uumEuwoeKxv/oQ6lVz4jgFEBOja4GSGepvuE9:GjzcjdvVYHluu C9xYxlN40FYODFbZn8d
File size	4.9 MB (5188982 bytes)
File type	Macintosh Disk Image
Magic literal	data
TrID	Macintosh Disk image (BZlib compressed) (97.6%) ZLIB compressed data (var. 4) (2.3%)
Tags	license dmg

VirusTotal metadata

First submission	2016-08-02 04:38:29 UTC (1 year, 11 months ago)
Last submission	2018-05-22 07:37:32 UTC (1 month, 3 weeks ago)
File names	Intego_v9.0.3_websetup.dmg

Imagen 28: Detalles del análisis mostrados por hybrid-analysis (securelist.com)

Esta web presenta más opciones al momento de analizar el archivo sospechoso, ya que, permite escoger el sistema operativo deseado para que sea ejecutado la muestra entre Windows 7 de 32/64 bit, Linux (Ubuntu 16.04, 64 bit), o un análisis estático de Android.

Otras opciones de análisis con la que cuenta esta web es la secuencia de comandos para tratar de imitar el comportamiento humano, duración del tiempo de ejecución, contraseña del documento es caso tal que esté protegido, habilitar

anti evasión, registro de scripts y otras opciones que pueden ayudar a brindar un informe más detallado.

Además, suministra la opción de permitir el acceso a la muestra por parte de terceros, que la comunidad de miembros acceda a ella y enviar la notificación del análisis completo a un correo electrónico suministrado por el usuario.

4.6 SANDBOX

Es un programa o aplicativo que permite aislar el Sistema operativo principal, protegiéndolo de una posible infección durante la ejecución de un análisis dinámico. Esto debido a que se les restringe el espacio en disco y de memoria y no pueden acceder a otras partes que no les haya sido asignada. De igual forma es posible configurarlos para limitarles el acceso a dispositivos externos, servidores de red, de sonido e incluso se puede configurar que se ejecuten en un sistema de archivos temporal.

4.6.1 CUCKOO SANDBOX

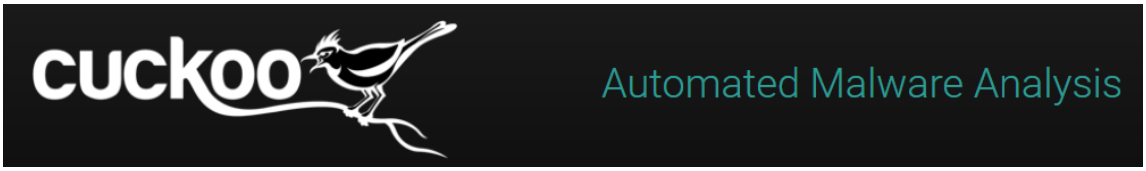


Imagen 29: Logo del Sandbox Cuckoo

Es un framework de código abierto desarrollado por Claudio “nex” Guarnieri que automatiza el trabajo de analizar un archivo sospechoso de ser malware en sistemas operativos Windows, Linux, Mac OS X y Android.

Este sandbox tiene un enfoque de análisis dinámico. Registra y almacena para su posterior informe los cambios que se realicen en el registro de la

máquina, la modificación de archivos y análisis de tráfico de la red, incluso cuando esté encriptado con SSL / TLS.

Gracias a su diseño modular, Cuckoo es personalizable y se pueden analizar diferentes tipos de archivos con él. Entre los tipos de archivos que se pueden examinar con esta herramienta están los archivos ejecutables de Windows, documentos PDF, archivos DLL, documentos de Microsoft office, scripts de PHP, archivos comprimidos en ZIP, archivos java JAR, URL, archivos HTML, entre otros.

