



universidad  
de león



# **Escuela de Ingenierías Industrial, Informática y Aeroespacial**

## **GRADO EN INGENIERÍA INFORMÁTICA**

Trabajo de Fin de Grado

**ANÁLISIS DE RANSOMWARE GROUPS EN REDES TOR**

**ANALYSIS OF RANSOMWARE GROUPS ON TOR  
NETWORKS**

Autor: Sergio del Ser Muñoz  
Tutor: Ángel Manuel Guerrero Higuera  
Cotutor: Juan Delfín Peláez Álvarez

**(Septiembre, 2022)**

**UNIVERSIDAD DE LEÓN**  
**Escuela de Ingenierías Industrial, Informática y**  
**Aeroespacial**

**GRADO EN INGENIERÍA INFORMÁTICA**  
**Trabajo de Fin de Grado**

**ALUMNO:** Sergio del Ser Muñoz

**TUTOR:** Ángel Manuel Guerrero Higuera

**TÍTULO:** Análisis de Ransomware Groups en redes TOR

**TITLE:** Analysis of Ransomware Groups on TOR networks

**CONVOCATORIA:** Septiembre, 2022

**RESUMEN:** Con la evolución de la tecnología y la proliferación de Internet, los ataques cibernéticos han aumentado de manera exponencial. En los últimos años, los ataques del tipo ransomware han estado muy presentes y obtenido un gran alcance debido a la actividad y repercusión, en algunos casos produciendo un enorme impacto económico y social. Los grupos de ciberdelinquentes han desarrollado nuevos tipos de malware con funciones y técnicas cada vez más eficaces y sofisticadas, siendo capaz de pasar por desapercibidas para algunos motores de búsqueda de antivirus. Estos malware utilizan técnicas de cifrado para bloquear el correcto funcionamiento de los dispositivos, y, además, usan técnicas de doble extorsión para aumentar el miedo y que las víctimas acepten a pagar un rescate.

En este informe se realiza un análisis de dos familias de Ransomware as a Service, siendo estas REvil y Avaddon, dos malware actuales de gran importancia.

El malware REvil, el cual ha sido uno de los ransomware más relevantes debido a su gran actividad, se cree que está asociado a los grupos "FIN7" y "GOLD SOUTHFIELD", ya que las métodos y técnicas que utilizan a la hora de infectar a las víctimas son prácticamente idénticas.

Avaddon se trata de un Ransomware as a Service que ha tenido su esplendor en 2021, cuando el malware sufrió una modificación para eliminar la capacidad de retorno, creando un ejemplar mucho más robusto y peligroso.

**ABSTRACT:**

**Palabras clave:** Lorem, ipsum, dolor, sit, amet.

**Firma del alumno:**

**VºBº Tutor/es:**

## Índice de contenidos

## Índice de figuras

## Índice de tablas

## Glosario de términos

### INCIBE

IAB: actores de amenazar que violan una red, mediante diferentes técnicas (phishing, exploits o fuerza bruta) y posteriormente venden ese acceso a otros ciberdelincuentes.

## Introducción

Los ataques cibernéticos han tenido una gran importancia en las últimas décadas, siendo efectuados por diferentes tipos de malware con el objetivo de tener un beneficio, ya sea económico o información de gran importancia, produciendo considerables problemas y pérdidas tanto a empresas como a usuarios estándar. En los últimos años, los malware denominados “Ransomware as a Service” han sido los protagonistas, llevando a cabo ataques con repercusión a nivel mundial.

Este Trabajo de Fin de Grado incluye las conclusiones del estudio realizado sobre diferentes muestras de dos tipos de Ransomware as a Service. Los ejemplares a analizar son “REvil”, cuyo desarrollo se atribuye a los grupos “FIN7” y “GOLD SOUTHFIELD”, y “Avaddon”.

El objetivo principal del análisis es recopilar información de interés para poder determinar funciones y características particulares de los ejemplares escogidos, permitiendo realizar un informe detallado de cada familia ransomware.

## Planteamiento del problema

En los últimos años, los ataques de tipo ransomware han incrementado su importancia de manera relevante respecto a la última década, debido al alto uso de dispositivos electrónicos y a la proliferación del teletrabajo, siendo esto un factor desencadenante.

Por otro lado, las variantes de cada grupo malware se encuentran en constante evolución, incorporando cada cierto periodo de tiempo pequeñas modificaciones para no ser detectados por los sistemas de antivirus y ejecutar de manera más efectiva la infección a las víctimas, completando el proceso en el menor tiempo posible.

## Objetivos

El objetivo principal de este proyecto consiste en realizar un estudio completo sobre los ejemplares Ransomware as a Service escogidos, siendo “REvil” y “Avaddon” las familias seleccionadas para llevar a cabo el análisis.

Los objetivos que se cumplirán a lo largo de este proyecto son:

- Objetivo 1. Estudio del contexto general del problema. Se llevará a cabo una investigación del contexto general del Ransomware as a Service a modo de introducción para presentar el tema a estudiar. Para cumplir el objetivo establecido es necesario:
  - Analizar cuáles son los principales grupos ransomware, sus sitios web en los que publican información relativa al malware y su forma de actuar.
  - Analizar los Ransomware Leaks y la forma de gestionar el sistema de afiliados.
  - Analizar los algoritmos de cifrado que utilizan los malware y las técnicas de extorsión usadas para exigir el pago del rescate.
  - Analizar cuáles son el tipo de empresas víctimas de este tipo de ataques.

- Objetivo 2. Búsqueda en diferentes fuentes públicas muestras ransomware y posterior selección para llevar a cabo los análisis establecidos.
- Objetivo 3. Realizar un estudio general sobre las familias ransomware escogidas, buscando información relevante para comprender el funcionamiento y comportamiento de los mismos.
- Objetivo 4. Realizar un análisis estático, observando y recopilando información de importancia del binario sin detonar el conjunto de muestras seleccionadas.
- Objetivo 5. Realizar un análisis dinámico, observando el comportamiento y funcionamiento del conjunto de muestras.
- Objetivo 6. Realizar un informe con los resultados recopilados de las investigaciones y análisis realizados.
- Objetivo 7. Evaluación y comparación de los resultados obtenidos de los diferentes análisis realizados al conjunto de muestras seleccionadas con el objetivo de encontrar detalles sobre las modificaciones sufridas a lo largo del tiempo.
- Objetivo 8. Estudio de las líneas de investigación futuras.

## Metodología

Con el propósito de llevar un seguimiento en el desarrollo del estudio, se ha utilizado Scrum, un marco de trabajo para la gestión de proyectos, en la cual su principal función es satisfacer las necesidades que desean los clientes.

Scrum sigue el ciclo de vida iterativo e incremental, en la cual se van liberando partes del producto (prototipos) periódicamente mediante iteraciones o ciclos de desarrollo, consiguiendo en cada iteración una versión más completa del proyecto incluyendo nuevas observaciones o funcionalidades.

En el marco de trabajo de Scrum se pueden observar varios tipos de roles dependiendo de sus responsabilidades y funciones:

- Product Owner: Usuario considerado el dueño o representante del producto. Su función es definir los objetivos necesarios para llevar a cabo el producto final deseado, mostrando los intereses del cliente estableciendo las prioridades o necesidades que deben ser cumplidas con antelación.
- Scrum Master: Usuario cuya función es actuar como nexo entre el Product Owner y el equipo Scrum, resolviendo los problemas que puedan surgir mediante el desarrollo del producto
- Scrum Team: Equipo de desarrollo que elabora el producto deseado por el cliente.

Teniendo en cuenta la forma en que se organizan los proyectos mediante Scrum, es necesario establecer los eventos de entrega y evaluación, en los que destacan:



## Estructura del trabajo

En este apartado se definen el contenido de cada una de las secciones que forman el proyecto. Este documento está dividido en seis capítulos, los cuales son:

- Introducción. En esta sección se incluye la contextualización del proyecto, para ello se detalla planteamiento del problema que se ha expuesto, así como los objetivos establecidos y la metodología usada para llevar a cabo el desarrollo del trabajo.
- Capítulo 1. Estudio del problema. En este capítulo se detalla el contexto del problema y se lleva a cabo un estudio de los grupos Ransomware as a Service. Se introduce al lector en los conocimientos básicos del problema, conociendo su forma de actuar y las técnicas que utilizan para llevar a cabo los ataques.
- Capítulo 2. Gestión del proyecto. En este capítulo se incluye la definición y planificación de las tareas establecidas y el presupuesto necesario para llevar a cabo el desarrollo del proyecto, así como la identificación y análisis de los riesgos asociados al mismo.
- Capítulo 3. Solución. En este capítulo se describe la solución al problema y el proceso llevado a cabo para realizar los análisis a las muestras ransomware seleccionadas.
- Capítulo 4. Evaluación. En este capítulo se lleva a cabo una evaluación de los resultados obtenidos en el análisis del conjunto de muestras seleccionado, haciendo una comparación y recopilación de la información más relevante.
- Capítulo 5. Conclusión. En este capítulo se recogen las conclusiones obtenidas en el desarrollo del proyecto, incluyendo los resultados más determinantes. Las líneas futuras de investigación son también incluidas.

## Capítulo 1. Estudio del problema

En este capítulo se presenta el contexto del problema de investigación planteado a la hora de realizar dicho trabajo, además del estado de la cuestión y la definición del problema.

Se elaborará un estudio en el cual se describirá la situación en la cual se encuentra el Ransomware as a Service y la repercusión que tiene en la sociedad actualmente, incluyendo información de interés, como los principales grupos creadores de estos malwares, así como la forma de actuar, herramientas de cifrado utilizadas, prototipos de empresas objetivo de este tipo de ataques y los métodos de extorsión usados para boicotear a sus víctimas.