Una vez los archivos son ejecutados y analizados de manera automatizada por este framework se puede obtener como resultado los rastros de llamadas a la API realizadas por todos los procesos iniciados por el malware, los archivos que se crean, eliminan y descargan durante la ejecución del malware, realiza capturas de pantalla durante la ejecución del archivo sospechoso, volcado de memoria completa de las maquinas utilizadas y del malware, traza de tráfico de red en formato .PCAP para su posterior análisis.

Malwr.com es una página web gratuita que fue abierta al público a finales de 2012 la cual cuenta con la tecnología de Cuckoo Sandbox. Por medio de esta web las personas pueden enviar archivos para su análisis y obtener resultados.

Cuckoo puede ser descargado totalmente gratis desde https://cuckoosandbox.org/download y la información completa y relevante de este sandbox como los requerimientos, las preguntas frecuentes, su instalación, su forma de uso y la manera de personalizar este framework en https://cuckoo.sh/docs/.

Los miembros del equipo de desarrollo de Cuckoo Sandbox ofrecen servicios empresariales para así respaldarlas y asegurarse de que aprovechen al máximo las funciones de este sandbox. Toda la información acerca de este

beneficio puede ser encontrada en https://cuckoo.sh/blog/pages/commercial-services.html

5. CONCLUSIÓN

Los ataques cibernéticos según los estudios realizados por diferentes compañías van en constante aumento tanto a personas naturales como a las organizaciones con el fin de alterar su funcionamiento o robar información confidencial, siendo el activo más importante en la actualidad.

Estos ataques son cada vez más fáciles, por decirlo de alguna manera, de propagarse gracias a la expansión del internet y la necesidad que tienen las personas y organizaciones de estar conectado en este mundo que cada vez es más globalizado.

Los diferentes avances tecnológicos que se presentan día a día hacen que los victimarios realicen ataques más sofisticados. La criptografía asimétrica, también conocida como de dos claves, es uno de los avances que se han dado en el mundo y es empleada en todos los campos de la sociedad como las comunicaciones, dispositivos de seguridad, transferencia de datos, entre otras utilidades o aplicaciones que necesiten autenticar e identificar de forma segura y la confidencialidad de información sensible.

Los diferentes métodos criptográficos se han empleado desde hace tiempo para proteger e intercambiar información crítica. Esta tecnología se está usando en todos lados para cifrar los datos que se transfieran entre personas, aplicaciones y sistemas. Los atacantes vieron en esta tecnología una oportunidad de perfeccionar sus ataques causando mayor daño y dificultar el rastreo o su ubicación a los investigadores.

Los ciberdelincuentes manipulan estos avances de la criptografía de clave pública y la emplean para dificultar la detección y el análisis del software dañino empleado y también para crear nuevas formas de ataque, como el Ransomware, que, a pesar de haber sido usado desde hace tiempo, en estos últimos años se ha vuelto popular este tipo de ataque, en gran parte debido a la falta de actualización de la infraestructura y la falta de formación de las personas.

Estos nuevos métodos de protección y nuevas formas de ataques usadas por los atacantes llevaron a que surgiera la criptovirología, la cual consiste en el análisis de malware que emplea encriptación simétrica, de una clave, o asimétrica, dos claves (llave pública y llave privada) en sus formas de ataque o en la protección de sus herramientas o métodos empleados para infectar.

Los pioneros en la criptovirologia e inclusive los que le asignaron este nombre fueron los doctores Adam Young y Moti Yung que inclusive fueron más allá de solo el análisis de las formas de ataques e investigaron los ataques a la generación de las claves RSA la cual denominaron ataque cleptográfico, donde se busca obtener los datos necesarios para tratar de conseguir la clave privada y sacarla a través de un canal subliminal y proteger el canal solo para uso del atacante.

Los primeros ataques donde se explotó la criptografía fue en el denominado como polimorfismo, en el cual partes del código del archivo dañino cambia con cada ejecución y el acceso al código es protegido por una clave. Esto no causó mayores inconvenientes para el análisis y posterior detección de los antivirus ya que usa encriptación simétrica, es decir, que utiliza la misma clave para encriptar y desencriptar y por lo general se encontraba en el mismo archivo, por lo cual las compañías de seguridad pudieron agregar una firma y crear mecanismos para desinfectar los archivos que hayan sido afectados.

Los antivirus no son ajenos a los avances que se dan de forma rápida en las herramientas y formas utilizadas por las atacantes y buscan constantemente la forma de proteger a sus usuarios de la forma más rápida posible e inclusive adelantarse a cualquier ataque nuevo que surja. Debido al veloz surgimiento de nuevo malware el método de firmas no era suficiente por lo que crearon la heurística, con las cuál analizan el comportamiento y los cambios de los ejecutables que se instalen o ejecuten en la PC.

La cantidad de infecciones por malware van en aumento constantemente día a día se hace necesario que los usuarios que utilicen PC para sus hogares o para su trabajo tengan por lo menos un conocimiento mínimo de cómo proteger su información y tengan alguna formación básica de la Seguridad Informática para de este modo dificultarle la tarea a los atacantes que buscan propagar el malware.

En la actualidad, no basta con solamente detectar y eliminar los diferentes tipos de malware que pueda llegar afectar un PC, es igual de valioso o inclusive de mayor importancia recopilar toda la información posible de cómo actúan o trabajan para mitigar de forma correcta y segura el posible ataque y en un futuro estar mejor preparado antes una posible infección, de igual forma el análisis también nos puede dar una ayuda a encontrar el objetivo del potencial ataque y las motivaciones del mismo.

No hay una herramienta mejor que otra solo hay herramientas más especializadas que otras las cuales ayudan a realizar el análisis de forma más rápida y sencilla. En la actualidad hay una gran cantidad de herramientas que pueden ser empleadas para la investigación del malware, todo queda a gusto del investigador al momento de escoger la herramienta informática con la cual se sienta más cómodo, le sea más fácil de emplear y se adecue de la mejor forma para el trabajo a realizar y obtener los mejores resultados.

Las herramientas empleadas para los análisis ayudan a la automatización y a optimizar los tiempos de análisis al momento de recopilar la mayor información posible del malware, con lo cual se puede conocer algunas funcionalidades comunes de los códigos maliciosos y sus variantes. Entre más conocimiento se tenga sobre alguna amenaza que coloque en riesgo cualquier activo valioso que tenga una persona o una organización en su máquina, es posible aumentar la seguridad y la precaución.

BIBLIOGRAFÍA ESPECIFICA

[1] Hard2bit Dr (10/09/2013).
Análisis de Malware: Enfoque y caso práctico [En línea] hard2bit.com. Disponible en: https://hard2bit.com/blog/analisis-de-malware-enfoque-y-caso-practico/. [Consultado: 21/02/2018]

[2] RDGMax (Fecha desconocida).
RDG Packer Detector [En línea] rdgsoft.net. Disponible en: http://rdgsoft.net/. [Consultado: 06/03/2018]

[3] Mark Russinovich (Feb 13 de 2018).
Autoruns [En línea] docs.microsoft.com. Disponible en: https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns [Consultado: Mar 22 de 2018]

[4] Michael Sikorski and Andrew Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, San Francisco, 2012

[5] (Sep 09 de 2016).
¿Qué es ESET SysInspector? [En línea] https://support.eset.com/kb762/?locale=en_US&viewlocale=es_ES [Consultado: abril 24 de 2018]

[6] What is cryptovirology? [En línea] http://www.cryptovirology.com/ [Consultado: enero 31 de 2019]

[7] What is kleptography? [En línea] http://www.cryptovirology.com/ [Consultado: enero 31 de 2019]