### 1.1. El contexto del problema

Con la evolución de la tecnología y la proliferación de Internet, los grupos de ciberdelincuentes han desarrollado nuevos tipos de malware con funciones y técnicas cada vez más eficaces y sofisticadas, siendo capaz de pasar por desapercibidas para algunos motores de búsqueda de antivirus. En los últimos años, los ataques ransomware han tomado gran importancia en nuestra sociedad, siendo una grave amenaza a nivel mundial y produciendo grandes daños a empresas y a usuarios. Este tipo de malware es usado para extorsionar a las víctimas, una vez el equipo se encuentra infectado, este bloquea la pantalla o encripta la información de interés, pidiendo un rescate con los detalles para realizar el pago y de esta forma retomar el control del dispositivo. [1\*]

Aprovechando la época de pandemia en la que la mayoría de los usuarios trabajaban desde sus casas, los grupos ransomware expandieron su negocio, incrementando las cifras de ataques realizados en 2020 un 485% respecto al año anterior [2]. Del mismo modo, en el año 2021 las cifras de ataques continuaron ascendiendo, llegando al 150% de incremento respecto a 2020 [3]. El conflicto de la guerra de Ucrania también ha afectado al ascenso de los ciberataques, consiguiendo llegar a cifras históricas superando las de años anteriores [4\*].

Entre los meses de febrero de 2021 y marzo de 2022, los ataques de ransomware aumentaron un 80% con respecto al año anterior, aumentando un 117% los ataques de doble extorsión, según el informe “El estado del ransomware de ThreatLabz 2022”, en el cual se inspeccionaron gran variedad de fuentes, además de 200.000 millones de transacciones diarias y 150 millones de amenazas bloqueadas a diario.

El Ransomware as a Service conocido como REvil/Sodinokibi fue detectado por primera vez en Asia en abril de 2019, siendo unos de los ransomware con mayor número de víctimas y con ataques de gran repercusión a compañías como JBS, Quanta Computer... En 2021, REvil lleva a cabo un ataque masivo en el que comprometió a más de 1000 empresas de al menos 17 países, infectando a más de un millón de sistemas utilizando un instalador de actualización del software de gestión IT de la compañía Kaseya [4] [5]. Los ataques realizados por este grupo tienen una amplia

variedad de sectores empresariales afectados, siendo los principales el consumo, finanzas, servicios e ingeniería. Se atribuye el desarrollo de este ransomware a “GOLD SOUTHFIELD” y “FIN7”, aunque ninguna de las técnicas utilizadas por estos dos grupos coincide. Este ejemplar se encuentra incrustado en un archivo ejecutable, cuando este detona, el malware genera un mutex paralizando el dispositivo para cumplir la misión de ser infectado. Posteriormente, escala algunos privilegios del sistema y elimina los archivos de recuperación como copias de seguridad para que no sea posible restablecer el dispositivo. Por último, se cifran todos los archivos del dispositivo utilizando los algoritmos de cifrado simétrico con AES y Salsa20, generando una nueva extensión en los archivos.

Avaddon se vio por primera vez a principios de 2020, obteniendo una versión optima en junio. Al principio, este malware realizaba ataques a pequeñas o medias empresas de Europa y Estados Unidos. Posteriormente, los ataques se centraban en general en el continente americano, siendo muy afectados los países de Brasil, Perú, Chile y Costa Rica, atacando a los sectores industriales, sanitario o las telecomunicaciones. Alguno de los ataques con más repercusión fueron el de la compañía AXA, en el cual se robó alrededor de 3TB de información y se amenaza con nuevos ataques DDoS contra la misma compañía si no se paga el rescate [5\*], o el ataque a la Lotería Nacional de México, en el cual este grupo obtuvo contratos, convenios y datos financieros de esta asociación durante 12 años, pidiendo pagar un rescate en 240 horas a cambio de la información [6\*]. Este ejemplar es conocido por utilizar las macros de Excel 4.0 como vector de infección y los ataques de negación de servicios distribuidos (DDoS), como método de extorsionar a sus víctimas para realizar el pago del rescate. [6] En junio de 2021, este grupo cierra la operación y entrega las claves de cada ataque en un correo electrónico, en la que la empresa Emsisoft publicó un descifrador gratuito en la que se incluían las 2934 claves pertenecientes a las víctimas.

## 1.2. El estado de la cuestión

Durante la época de pandemia, los grupos ransomware han aprovechado esta oportunidad y han incrementado el número de ataques, siendo un problema para la sociedad. Según el informe semestral de la empresa “S12sec” incluyen a España en el TOP 10 de países más afectados por este tipo de malware, ocupando el octavo puesto con 32 ataques de los 757 ataques registrados en el último semestre. [7\*]

### 1.2.1. Contexto del Ransomware as a Service

Según la página oficial de Malwarebytes, definen ransomware “como un tipo de **malware** que impide a los usuarios acceder a su sistema o a sus archivos personales, ya sea bloqueándolos o cifrándolos, y que exige el pago de un rescate para poder acceder a ellos.” [7]

En 1989, fue reconocido el primer ransomware, “AISD (Aids Info Desk)” o “PC CyborgTrojan”, escrito por el Dr. Joseph Popp y distribuido en un **floppy disk** durante

una conferencia sobre el SIDA. El funcionamiento de este software malicioso se trataba de un contador que enumeraba los encendidos del dispositivo, cifrando y ocultando todos los archivos y directorios que se encontraran en la unidad C: cuando este llegaba a 90. Para obtener el acceso al dispositivo, el usuario tendría que pagar 189 dólares a PC Cyborg Corp., en un apartado de Correos en Panamá Popp. [8]

Con la expansión del uso de Internet y la necesidad del teletrabajar que surgió durante la época de pandemia del COVID-19, los grupos de ciberdelincuentes están constantemente creando nuevas variantes de malware.

#### 1.2.2. Que es el RaaS

La forma de distribuir malware conocida como “Ransomware as a Service (RaaS)” se trata de una variación del modelo de negocio “Software as a Service (SaaS)”. Este plan que puede ser adquirido en el sitio oficial del grupo al que pertenece, ofreciendo a sus clientes un conjunto de herramientas y servicios desarrollados por los grupos ransomware, con las cuales se pueden llevar a cabo una campaña de ataque sobre un objetivo. Son útiles para clientes que no tienen los conocimientos necesarios o no disponen del tiempo suficiente para desarrollar su propio programa. Algunos grupos proporcionan un servicio al cliente 24 horas a la semana, además de reseñas, foros en los cuales los usuarios pueden encontrar información útil. [9]

Esta forma de distribuir software permite a los grupos ransomware centrarse especialmente en la tarea de desarrollo, ya que los clientes son los que llevan a cabo la mayor parte de los ataques.

#### 1.2.3. cuáles son los principales grupos

Los principales grupos de RaaS se pueden definir como las bandas ciberdelincuentes a las cuales se las atribuye un mayor número de incidencias, generando un gran impacto en la sociedad y obteniendo cuantiosos beneficios gracias a los delitos cometidos.

Los principales grupos ransomware han estado presentes durante los últimos años, teniendo una gran actividad durante 2020 y continuando de igual manera en 2021. [10\*] Estos grupos son:

- REvil: Este ransomware, también conocido como “Sodinokibi”, comenzó a operar en 2019, siendo responsable de ataques muy importantes como la actualización a manos de la empresa Kaseya o el ataque a la compañía de alimentos JBS, interrumpiendo completamente los servicios de venta de carne.
- Conti: Al igual que REvil, fue detectado por primera vez en 2019, siendo uno de los malware más importantes hasta la fecha. Se trata del grupo que ha afectado a más organizaciones, llevando a cabo ataques contra el sistema de salud de Irlanda y otras 16 instituciones de salud de EE.UU.
- Lockbit 2.0: Se trata de la segunda versión del malware “LockBit”, detectado por primera vez a finales de 2019, produciendo ataques de gran impacto como

el realizado a la empresa Accenture. Esta versión contiene una función para extraer de manera total y rápida los archivos de la víctima, cifrando los archivos más rápidos que cualquier otro malware.

- Pysa: Surgió a finales del año 2019, pero no tuvo importancia hasta 2020 cuando llevó a cabo ataques contra instituciones educativas, gubernamentales, de la salud...
- Avaddon: Es detectado por primera vez en 2020, siendo relevante en 2021 por el gran número de ataques en América Latina, afectando principalmente a países como Brasil, Chile, Colombia, Costa Rica, México y Perú. Se cree que el grupo ha obtenido alrededor de 40.000 millones de dólares gracias al pago de los rescates exigidos.

#### 1.2.4. Cuáles son sus hidden sites en TOR

La “Dark Web” se trata de la parte de Internet que no está indexada por ningún motor de búsqueda, con el objetivo de proporcionar anonimato mediante el cifrado de las comunicaciones y el enrutamiento a través de múltiples servidores. Para limitar el acceso a estos sitios web, los usuarios necesitan un navegador especializado, como puede ser TOR Browser, y una URL específica que solo es posible de obtener a través de divulgación directa.

El navegador TOR Browser se trata de una herramienta que ayuda a mantener el anonimato a los usuarios que navegan por la Dark Web, utilizando la técnica del “enrutamiento cebolla”, la cual usa técnicas de cifrado y enrutamiento del sitio web a través de múltiples servidores con el objetivo de ocultar la dirección IP. [HS1] Si se produce algún error en estas configuraciones, la actividad puede volverse pública, y, por lo tanto, rastrearse, atrayendo la atención y pudiendo ser investigado.

Los grupos ransomware utilizan la Dark Web con el propósito de ocultar las actividades que realizan y la información relativa a su malware, ya que se tratan de actividades ilegales. En estos sitios web, los grupos ofrecen sus servicios y herramientas, distribuyendo el malware mediante campañas para reclutar a usuarios y que formen parte de su sistema de afiliados. Una vez realizado satisfactoriamente un ataque, los atacantes publican un informe y adjunta información de gran valor para extorsionar a las víctimas.

Con el objetivo de ayudar a los afiliados, en estos sitios web los grupos han incluido soporte técnico disponible para los usuarios que tengan algún tipo de problema con la herramienta distribuida, además de ofertas personalizadas, foros, reseñas de los usuarios y documentación para utilizar correctamente el ransomware.

#### 1.2.5. Cómo actúan estos grupos

Normalmente los grupos de RaaS infectan a las víctimas mediante técnicas de phishing, enviando correos electrónicos con una apariencia convincente, incorporando un link o un archivo malicioso que debe ser ejecutado para comenzar con la infección.

Por otro lado, algunos grupos penetran en dispositivos o empresas comprando el acceso a otros grupos que han descubierto la vulnerabilidad.

Una vez detonado el ransomware, comienzan a ejecutarse todos los procesos y tareas relacionados con el ejemplar, guardando una copia original de los archivos que posteriormente serán encriptados mediante distintos algoritmos.

Completado el proceso de encriptado, comienza la extorsión, para ello los grupos incluyen una nota de rescate en la que se informa a la víctima los pasos a seguir para pagar el rescate. Normalmente se indica a la víctima que tiene que acceder a su sitio web situado en la Dark Web y accediendo mediante el navegador web “TOR Browser”.

Los pagos de los rescates se realizan utilizando criptomonedas con el objetivo de que los movimientos sean irrastreables, ocultando la trayectoria de los fondos e información comprometida de los delincuentes.

#### 1.2.6. Qué herramientas de cifrado usan y como son de efectivas

Una vez infectado un dispositivo, el ransomware comienza a utilizar técnicas de bloqueos de acceso o cifrado de datos y archivos para que no puedan ser utilizados, con el objetivo de que la víctima pague un rescate.

El cifrado garantiza la confidencialidad de los datos, permitiendo únicamente obtenerlos o acceder a su contenido original a los usuarios que contienen la clave secreta, lo que hace que sea una técnica de extorsión para las víctimas. Esta técnica también se utiliza para asegurar la comunicación entre el malware y su servidor de comando y control “C&C”, que en el último paso proporcionará la clave necesaria a la víctima para descifrar los datos y recuperar los archivos [C1].

A la hora de cifrar los datos, los grupos buscan los archivos que contiene mayor cantidad de información importante, teniendo la mayor repercusión posible y obligando a pagar el rescate. Los tipos de archivos por los cuales tienen predilección son [C2]:

- Documentos del paquete Microsoft Office.
- Imágenes y videos.
- Datos.
- Compresión y copias de seguridad.

Estos malware utilizan algoritmos criptográficos muy variados, o combinaciones de ellos para aumentar la eficacia de las técnicas de cifrado. Los mecanismos en esta acción pueden ser muy diferentes, dependiendo de la simetría y el tipo algoritmo escogido, entre los que destacan:

- Cifrado simétrico: En este tipo de cifrado, también conocido como “cifrado de clave secreta”, tanto la víctima como el atacante cambian el mismo número fijo de posiciones, denominado como “clave”. Por este motivo es imprescindible

que la clave se mantenga en secreto. Los algoritmos de cifrado simétrico no necesitan gran cantidad de requisitos computacionales para realizar su función, además solo necesitan de una clave para encriptar y desencriptar. [C3]

Existen dos tipos principales de cifrado simétrico:

- Cifrado por bloques: Los datos o archivos se dividen en bloques de tamaño de byte. Posteriormente, se añaden los bloques cifrados en un bloque completo usando la misma clave. Los algoritmos más comunes de este tipo de cifrado son:
  - AES: Se trata de uno de los algoritmos por bloques más utilizado por los ransomware para cifrar archivos y permite utilizar claves de longitud variable. El modo de cifrado por bloques utilizado por los malware suele ser **CBC**, en el que el cifrado del bloque depende del bloque cifrado anterior. Algunos expertos opinan que no es conveniente confiar en la seguridad que proporciona este algoritmo.
  - Blowfish: Este algoritmo permite el uso de una clave de longitud variable entre 32 y 448 bits, siendo uno de los más rápidos en completar su función y sin necesidad de requerir licencia para su uso. [C4]
- Cifrado de flujo: Los datos o archivos se cifran dígito a dígito, es decir, en forma de bit con ayuda de un flujo de claves pseudoaleatorias, utilizando una clave diferente de la secuencia para cada uno de los bits. Los algoritmos más comunes de este tipo de cifrado por flujo son:
  - RC4: Se trata de uno de los algoritmos por flujo más utilizados por los ransomware debido a su velocidad y simplicidad a la hora de cifrar archivos. En caso de utilizar este algoritmo es importante no utilizar la misma clave para cifrar datos distintos, ya que la clave puede averiguarse fácilmente.
  - Salsa20: Se trata de un algoritmo desarrollado por Daniel J. Bernstein en 2005. Este tipo está formado en una función pseudoaleatoria basada en operaciones “agregar-rotar-XOR”. El algoritmo completa su función una vez completados los 20 pasos que definen el proceso. [C5]
- Cifrado asimétrico: Este tipo de cifrado también es conocido como “cifrado de clave pública”, debido a que el algoritmo utiliza dos claves para llevar a cabo el encriptado. La clave pública está destinada a ser publicada ampliamente, mientras que la clave privada solo se encuentra en posesión del propietario, en este caso los grupos ransomware. Los datos o archivos son cifrados utilizando la clave pública, mientras que el descifrado solo puede conseguirse si se conoce la clave privada. Este tipo de cifrado se considera seguro, pero en casos en los cuales los conjuntos de datos sean grandes es inviable debido a la complejidad computacional a la hora de encriptar los archivos. [C3]

Algunos algoritmos de cifrado asimétrico son:

- RSA: Se trata del algoritmo más usado y sencillo de entender e implementar de los algoritmos asimétricos. La dificultad de este algoritmo se produce a la hora de calcular las claves públicas y privadas, ya que se obtiene como producto de dos primos grandes. [C6]
- Diffie-Hellman-Merkle: Se trata de uno de los protocolos de intercambio de claves más antiguos, ya que fue creado en 1976 y actualmente se sigue usando en la actualidad. Este algoritmo permite crear una clave secreta entre dos equipos que nunca han tenido contacto, a través de un canal inseguro, mediante el envío de dos mensajes. Esta clave solo podrá ser conocida por los dos equipos anteriormente citados, siendo imposible de descifrar debido a que el propio algoritmo cifra de la misma forma la comunicación. [C7]
- Criptografía de curva elíptica: Se trata de un algoritmo que utiliza las propiedades de las curvas elípticas para generar un cifrado prácticamente imposible de descifrar. Este algoritmo reduce el tamaño de las claves, de la misma forma minimizando los recursos necesarios para su proceso, proporcionando el mismo nivel de seguridad que un RSA. [C8]

#### 1.2.7. Sistema de afiliados

La gran mayoría de grupos Ransomware as a Service proporcionan sus servicios en sus sitios web oficiales, ubicados en Dark Web, un lugar oculto en Internet al cual solo se puede acceder mediante un navegador web especializado TOR Browser, o similar. Por otro lado, algunos grupos también disponen de sitios web en el Internet convencional, informando a ciertos usuarios de los ataques realizados y dando la posibilidad a las víctimas de realizar el rescate de una manera más cómoda.

Dependiendo de la organización, los requisitos para registrarse en el sistema de afiliados son diferentes, algunas solo permiten el acceso a usuarios con habilidades determinadas, en cambio, otras buscan distribuir el malware de forma rápida.

Cabe destacar que cualquier transacción que se realice para obtener un servicio o una comisión, se realizará en criptomonedas disminuyendo la posibilidad de ser detectados.

Estas comunidades proporcionan a sus usuarios escoger 4 formas de suscripción[A1]:

- Suscripción mensual a cambio de utilizar el ransomware proporcionado.
- Perteneciendo al sistema de afiliados, en el que además de pagar una suscripción mensual deben aportar una comisión del rescate.
- Suscripción de un ransomware con un solo uso.
- Los usuarios no deben pagar ninguna suscripción, pero deben de aportar una comisión de cada ataque realizado con éxito.



Además, los afiliados tendrán disponible una documentación de incorporación que incluye un tutorial de cómo llevar a cabo un ataque.

#### 1.2.8. Publicación de Ransomware Leaks

Una vez llevado a cabo el proceso de infección y posterior cifrado de datos, los grupos ransomware completan este proceso incluyendo técnicas de doble extorsión. Se trata de una extensión de las campañas ransomware, ya que, si la víctima se niega a pagar el rescate, los grupos amenazan a las víctimas con publicar los datos obtenidos en los sitios web en los que publican las filtraciones, denominados Ransomware Leaks.

Cada grupo ransomware dispone de su propio sitio web, normalmente ubicado en la Dark Web, produciéndose excepciones en las que estas bandas disponen adicionalmente sitio web en el Internet convencional.

Según el “Informe de Ciber amenazas 2021/22” llevado a cabo por la empresa Hornet Security Lab, los grupos no han publicado gran cantidad de información sobre las víctimas, siendo un número muy pequeño comparado con los ataques realizados. El grupo Avaddon, ocupa el cuarto lugar en el TOP 5 de grupos ransomware que han publicado filtraciones, con 160 publicaciones. Siguiendo el grupo REvil, cuyo ransom leaks sigue activo y se denomina “Happy Blog”, con 134. [RL2]

#### 1.2.9. Que tipo (tamaño, país, sector) de empresas atacan

Algunos grupos, antes de llevar a cabo un ataque ransomware, obtienen el acceso a la red corporativa mediante una compra de alto valor a través de intermediarios de acceso inicial (IAB).