BIBLIOGRAFÍA GENERAL

- Carlos Zapata Pareja, Ivan Cubides Corrales, Maria Murcia Guzman (2015). Proyecto: Técnicas De Detección Y Análisis De Malware En Entornos Corporativos Con Sistemas Operativos Windows. [En línea] Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/4208/1/Tecnicas_Deteccion_Analisis_Zapata_2015.pdf. [Consultado: Feb 21 de 2018]
- Practical Malware Analysis: A Hands-On Guide to Dissecting Malicious Software (2012).
  Michael Sikorski - Andrew Honig
  ISBN-10: 1-59327-290-1
  ISBN-13: 978-1-59327-290-6
- Malicious Cryptography: Exposing Cryptovirology (2004).
  Adam Young and Moti Yung

ISBN: 0-7645-4975-8
- Marcelo Rivero (Oct 1 de 2016).
¿Qué son los Malwares? [En línea] Disponible en: https://www.infospyware.com/articulos/que-son-los-malwares/. [Consultado: Feb 21 de 2018]
- Malware & Antimalware [En línea] Disponible en: https://www.avast.com/es-es/c-malware. [Consultado: Feb 21 de 2018]
- Cómo hacer un análisis de malware: parte 1 [En línea] Disponible en: http://elixircorp.com/blog/como-hacer-un-analisis-de-malware-parte-1/. [Consultado: Feb 21 de 2018]
- WinVi [En línea] Disponible en: http://www.winvi.de/es/. [Consultado: Feb 26 de 2018]
- BinText [En línea] Disponible en: https://www.mcafee.com/es/downloads/free-tools/bintext.aspx. [Consultado: Mar 7 de 2018]
- Mark Russinovich (Julio 4 de 2016).
Strings [En línea] Disponible en: https://docs.microsoft.com/en-us/sysinternals/downloads/strings. [Consultado: Mar 7 de 2018]
- Oleh Yuschuk.
OllyDbg [En línea] Disponible en: http://www.ollydbg.de/. [Consultado: Mar 08 de 2018]
- IDA: About [En línea] Disponible en: https://www.hex-rays.com/products/ida/. [Consultado: Mar 08 de 2018]
- Hard2bit Dr (Oct 09 de 2013).
Análisis de Malware: Enfoque y caso práctico [En línea] Disponible en: https://hard2bit.com/blog/analisis-de-malware-enfoque-y-caso-practico/. [Consultado: Feb 21 de 2018]
- Dependency Walker [En línea] Disponible en: http://www.dependencywalker.com/. [Consultado: Mar 08 de 2018]
- Explorer Suite (CFF Explorer) [En línea] Disponible en: http://www.ntcore.com/exsuite.php. [Consultado: Mar 12 de 2018]
- FileAlyzer [En línea] Disponible en: https://www.safer-networking.org/products/filealyzer/. [Consultado: Mar 13 de 2018]
- Mark Russinovich (mayo 16 de 2017).
Process Explorer [En línea] Disponible en: https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer [Consultado: Mar 22 de 2018]
- Mark Russinovich (Feb 13 de 2018).
Process Monitor [En línea] Disponible en: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon [Consultado: Mar 22 de 2018]
- Mark Russinovich (Feb 13 de 2018).
Autoruns [En línea] Disponible en: https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns [Consultado: Mar 22 de 2018]
- Mark Russinovich (Julio 25 de 2012).
Autoruns [En línea] Disponible en: https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview [Consultado: Mar 26 de 2018]