Una vez examinados los anuncios llevados a cabo por los grupos ransomware para obtener acceso, la empresa KELA, dedicada a la inteligencia de seguridad cibernética, ha establecido una serie de criterios que llevan a cabo a la hora de buscar una víctima: [E1]

- Geografía: Las víctimas preferidas por estos grupos están ubicadas en EE.UU. (47%), Canadá (37%), Australia (37%) o Europa (31%), esperando que, al pertenecer a países más grandes y desarrollados, estas sean más ricas.
- Ingresos: El ingreso mínimo deseado es de 100 millones de dólares, pudiendo variar dependiendo de la ubicación de la víctima.
- Bloqueo de sectores: Ciertos grupos evitan sectores como la salud, la educación o el sector gubernamental.
- Bloqueo de países: Gran parte de los grupos ransomware evitan atacar a empresas ubicadas en el CEI. Entre los países se encuentran Rusia, Ucrania, Moldavia, Bielorrusia...

Utilizando como referencia los informes de “El estado del Ransomware 2020” [E2] y “El estado del Ransomware 2021” [E3] llevados a cabo por la empresa británica Sophos.

Todas las encuestas fueron realizadas de manera independiente y desvinculada de cualquier proveedor.

En 2020, participaron unos 5000 responsables de TI pertenecientes a compañías de 26 países diferentes. Dentro de cada país, la mitad de los encuestados pertenecían a organizaciones de entre 100 y 1000 empleados, mientras que la otra mitad pertenecían a organizaciones de un tamaño mayor, siendo de 1001 a 5000 empleados.

#### 1.2.10. Triple extorsión.

Las técnicas de extorsión que son utilizadas por estas bandas criminales han ido evolucionando a lo largo del tiempo, mejorando las formas de actuación y los métodos para obtener la mayor cantidad de recursos posible. Al principio, únicamente cifraban los archivos y pedían un pago a cambio de la clave de descifrado. A posteriori de la gran popularización de este modelo de negocio, dependiendo de las filtraciones o las interrupciones que se lleven a cabo se puede hablar de diferentes modelos de extorsión:

- Extorsión única: Se trata de la técnica más antigua de extorsión, en el que las víctimas tienen que pagar una recompensa a cambio de descifrar los archivos.
- Doble extorsión: Como las empresas aumentaron su seguridad y perfeccionaron sus copias de seguridad, podían establecer cualquier sistema y tenerlo operativo en cuestión de tiempo, por lo que los grupos criminales empezaron a amenazar con difundir o divulgar cualquier información obtenida.
- Triple extorsión: Si las empresas no tienen ninguna preocupación sobre la filtración de sus datos, los grupos ransomware utilizan negación de servicios para sobrecargar un servidor o red con tráfico y dejarlo inoperativo.
- Cuádruple extorsión: Una vez comenzado un ataque ransomware, las bandas se ponen en contacto con los usuarios más influyentes en la empresa o principales clientes, creando una gran situación de estrés y presión.
- Extorsión quintuple: Intimidan y presionan a las empresas con vender información confidencial a competidores o usuarios interesados en la víctima.

#### 1.3. La definición del problema

En los últimos años, las tecnologías e Internet han sufrido un gran desarrollo técnico, tomando un papel fundamental en la vida cotidiana de las personas. Del mismo modo, las bandas de ciberdelincuentes han utilizado este crecimiento para desarrollar malwares con el objetivo de infectar a víctimas a través de ataques y obtener algún tipo de beneficio.

El objetivo de este proyecto es llevar a cabo un estudio de dos familias ransomware, denominadas “REvil” y “Avaddon”. Se recopilará información de la investigación realizada al contexto actual del Ransomware as a Service, incluyendo datos de importancia como la forma de actuar de estos grupos, técnicas de cifrado utilizadas, métodos de extorsión que usan contra las víctimas, empresas objetivo de estos

ataques, etc. Para completar el estudio, se llevarán a cabo dos tipos de análisis sobre los conjuntos de muestras seleccionados, uno dinámico y otro estático.

En el análisis estático se analizará la muestra sin ejecutarla, recopilando información sobre las cabeceras, strings, lenguajes de programación, procesos y librerías. En el análisis dinámico, se ejecutará la muestra para analizarla, observando su comportamiento y proceso de infección

Posteriormente, se realizará un informe con toda la información recopilada durante el proceso de investigación y los análisis realizados al conjunto de muestras ransomware.

## Capítulo 2. Gestión del proyecto

En este capítulo se presentan los recursos que se han utilizado en la elaboración del proyecto. Elementos de importancia como el alcance, la planificación seguida o los recursos requeridos del proyecto.

### 2.1. Alcance del proyecto

El objetivo final de este proyecto es la elaboración de un informe de dos muestras Ransomware as a Service actuales y de gran importancia, denominadas “REvil” y “Avaddon”.

El estudio comienza con la investigación de los grupos a los cuales se les atribuye la creación de los ejemplares anteriormente citados, técnicas de cifrado que utilizan, sus “hidden sites” y los métodos de extorsión usados. Posteriormente, se escogerán varias muestras de cada ejemplar y se analizarán de manera estática, obteniendo información de interés como fechas de creación, IOCs, Hashes, carteras virtuales... De la misma manera se realizará un análisis dinámico, en el que se observará el comportamiento de la muestra, cifrando los ficheros y archivos del ordenador mientras no se pague el rescate.

Finalmente, se cotejarán los datos obtenidos con el objetivo de analizar en profundidad los malwares seleccionados, buscando información de interés como la evolución de las técnicas usadas, monederos de criptomonedas...

### 2.2. Plan de trabajo

En esta sección se identifican y describen las tareas seguidas para llevar a cabo el desarrollo del proyecto.

#### 2.2.1. Identificación de tareas

Las tareas definidas en el desarrollo del proyecto se detallan a continuación:

- Tarea 1. Estudio del estado del arte. Se lleva a cabo un trabajo de investigación sobre el modelo de negocio Ransomware as a Service, recopilando información de las técnicas, herramientas, formas de actuar, ataques realizados y métodos de extorsión que utilizan estos malwares.
  - Tarea 1.1. Analizar que es el Ransomware as a Service.
  - Tarea 1.2. Analizar cuáles son los principales grupos.
  - Tarea 1.3. Analizar cuáles son sus hidden sites en TOR.
  - Tarea 1.4. Analizar la forma de actuar de estos grupos.
  - Tarea 1.5. Analizar las herramientas de cifrado que utilizan.
  - Tarea 1.6. Analizar los sistemas de afiliados.
  - Tarea 1.7. Analizar las publicaciones de Ransomware Leaks.
  - Tarea 1.8. Analizar qué tipo de empresas atacan.
  - Tarea 1.9. Analizar los métodos de extorsión que utilizan

- Tarea 2. Creación y configuración del entorno de pruebas y herramientas. Se lleva a cabo la instalación y configuración de las herramientas necesarias para realizar los análisis, tanto estático como dinámico, que serán realizados posteriormente.
  - Tarea 2.1. Creación del entorno de pruebas
  - Tarea 2.2. Configuración del entorno de pruebas.
  - Tarea 2.3. Configuración herramientas
- Tarea 3. Búsqueda de muestras Ransomware as a Service. Se lleva a cabo una selección de diferentes muestras de los ejemplares “REvil/Sodinokibi” y “Avaddon” para posteriormente realizar el análisis.
- Tarea 4. Análisis estático de las muestras. Se lleva a cabo el análisis estático del conjunto de muestras sin ejecutar. En este estudio se obtiene información del binario de los archivos, las librerías, strings, lenguaje de programación...
  - Tarea 4.1. Obtener información general de la muestra.
  - Tarea 4.2. Analizar las cabeceras y secciones del binario.
  - Tarea 4.3. Analizar las librerías y strings.
  - Tarea 4.4. Analizar las técnicas anti detección y anti ingeniería inversa.
- Tarea 5. Análisis dinámico de las muestras. Se lleva a cabo el análisis dinámico, en el que se ejecutan las muestras de las familias “REvil” y “Avaddon”, recopilando datos mediante la monitorización de procesos y visualizando el comportamiento de la muestra.
  - Tarea 5.1. Monitorizar CPU, memoria y procesos de ejecución.
  - Tarea 5.2. Analizar la extensión generada.
  - Tarea 5.3. Analizar el contenido de los archivos encriptados.
  - Tarea 5.4. Analizar la nota de rescate.
- Tarea 6. Elaborar el informe técnico sobre el estudio de las muestras. Se lleva a cabo un informe recopilando la información obtenida de los diferentes análisis realizados a las muestras seleccionadas.
  - Tarea 6.1. Detalles generales.
  - Tarea 6.2. Procedimiento de infección.
  - Tarea 6.3. Análisis estático.
  - Tarea 6.4. Análisis dinámico.

#### 2.2.2. Estimación de tareas

La duración del proyecto ha sido seis meses y medio, empleando 2 horas diarias en la realización del mismo, por lo que se han necesitado alrededor de 400 horas de trabajo para completar el estudio. Las

Tareas	Días	Horas	Fecha inicio	Fecha fin
Tarea 1				
Tarea 2				
Tarea 3				
Tarea 4				
Tarea 5				

Tarea 6				
Tarea 7				

### 2.2.3. Planificación de tareas

Con el objetivo de exponer el tiempo de dedicación previsto para realizar las diferentes tareas previstas en la ejecución del proyecto, se ha elaborado un diagrama Gantt correspondiente a los periodos utilizados. El proyecto se ha planificado con seis meses y medio de duración, dedicando diariamente 2 horas de trabajo, comenzando a mediados de marzo y finalizando en agosto.

## 2.3. Gestión de recursos

En esta sección se detallan los recursos empleados en la realización del proyecto, exponiendo tanto los recursos físicos como humanos, además de incluir los costes y características.

### 2.3.1. Especificación de recursos físicos

Los recursos físicos utilizados en el desarrollo del proyecto ha sido un ordenador portátil personal. Sus características principales son:

- Procesador: Intel Core i7-7700HQ con una frecuencia básica de 2.80GHz, 4 procesadores principales y 8 procesadores lógicos.
- Memoria RAM: 16 GB.
- Almacenamiento: 1TB de disco duro sólido y 128 GB SSD.
- Tarjeta gráfica: NVIDIA GeForce GTX 1050Ti 4GB.

Además, se incluirá un espacio de trabajo en el cual se pueda realizar las reuniones o encuentros necesarios para desarrollar el proyecto.

### 2.3.2. Especificación de recursos humanos

Los recursos humanos utilizados en el desarrollo del proyecto son:

Al ser un proyecto de fin de grado, se ha realizado de forma individual, centrando el autor del documento todos los roles asociados a estos recursos humanos.

### 2.3.3. Presupuesto

El presupuesto de un proyecto tiene como objetivo controlar los costes que se producirán

## 2.4. Gestión de riesgos

A la hora de planificar un proyecto de investigación es fundamental tener en cuenta los riesgos que pueden afectar a los objetivos del proyecto. En esta sección se realizará un análisis de riesgos en el cual se identifican, analizan y se valoran los riesgos que pueden surgir durante el desarrollo del proyecto.

Existen numerosas metodologías y guías en las que definen como realizar una correcta gestión de riesgos del proyecto. En este caso, se ha utilizado como referencia el informe “A Guide to the Project Management Body of Knowledge (PMBOK)”, en el cual se presentan los estándares, pautas y normas que se deben de seguir, con el objetivo de disminuir la probabilidad y el impacto de eventos negativos para el proyecto.

#### 2.4.1. Identificación de riesgos

Según la guía PMBOK, los riesgos que se pueden producir en el desarrollo de un proyecto pueden ser de cuatro tipos:

- **Riesgos técnicos:** Los riesgos técnicos engloban los riesgos relacionados con los requisitos del proyecto, es decir, las tecnologías empleadas, la calidad, fiabilidad, complejidad y el rendimiento.
- **Riesgos externos:** Los riesgos externos engloban a los agentes externos al desarrollo del proyecto, es decir, los clientes, subcontratistas, proveedores. Se incluye dentro de este grupo las condiciones de legislación vigente, de mercado y climáticas.
- **Riesgos de la organización:** En esta categoría se incluyen los riesgos relacionados con la financiación, los recursos disponibles y las dependencias en las diferentes partes del proyecto.
- **Riesgos de la dirección de proyectos:** En esta categoría se incluyen los riesgos relacionados con la gestión de las tareas del proyecto, la estimación de la duración de las tareas, control y dependencia de tareas.

Utilizando de modelo de clasificación de los tipos de riesgos descritos en el PMBOK, se han descubiertos los siguientes riesgos relacionados con el proyecto.

ID	Categoría	Descripción
R1	Técnicos	Fallo en las herramientas utilizadas. En el desarrollo de las pruebas se puede producir un fallo o incompatibilidad de las tecnologías implementadas en el proyecto.
R2	Externos	Acceso a las muestras ransomware.
R3	Organización	Fallo o rotura del dispositivo empleado en el proyecto.
R4	Dirección de proyectos	Desfases temporales respecto la planificación.

#### 2.4.2. Análisis de riesgos

Mediante el análisis de los riesgos identificados se permite estimar la gravedad asociada a cada riesgo, así como los costes o los retrasos producidos. A continuación, se plantean los riesgos además de su solución, con el objetivo de obtener un plan de riesgos completo en la ejecución del proyecto.

R1. El riesgo asociado a que se produzca un fallo o una incompatibilidad durante el uso de una tecnología o herramienta en la realización de un proyecto de este tipo es muy común, por lo que se considera un riesgo de bajo nivel. Debido a este problema,

podrían surgir retrasos a la hora de llevar a cabo los análisis. En este caso, se buscaría una herramienta de características similares que permitiera completar la acción necesaria.

R2. La dificultad de obtener una muestra favorable para el estudio debido a que no se encuentre en una fuente publica o que el propio ejemplar dificulte la ejecución, puede convertirse en un riesgo de nivel medio. Como solución, se plantea disponer de diferentes fuentes para obtener las muestras o buscar los hashes con los que se identifican para realizar una exploración más enfocada.

R3. La probabilidad de que se produzca un fallo o una rotura en el dispositivo empleado para la realización del proyecto es relativamente baja debido a que es poco común, en cambio, se considera como un riesgo de alto nivel. La solución a este riesgo sería realizar copias de seguridad en la nube o en un dispositivo de almacenamiento externo.

R4. La posibilidad de que se produzca algún tipo de dificultad o problema a la hora de realizar una tarea puede tener repercusión en las entregas del proyecto, por lo que se considera un riesgo de bajo nivel. En este caso, se tendrían que adaptar los nuevos plazos de entrega del proyecto retrasando las tareas.



## Capítulo 3. Solución.

Una vez finalizada la recopilación de información del estudio del problema y gestión de tareas, recursos y costes, es necesario realizar un diseño que presente la solución que cumpla con todos los requerimientos del proyecto.

Este capítulo pretende informar al lector del desarrollo seguido para realizar el informe del par de muestras malware seleccionados, incluyendo una descripción de la solución y el proceso de desarrollo, constituido por la identificación de muestras, detalles generales, proceso de infección, análisis estático y análisis dinámico.

Antes de comenzar con el informe de las muestras es necesario crear y configurar el entorno y las herramientas necesarias para llevar a cabo los análisis.

### 3.1. Creación y configuración de máquinas virtuales y herramientas

#### 3.1.1. Creación y configuración de las máquinas virtuales

Antes de ejecutar cualquier tipo de análisis sobre una muestra malware, es necesario disponer de un entorno de trabajo seguro y controlado. Se utilizará la ayuda de máquinas virtualizadas en un dispositivo anfitrión que será configurada de una manera determinada dependiendo del tipo de análisis que se quiera realizar en cada momento.

La virtualización se llevará a cabo con el software “VirtualBox”, “una potente herramienta de uso empresarial y doméstico, rico en funciones y de alto rendimiento para clientes empresariales. Además, se trata de la única solución profesional que está disponible de manera gratuita como software de código abierto bajo los términos de la licencia publica general GNU (GLP) versión 2”.

Para crear el entorno de trabajo deseado se llevará a cabo la virtualización **OVA**s, utilizando el software “VirtualBox”, proporcionando una configuración estable, siendo modificada a lo largo del estudio para mantener las condiciones de los equipos seguras.

Como maquina principal se utilizará un sistema operativo “IE11 on Windows7 (x86)”, obtenido de la página oficial de desarrollo de Microsoft, que proporciona el servicio gratuito con un límite de uso de 90 días. Aceptando la configuración estándar que nos proporciona la herramienta VirtualBox.

Una vez creado el servicio virtualizado de manera correcta, es necesario configurar la maquina con las herramientas y servicios para llevar a cabo correctamente los análisis estáticos y dinámicos de los ejemplares ramsonware.

En el análisis estático no se necesita modificar ninguna configuración de la máquina virtual, ya que las pruebas que se realizan a los malware se ejecutan sin detonar la muestra, lo que no provoca un alto riesgo para la infección de nuestro dispositivo. Por el contrario, en el análisis dinámico es necesario e indispensable modificar la

configuración de la máquina, estableciendo una conexión segura y aislada con el dispositivo anfitrión y el resto de sistemas.

Para aislar la máquina virtual para que la ejecución sea totalmente segura es necesario:

- Bloqueamos la salida a Internet (Todos los adaptadores)
  - Configuración/Red/Deshabilitar adaptador de red.
  - Conectado a: No conectado.
- Deshabilitar las carpetas compartidas entre las máquinas virtuales y el host si existen.
- Deshabilitar portapapeles y arrastrar y soltar:
  - Configuración/General/Avanzado/Compartir portapapeles: Inhabilitado.
  - Configuración/General/Avanzado/Arrastrar y soltar: Inhabilitado.
- Prevenir la conexión de dispositivos de memorias extraíbles.
  - Configuración/USB/Deshabilitar USB.
- Mantener actualizado el software de virtualización.
  - Archivo/Comprobar actualizaciones.
- Realizar un snapshot que permita recuperar la máquina.
  - Instantáneas/Tomar Instantánea.
- Comprobar que no se tiene conexión a Internet

### 3.1.2. Herramientas necesarias para realizar los análisis

Las herramientas utilizadas para llevar a cabo el análisis son muy variadas, obteniendo de cada una información de importancia para conocer detalladamente las familias ransomware elegidas para estudiar.

Dividiremos las herramientas dependiendo en que análisis hayan participado:

- Plataformas de análisis:
  - VirusTotal: Se trata de una página web que sirve como herramienta de análisis en la cual “se inspeccionan los elementos seleccionados con más de 70 escáneres antivirus y servicios en listas de bloqueos de dominios, además de una gran variedad de herramientas para extraer señales del contenido y la propia base de datos de la empresa. Es un servicio gratuito para los usuarios finales para uso no comercial.” Permite al usuario insertar la consulta a realizar de varios métodos diferentes, pudiendo elegir entre un archivo, una URL o una búsqueda identificada por un elemento como puede ser una dirección IP, dominio, hashes...
  - ANY RUN: Se trata de una página web que trabaja como servicio de sandbox para el análisis de malware, permitiendo a los usuarios detonar la muestra en diferentes entornos y con diferentes características. La herramienta proporciona una ejecución estándar que dura 60 segundos en la cual se extrae información como el comportamiento que sigue el malware, los datos del análisis...