- Wireshark [En línea] Disponible en: https://www.wireshark.org/#download [Consultado: Mar 27 de 2018]
- ¿Qué es virtualización? [En línea] Disponible en: https://azure.microsoft.com/es-es/overview/what-is-virtualization/ [Consultado: abril 10 de 2018]
- VirtualBox [En línea] Disponible en: https://www.virtualbox.org/ [Consultado: abril 16 de 2018]
- Chapter 1. First steps VirtualBox [En línea] Disponible en: https://www.virtualbox.org/manual/ch01.html [Consultado: abril 16 de 2018]
- Workstation Pro [En línea] Disponible en: https://www.vmware.com/latam/products/workstation-pro.html [Consultado: abril 16 de 2018]
- systeminfo [En línea] Disponible en: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo [Consultado: abril 20 de 2018]
- ssdeep - Fuzzy hashing program [En línea] Disponible en: https://ssdeep-project.github.io/ssdeep/ [Consultado: abril 24 de 2018]
- ¿Qué es ESET SysInspector? [En línea] Disponible en: https://support.eset.com/kb762/?locale=en_US&viewlocale=es_ES [Consultado: abril 24 de 2018]
- SysAnalyzer Overview [En línea] Disponible en: http://sandsprite.com/iDef/SysAnalyzer/index.html [Consultado: abril 24 de 2018]
- German Sánchez. 4n4lDetector [En línea] Disponible en: http://www.enelpc.com/p/4n4ldetector.html [Consultado: mayo 10 de 2018]
- What is Cuckoo [En línea] Disponible en: https://cuckoosandbox.org/ [Consultado: mayo 21 de 2018]
- Cuckoo Sandbox Book [En línea] Disponible en: https://cuckoo.sh/docs/index.html [Consultado: mayo 21 de 2018]
- What is Cuckoo? [En línea] Disponible en: https://cuckoo.sh/docs/introduction/what.html [Consultado: mayo 21 de 2018]
- Cuidado con los memes de Twitter, pueden tener virus [En línea] Disponible en: https://www.unocero.com/redes-sociales/virus-memes-twitter/ [Consultado: enero 31 de 2019]
- Virus polimórfico [En línea] Disponible en: https://www.ecured.cu/Virus_polim%C3%B3rfico [Consultado: febrero 13 de 2019]
- Virus polimórficos: Proyecto Malware [En línea] Disponible en: https://proyecto-malware.webnode.es/investigacion-del-fenomeno/tipos-de-virus-/virus-polimorficos/ [Consultado: febrero 13 de 2019]
- Qué es el malware polimórfico y cómo evoluciona para infectar tu sistema [En línea] Disponible en: https://omicrono.elespanol.com/2016/03/malware-polimorfico/ [Consultado: febrero 13 de 2019]
- Cryptovirology FAQ [En línea] Disponible en: http://www.cryptovirology.com/ [Consultado: febrero 13 de 2019]

- Criptovirología: del polimorfismo a la kleptografía [En línea] Disponible en: https://www.s21sec.com/es/blog/2009/10/criptovirologia-del-polimorfismo-a-la-kleptografia/ [Consultado: febrero 13 de 2019]
- Antes de ransomware se volvió viral: Criptovirología, Kleptography [En línea] Disponible en: https://sensorstechforum.com/es/before-ransomware-went-viral-cryptovirology-kleptography/ [Consultado: febrero 13 de 2019]
- Nuevas formas de hacer dinero ilegal: Ransomware [En línea] Disponible en: https://www.segu-info.com.ar/articulos/29-formas-hacer-dinero-ilegal-ransomware.htm [Consultado: Febrero 13 de 2019]
- Heurística antivirus y la detección proactiva de amenazas [En línea] Disponible en: https://www.welivesecurity.com/la-es/2013/03/18/heuristica-antivirus-deteccion-proactiva-amenazas/ [Consultado: mayo 9 de 2019]
- Heurística Antivirus – Detección Proactiva de Malware [En línea] Disponible en: http://www.eset-la.com/pdf/prensa/informe/heuristica_antivirus_deteccion_proactiva_malware.pdf [Consultado: mayo 9 de 2019]
- Eliminadores de malware frente al software de antivirus: ¿cuál es la diferencia? [En línea] Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/malware-remover-vs-antivirus-software [Consultado: mayo 9 de 2019]
- Falsos Positivos: ¿y eso qué es? [En línea] Disponible en: https://www.pandasecurity.com/spain/mediacenter/malware/falsos-positivos-y-eso-que-es/ [Consultado: mayo 9 de 2019]
- Falsos Positivos: ¿por qué son tan importantes como la detección? [En línea] Disponible en: https://www.somoseset.com/2018/04/11/falsos-positivos-importantes-deteccion/ [Consultado: mayo 9 de 2019]
- AV-Test nos muestra los mejores antivirus para Windows 10 Fall Creators Update [En línea] Disponible en: https://www.redeszone.net/2018/02/01/av-test-mejores-antivirus-windows-10-fall-creators-update/ [Consultado: mayo 9 de 2019]
- AV-Test nos muestra los mejores antivirus para Windows 10 Fall Creators Update [En línea] Disponible en: http://www.mejor-antivirus.es/noticias/windows-defender-esta-detectando-archivo-legitimos-como-troyanos.html [Consultado: mayo 9 de 2019]
- One_Half [En línea] Disponible en: https://www.f-secure.com/v-descs/one_half.shtml [Consultado: mayo 9 de 2019]
- One_Half [En línea] Disponible en: https://www.symantec.com/security-center/writeup/2000-121513-2517-99#summary [Consultado: mayo 9 de 2019]
- Cómo identificar archivos DLL maliciosos con análisis estático [En línea] Disponible en: https://www.welivesecurity.com/la-es/2015/07/03/identificar-archivos-dll-maliciosos-analisis-estatico/ [Consultado: mayo 17 de 2019]