- MITRE ATT&CK: Se define como “una base de conocimientos accesible a nivel mundial sobre el comportamiento de los ataques cibernéticos y la taxonomía de las acciones a lo largo de su ciclo de vida. Surge en 2013 para solucionar la necesidad de documentar las tácticas, técnicas y procedimientos (TTP) comunes que las amenazas avanzadas utilizan contra las redes empresariales de Windows en un proyecto de investigación.” [H3]
- Herramientas de análisis estático:
  - HxD: es un editor hexadecimal rápido, desarrollado por Maël Hörz, que permite editar el disco sin procesar y modificar la memoria principal, además de observar la representación en formato ASCII del archivo.
  - HashMyFiles: es una herramienta que permite calcular los hashes MD5, SHA1, SHA256, también incorpora información como la fecha de compilación, el tamaño y extensión del archivo...
  - Exeinfo PE: es una herramienta que nos permite analizar cualquier archivo y observar sus propiedades, como son identificar el lenguaje de programación utilizado para desarrollar el ejecutable, las técnicas de empaquetado usadas o el tipo de archivo que se trata.
  - PEView: Se trata de una herramienta de identificación del binario, desarrollada y mantenida por Wayne J. Radburn, que permite trabajar como un visor de archivos PE. Los detalles que proporciona esta aplicación pueden ser un poco pobre, ya que solo muestra la información básica sobre el Header PE.
  - PEBear: Se trata de una herramienta gratuita de inversión de archivos PE, con el objetivo de ofrecer a los analistas malware un software capaz de manejar archivos PE con formato incorrecto. Se trata de una herramienta de identificación del binario como las anteriormente citadas.
  - PEStudio: Se trata de una herramienta con el objetivo de analizar cualquier tipo de archivo ejecutable, identificando y mostrando la información relevante de los mismos de forma ordenada y fácil de entender, para realizar una evaluación rápida del malware.
- Herramientas de análisis dinámico:
  - Process Explorer: Es un administrador de tareas y un monitor de sistema para Windows, creado por SysInternals y posteriormente adquirido por Microsoft. Proporciona la funcionalidad de administrador de tareas incluyendo técnicas para recopilar información sobre los procesos que se ejecutan en el sistema.
  - Autoruns: Se trata de una herramienta que permite analizar programas, servicios o cualquier otro tipo de elemento que se ejecuta al iniciar el sistema.
  - Visor de eventos: Se trata de una herramienta que registra toda la actividad del dispositivo a través de una lista de eventos.

- Administrador de tareas: Se trata de una herramienta que proporciona información sobre los procesos y programas que se están ejecutando en un dispositivo, además de la actividad de red y servicios del sistema.

## 3.2. REVIL

### 3.2.1. Descripción de la solución

La primera vez que apareció el Ransomware as a Service de origen ruso “REvil”, también conocido como “Sodin” o “Sodinokibi” fue en el continente asiático sobre abril del 2019, convirtiéndose uno de los malware más importantes hasta la fecha.

El desarrollo de esa familia se les ha atribuido a dos grupos. Por un lado, “GOLD SOUTHFIELD”, que proporciona infraestructura back-end para los afiliados que han sido reclutados en foros clandestinos para llevar a cabo ataques y cobrar pagos por el rescate. Este grupo limita la cantidad de afiliados que se encuentran suscritos a un programa, dando preferencia a los afiliados que puedan realizar ataques con un mayor valor para la organización. En cambio, los usuarios de habla nativa inglesa tienen vetado incluirse a su programa de afiliados [DS1]. Por otro lado, “FIN7”, se trata de un grupo que se encuentra activo desde 2013 y es también conocido como “Carbanak” o “Navigator”. Este grupo crea empresas falsas con el objetivo de camuflar sus intenciones, para ello ha utilizado la imagen de consultores de seguridad de la información, denominándose “Combi Security”, o más recientemente “Bastion Secure”.

Algunas fuentes vinculan el desarrollo de REvil al mismo grupo que el malware “GrandCrab”, ya que los dos comparten similitudes en el código fuente, modelo de actualización y versionado y los vectores de propagación.

Utilizando la herramienta “Navigator” proporcionada por MITRE ATT&CK, observamos que los grupos a los cuales se les atribuye el desarrollo del Ransomware as a Service “REvil” no comparten ninguna técnica de las que utilizan para llevar a cabo sus ataques.

Esta familia ransomware esquivó infectar dispositivos de Irán, Rusia, Ucrania, Bielorrusia, Estonia, Letonia, Lituania, Armenia, Siria... es decir, países que anteriormente formaban parte de la URSS. [\*DS2] Por otro lado, ha tenido repercusión a nivel global, ya que ha afectado a un gran número de países, destacando principalmente Europa, Asia e India [DS2]. Siendo más específicos, entre los países afectados España se encuentra en el noveno lugar (5,26%). [DS\*]



REvil se caracteriza por su gran capacidad de evasión, utilizando gran número de medidas para evitar ser detectado por motores antivirus o sistemas de detección de intrusiones (IDS), convirtiéndolo en extremadamente peligroso. Además, aprovecha una vulnerabilidad de Oracle WebLogic con la que se obtiene acceso a la máquina del objetivo, consiguiendo escalar algunos de los privilegios del usuario para acceder a los archivos y recursos del sistema. En enero de 2020, comienza a utilizar la técnica de doble extorsión, es decir, publicar los datos obtenidos de los ataques en su sitio web oficial, que posteriormente será también usado para reclutar a los usuarios.

El ransomware se encuentra incrustado en un archivo ejecutable, empaquetando las diferentes cadenas de texto, nombres de librerías y archivos DLL mediante un algoritmo criptográfico RC4, utilizando una clave aleatoria diferente y de longitud variable para los distintos elementos cifrados, siendo capaz de pasar sin ser detectado por los motores de búsqueda de antivirus. Una vez ejecutado el archivo, la información se descifra utilizando el hash de la cadena, dificultando la detección. Posteriormente, la primera acción del código es generar un mutex, impidiendo que entre más de un proceso a la vez en la sección crítica, previniendo de fallo y dificultando la detección.

Una vez ejecutado el malware, comienza con la escalada de privilegios en el sistema, utilizando la vulnerabilidad CVE-2018-8453, que ejecutará un exploit con el que se comprobará si el sistema que está siendo infectado es vulnerable, comparando la fecha de creación del archivo con la del sistema. Si el malware no ha conseguido la escalada de privilegios de forma anterior, se ejecuta la función "RunAs" con la que se fuerza la ejecución de privilegios elevados y evitar el sistema de Control de Cuentas de Usuario "UAC".

Si el malware consigue obtener estos privilegios, se recopilan los datos de la configuración del sistema y sesión, comprobando detalles del sistema como el idioma de la interfaz o del teclado, comprobando si pertenece a alguno de los países excluido de los ataques, ya que si es así se finalizará el proceso. De la misma forma terminará el ataque si el malware no obtiene los privilegios necesarios para llevar a cabo la infección.

Con el objetivo de dificultar la recuperación de los archivos del sistema a manos de la víctima, se bloquean las opciones "Shadow Copy", desactivando el proceso "vssadmin"

y utilizando “bsdedit”, que desactivará las copias de seguridad y borrará todas las instantáneas y copias de seguridad para no poder ser restablecido y subsanar el problema de la infección.

Si se continua con el proceso de ataque, el malware comenzará a cifrar los archivos, tanto las unidades locales como las unidades de red conectadas al mismo dispositivo, con excepción de algunas carpetas y extensiones del sistema operativo que llevan a cabo el funcionamiento mínimo del dispositivo. Para llevar a cabo el cifrado se utilizan distintos algoritmos, generando varias claves tanto simétricas como asimétricas haciendo uso del algoritmo de curva elíptica “Diffie-Hellman” (ECDH).

Los algoritmos de cifrado utilizados son:

- Cifrado simétrico con AES: Es utilizado para el cifrado de la clave privada de un par de claves generadas localmente en el equipo infectado, en la que la clave publica será utilizada para el cifrado de ficheros. De la misma forma es utilizado para cifrar los datos que se intercambian con la consola de comando y control si se produce este tipo de comunicación.
- Cifrado simétrico con Salsa20: Es utilizado para el cifrado de los archivos secuestrados, a partir de la clave publica generada anteriormente y la clave privada generada para cada fichero.

Completado el cifrado del dispositivo, los archivos que se encuentran en la maquina sufrirán una modificación en la que serán renombrados incluyendo una extensión dependiendo de la configuración. Además, generará un archivo que representa la nota de rescate, incluyendo las instrucciones que deberá de llevar a cabo la victima para obtener el descifrador que permite recuperar el control del sistema infectado. [DS4]

### 3.2.2. Proceso de desarrollo

En esta sección se detalla el proceso de desarrollo seguido en el análisis de las familias ransomware escogidas, formado por cinco fases bien diferenciadas.

La primera fase se trata de la identificación de las muestras, seleccionando ejemplares que permitan ser analizados. Posteriormente, se explicarán los detalles generales y el proceso de infección de esta familia, siendo común en todas las muestras, ya que se trata del mismo malware. Las últimas fases se tratan de los análisis, tanto estático como dinámico.

#### 3.2.2.1. Identificación de las muestras

Los ejemplares escogidos para el estudio de la familia ransomware REvil ha sido un conjunto de 9 muestras, adquiridas de la fuente publica “ANY RUN”, siendo clasificados teniendo como referencia la primera fecha de aparición en la página “VirusTotal”, pudiendo ser de ayuda para observar las modificaciones temporales que realizaban los grupos para alterar los comportamientos y no ser detectados.

Se hará una búsqueda en la página “VirusTotal” de cada una de las muestras, obteniendo la información de relevancia que se incluye en la tabla, compuesto por el hash SHA-256, primera fecha de aparición y varios nombres con los que se denominan entre los motores de búsqueda de antivirus.