TABLA DE ILUSTRACIONES

Imagen 1: Mensaje mostrado por WannaCrypt (xataka.com) 9
Imagen 2: Ejemplo de un Cryptosistema de caja negra (http://informatica.blogs.uoc.edu)..... 11
Imagen 3: Ejemplo de implementación de SSL (cosmomedia.es) 12
Imagen 4: Crypter Poliformico (enelpc.com) 15
Imagen 5: Métricas del total de malware desde el 2015 (av-test.org) 16
Imagen 6: Funciones adicionales de Kaspersky AV para el Hogar (kaspersky.com)..... 17
Imagen 7: Métodos de detección de los AV (welivesecurity.com)..... 18
Imagen 8: Malware Protection Test March 2019 - Falses Positives (av-comparatives.org) 19
Imagen 9: Análisis de AV-TEST – Febrero 2019 (av-test.org) 20
Imagen 10: Antivirus analizados por AV-TEST – Febrero 2019 (av-test.org)..... 21
Imagen 11:Pantallazo del programa Winvi (winvi.de)..... 25
Imagen 12:Pantallazo de Exeinfo (download.cnet.com)..... 26
Imagen 13: Pantallazo de FileAlyzer (safer-networking.org) 27
Imagen 14: Pantallazo RGD Packer (rdgsoft.net) 28
Imagen 15: Pantallazo BinText (bintext.soft32) 29
Imagen 16: Pantallazo de OllyDbg (ollydbg.de) 31
Imagen 17: Pantallazo de IDA PRO (hex-rays.com) 32
Imagen 18: Pantallazo de Dependency Walker (dependencywalker.com) 33
Imagen 19: Process Explorer en ejecución (download.cnet.com)..... 35
Imagen 20: Process Monitor en ejecución (bleepingcomputer.com)..... 36
Imagen 21: Pantallazo de autoruns (bleepingcomputer.com) 37
Imagen 22: Pantallazo de Wireshark (wireshark.org)..... 39
Imagen 23: Pantallazo de Fakenet (fireeye.com) 40
Imagen 24Pantallazo de Regshot (howtogeek.com) 41

Imagen 25: Virtual en maquina Windows ejecutando Ubuntu (virtualbox.org) 43
Imagen 26: VMWARE virtualizando varios SO (blogs.vmware.com) 44
Imagen 27: Página mostrada por Virustotal despues de un análisis (blog.virustotal.com) 50
Imagen 28: Detalles del análisis mostrados por hybrid-analysis (securelist.com) 52
Imagen 29: Logo del Sandbox Cuckoo 53