Nombre de la muestra	SHA-256	Primera vez subido a VirusTotal	Nombre (GData)	Nombre (Microsoft)
REvil_1	a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60	28/04/2019	“Trojan.Brsecmon.1”	“Trojan:Win32/Malgent.B”
REvil_2	ed49b23df7defab3df933c778183b12c019ab253330090f214f4bb5c2f89bcbc	06/08/2019	“DeepScan:Generic.Ransom.AmnesiaE.04123F8A”	“Ransom:Win32/R evil.B”
REvil_3	7227cb2316b9e3b678698609b41ba67958d509fbf37c46cbde714b105b71bd68	27/12/2019	“Win32.Virus.Neshta.D”	“Virus:Win32/Nestha.A”
REvil_4	140f831ddd180861481c9531aa6859c56503e77d29d00439c1e71c5b93e01e1a	17/06/2020	“Gen:Variant.Zusy.306770”	“Ransom:Win32/Sodinokibi!MSR”
REvil_5	14c8e3f1f23d16c2c9a4272cd05d00461d27b372cc5f588b4bbfc6102bbed708	03/08/2020	“Gen:Variant.Razy.525651”	“Ransom:Win32/R evil.A”
REvil_6	52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85	17/03/2021	“Win32.Trojan-Ransom.Revil.A”	“Ransom:Win32/R evil.A”
REvil_7	ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83	09/09/2021	“Gen:Variant.Ransom.Sodinokibi.66”	“Ransom:Win32/R evil.A”
REvil_8	0c10cf1b1640c9c845080f460ee69392bfaac981a4407b607e8e30d2ddf903e8	29/04/2022	“Trojan.GenericKD.49038346”	“Ransom:Win32/R evil.D!MTB”
REvil_9	dd59a759331f7d6c46ed43cba3d55b8325985e215b94027972006c06b1ec1f1c	08/07/2022	“Trojan.BrsecmonE.2”	“Trojan.Generic@Al.92 (RDML:MLNQkgPg3+7IKljbgeBc/A)”

Para realizar el estudio y posteriormente una comparación con el conjunto de ejemplares, se seleccionará como modelo la muestra 3, aunque las tareas seguidas en

los procesos de análisis han sido equivalentes. Esta muestra ha sido elegida como referencia gracias a la cantidad de información y detalles que nos proporcionan las diferentes herramientas en los análisis estáticos y dinámicos, facilitando su estudio.

#### 3.1.2.2. Detalles generales

La muestra escogida como modelo se ha observado por primera vez el 27 de diciembre de 2019, denominada como “svhost.exe”, y detectado en la herramienta “VirusTotal” como maliciosa por 60 de 70 motores de búsqueda antivirus que se encuentran disponibles en su base de datos.

Las muestras han sido desarrolladas como un fichero de imagen ejecutable para máquinas de 32 bits, sin utilizar ninguna técnica de método de empaquetado para dificultar la detección del malware. En la mayoría de casos por el programa “Microsoft Visual C++”, modificando las versiones anteriores para incrementar la funcionalidad y rendimiento en los ataques.

Pese a que se trate de un software relativamente antiguo, se ha comprobado que sigue en continuo desarrollo, debido a que las últimas modificaciones han sido vistas estos últimos meses.

En lo respectivo con las variaciones, se ha observado que la funcionalidad principal de las muestras permanece sin cambios aparentes, alterando en cierta manera métodos como el comportamiento de cifrado, carteras de criptomonedas o los ransomware Leaks a los que deben acudir las víctimas infectadas.

#### 3.1.2.3. Proceso de infección

Este malware tiene varias formas de propagación, consiguiendo extenderse a nivel mundial, siendo Asia la región más afectada [IN1].

Los principales métodos de propagación de este malware son:

- Campañas de spam mediante el envío de correos electrónicos maliciosos.
- Técnicas de “malvertising” o publicidad maliciosa, en la cual los anuncios que aparecen durante la navegación en internet contienen un código malicioso, el cual se puede ejecutar directamente en el equipo o redirigir la navegación hacia servidores para descargar un ejecutable.
- Ataques de fuerza bruta sobre el protocolo RDP (Remote Desktop Protocol).
- Técnicas en las cuales se engañan a la vulnerabilidad CVE-2019-2725 que afecta a sistemas Oracle.

#### 3.1.2.4. Análisis estático

Se denomina “análisis estático” al estudio realizado sobre una muestra sin detonar, es decir, sin ejecutar la función establecida dependiendo del tipo de archivo o componente a analizar, estudiando elementos como el código ensamblador, dominios, dependencias, cabeceras, etc... [AE1]



Las herramientas utilizadas en este proceso permiten extraer información sin necesidad de ejecutar la muestra, ya que la información está disponible para el usuario de manera inmediata y puede servir como base para guiar la investigación.

En este proceso se obtendrá información de gran importancia para comprender el comportamiento y funcionamiento del malware, realizando tareas de identificación del binario, obtención de strings, técnicas de anti detección o anti ingeniería inversa y debuggers.

Antes de comenzar el análisis estático, es de gran utilidad conocer los detalles más generales de la muestra a analizar, para ello emplearemos la herramienta online “VirusTotal”. En el historial de la muestra se puede observar que la fecha de creación de esta muestra es de junio de 1992, por lo que se puede sospechar que los desarrolladores de esta versión modificaron la fecha con el objetivo de no ser detectado por algún motor de búsqueda antivirus.

---

Creation Time	1992-06-19 22:22:17 UTC
First Seen In The Wild	2020-06-11 13:11:25 UTC
First Submission	2019-12-27 12:11:27 UTC
Last Submission	2022-07-29 16:15:20 UTC
Last Analysis	2021-06-02 19:17:04 UTC

La herramienta “HxD” nos permitirá obtener el formato del archivo gracias a un conjunto de valores formados por el valor numérico con el que se identifica el formato de un archivo, denominado “Magic Number”, el texto del archivo y el PE Header. En ciertas ocasiones los grupos intentan ocultar la verdadera extensión del fichero con el objetivo de dificultar la detección del software malicioso e infectar a las víctimas. En el caso de esta muestra los valores que toman estos elementos son:

- Magic Number: MZP (4D 5A 50). Este identificador de formato nos indica con los dos primeros valores (MZ) que se trata de un archivo ejecutable. El tercer valor (P), nos indica que el archivo esta desarrollado mediante el software “Borland Delphi”.
- Texto del archivo: “This program must be run under Win32”.
- PE Header: PE (50 45).

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texto decodificado
00000000	4D	5A	50	00	02	00	00	00	04	00	0F	00	FF	FF	00	00	MZP.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	1A	00	00	00	00	00	.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	01	00	00	.....
00000040	BA	10	00	0E	1F	B4	09	CD	21	B8	01	4C	CD	21	90	90	°.....'í!..Lí!..
00000050	54	68	69	73	20	70	72	6F	67	72	61	6D	20	6D	75	73	This program mus
00000060	74	20	62	65	20	72	75	6E	20	75	6E	64	65	72	20	57	t be run under W
00000070	69	6E	33	32	0D	0A	24	37	00	00	00	00	00	00	00	00	in32..\$7.....
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	50	45	00	00	4C	01	08	00	19	5E	42	2A	00	00	00	00	PE..L....^B*....
00000110	00	00	00	00	E0	00	8E	81	0B	01	02	19	00	74	00	00	....à.Ž.....t..

Revisando la muestra se puede observar cómo ciertas partes del archivo no se encuentran cifradas, visualizando tanto las secciones, DLL o funciones que forman este ejecutable.

000083A0	00	00	43	72	65	61	74	65	43	6F	6D	70	61	74	69	62	..CreateCompatib
000083B0	6C	65	42	69	74	6D	61	70	00	00	00	00	42	69	74	42	leBitmap....BitB
000083C0	6C	74	00	00	75	73	65	72	33	32	2E	64	6C	6C	00	00	lt..user32.dll..
000083D0	00	00	52	65	6C	65	61	73	65	44	43	00	00	00	47	65	..ReleaseDC...Ge
000083E0	74	53	79	73	43	6F	6C	6F	72	00	00	00	47	65	74	49	tSysColor...GetI

000002A0	08	00	00	00	00	60	01	00	00	00	00	00	86	00	00	00	.....`.....†..
000002B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	C0	.....À
000002C0	2E	72	64	61	74	61	00	00	18	00	00	00	00	70	01	00	..rdata.....p..
000002D0	00	02	00	00	00	86	00	00	00	00	00	00	00	00	00	00	.....†.....
000002E0	00	00	00	00	40	00	00	50	2E	72	65	6C	6F	63	00	00	....@...P.reloc..

Posteriormente, analizaremos el ejemplar utilizando la herramienta “HashMyFiles”, proporcionando información relativa a los hashes y algoritmos de codificación utilizados (MD5, SHA-256, SHA-512...), datos como el tamaño, extensión o la ruta en la que se encuentra.

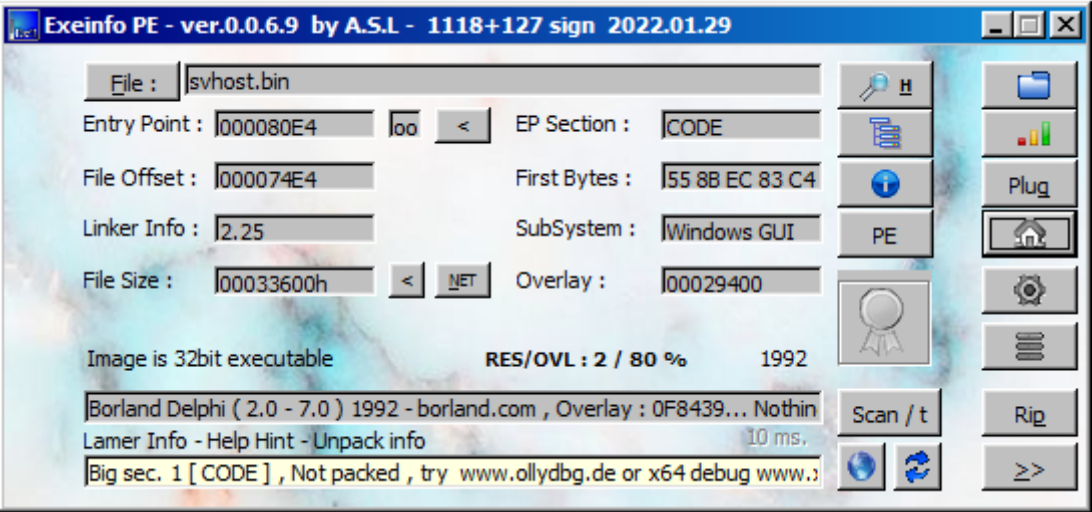
```

=====
Filename       : svhost.bin
MD5            : ea0acb3bfaee6386a9270cc314ebfed9
SHA1           : bdc92076c2851d408af99a4c6a6a42a4a12c5d9d
CRC32          : f7afb811
SHA-256        : 7227cb2316b9e3b678698609b41ba67958d509fbf37c46cbe714b105b71bd68
SHA-512        : f29d4808705e8fb3502b48d97f8499baa379bfc91a0b96bdc1e733b24eb0f5ad8baca41f145614943746fc42a30c3408b6a3e4332c8ddb2c14cf45a406f532
SHA-384        : 20a153a913438d19d5720dfbc74429b2e58aa864ebdbc69bffe7f9e74e66d0fca8c74e027c3553c6e74148036ba6c56
Full Path      : C:\Users\IEUser\Downloads\FINAL\REVIL\FINAL\3\svhost.bin
Modified Time   : 7/29/2022 9:15:00 AM
Created Time    : 7/29/2022 9:15:00 AM
Entry Modified Time: 7/31/2022 11:00:20 AM
File Size       : 210,432
File Version    :
Product Version :
Identical       :
Extension       : bin
File Attributes  : A
=====

```

“Exeinfo PE” nos permite obtener detalles sobre los métodos y programas utilizados para su creación, observando que fue desarrollado mediante el compilador “Borland Delphi (2.0 – 7.0)”, siendo un fichero ejecutable en máquinas de 32 bits. Además, nos

indica que el archivo no se encuentra empaquetado, mostrando la opción de utilizar debuggers como pueden ser “OllyDBG” o “64 Debug” en el caso de querer intentarlo.



La herramienta “PEView” nos permite observar los elementos del binario sobre las secciones de un archivo del tipo PE, ofreciendo información de una manera pobre pero simple.

“PEStudio” es una herramienta que proporciona gran cantidad de información de forma ordenada y clara, permitiendo obtener elementos como hash, IOCs, strings, librerías... En la sección de librerías utilizadas de la muestra analizada podemos observar que se forma por un conjunto de 6 DLL’s, no detectando ninguna como maliciosa.

library (6)	flag (0)	type (1)	functions (42)	description
kernel32.dll	-	implicit	21	Windows NT BASE API Client DLL
user32.dll	-	implicit	2	Multi-User Windows USER API Client DLL
advapi32.dll	-	implicit	3	Advanced Windows 32 Base API
oleaut32.dll	-	implicit	2	oleaut32.dll
gdi32.dll	-	implicit	12	GDI Client DLL
shell32.dll	-	implicit	2	Windows Shell Common DLL

Por otro lado, en las funciones que lleva a cabo el malware a la hora de la infección, obtenemos que 15 de los 85 procesos que se llevan a cabo son maliciosos, formando parte de las DLL’s “kernel32.dll”, “user32.dll” y “advapi32.dll”.

c:\users\ieuser\downloads\revil-20220809t18090

indicators (48) \*

virustotal (60/70)

dos-header (64 bytes)

dos-stub (192 bytes)

rich-header (n/a)

file-header (Jun.1992)

optional-header (GUI)

directories (time-stamp)

sections (file)

libraries (6) \*

**functions (85)**

exports (n/a)

tls-callback (n/a)

.NET (n/a)

resources (unknown)

strings (4489)

debug (n/a)

manifest (n/a)

version (n/a)

overlay (unknown)

functions (85)	flag (15)	ordinal (0)	library (6)
GetCurrentThreadId	x	-	kernel32.dll
WriteFile	x	-	kernel32.dll
RaiseException	x	-	kernel32.dll
GetKeyboardType	x	-	user32.dll
RegSetValueExA	x	-	advapi32.dll
WriteFile	x	-	kernel32.dll
WinExec	x	-	kernel32.dll
SetFileAttributesA	x	-	kernel32.dll
SetCurrentDirectoryA	x	-	kernel32.dll
GetLogicalDriveStringsA	x	-	kernel32.dll
FindNextFileA	x	-	kernel32.dll
FindFirstFileA	x	-	kernel32.dll
DeleteFileA	x	-	kernel32.dll
CopyImage	x	-	user32.dll
ShellExecuteA	x	-	shell32.dll
DeleteCriticalSection		-	kernel32.dll
LeaveCriticalSection		-	kernel32.dll
EnterCriticalSection		-	kernel32.dll
InitializeCriticalSection		-	kernel32.dll

### 3.1.2.5. Análisis dinámico.

Se denomina “análisis dinámico” al estudio realizado sobre una muestra detonándola, es decir, llevando a cabo la función del archivo que se haya ejecutado. De esta forma se puede observar en primera persona cual es el comportamiento y funcionamiento del malware.

Este estudio es necesario realizarlo en un entorno de pruebas aislado y seguro, para no dañar ninguna unidad importante de nuestro dispositivo anfitrión. [AD1]

Aunque la ejecución de la muestra se llevará a cabo en un entorno controlado, el análisis dinámico se puede realizar de dos formas, dependiendo como se detone la muestra:

- Ejecución en un entorno de pruebas controlado.

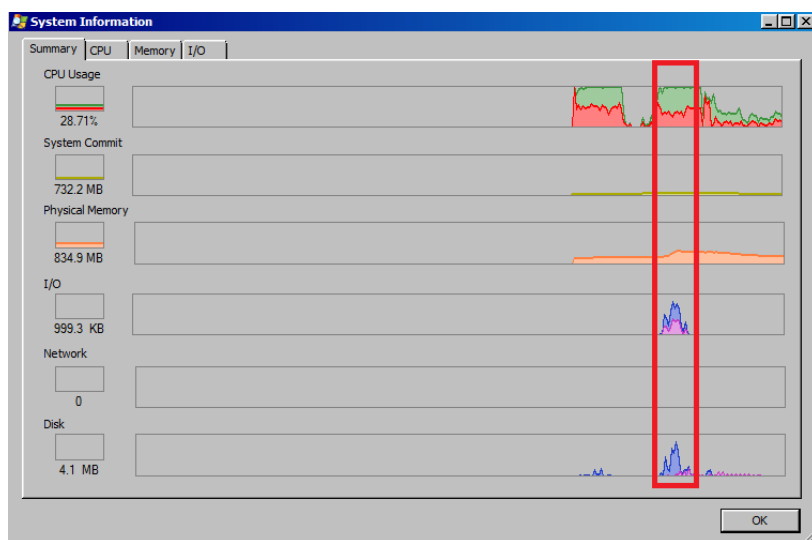
La ejecución en un entorno de pruebas controlado se realizará en la máquina virtual Windows 7, configurada anteriormente para que se encuentre aislada y sea un ambiente correcto para el estudio de las muestras.

Antes de detonar cualquiera de las muestras, es necesario modificar la extensión del archivo de origen por “.exe”, convirtiéndolo en un ejecutable y comenzando la infección de la máquina. Además, se iniciarán las herramientas que utilizaremos en el análisis dinámico para comparar los cambios que se producen a nivel de procesos y tareas cuando la muestra malware se ejecuta.

La herramienta “Process Explorer” se trata de un administrador de tareas y monitor de procesos que nos permite observar la carga que realiza la ejecución de la muestra malware al dispositivo que está infectando. A la hora de ejecutar la muestra, se observa cómo se crea un proceso que consume el 96.44 de los recursos de la CPU, en algunos casos bloqueándola por segundos debido a la sobrecarga.

Process	Private Bytes	Private Bytes (K)	Private Bytes (K)	Private Bytes (K)
svchost.exe	< 0.01	3,492 K	7,496 K	3504
svchost.exe	96.44	5,092 K	6,024 K	3288
sshd.exe		6,092 K	5,760 K	840

Si observamos la gráfica en el tiempo que nos proporciona esta misma herramienta, se puede ver que, en el momento de detonar el malware, en todas las áreas del dispositivo, es decir, CPU, Memoria, Disco e I/O, se exigen gran cantidad de recursos, en ciertos instantes realizando un consumo completo.



Los archivos que se encontraban en el dispositivo infectado han sido encriptados y modificados. Además, se ha generado un archivo que contiene la nota de rescate, especificando las instrucciones que tiene que seguir la víctima para retomar el control del dispositivo, incluyendo información de interés como el navegador y dirección web que debe utilizar, la clave de cifrado o la extensión con la que cifra la muestra.

[illegible]

- Ejecución en la nube.

La herramienta online “Any Run” nos permite ejecutar el malware en una máquina online por tiempo limitado, configurando algunos valores de la forma que mayor nos convenga en cada análisis. En nuestro caso, seleccionaremos la misma máquina con la que se han realizado el resto de pruebas, un sistema operativo Windows 7 y una duración de análisis de 60 segundos, el tiempo que proporciona la página para los análisis estándar.

Una vez completado el tiempo de análisis, la herramienta nos proporciona información relevante como los principales procesos realizados, archivos generados y encriptados, rendimiento de RAM y CPU. Además, genera un documento que puede ser descargado con un resumen de toda la información obtenida durante el estudio de la muestra.

La herramienta produce un esquema de ejecución en el cual se muestran los procesos que se llevan a cabo a la hora de la infección, esquematizando cual es el camino que sigue el malware en su ejecución.



De la misma manera se muestran los recursos de CPU y memoria empleados durante todo el proceso, indicando con el color amarillo los periodos en los que se produce un mayor uso de recursos.



## 3.2. AVADDON

### 3.2.1. Descripción de la solución

El ransomware, Avaddon, apareció por primera vez a finales de 2019, pero no fue hasta junio de 2020 cuando obtuvo su mayor importancia, ya que comenzó a reclutar afiliados en foros y a trabajar como la variante Ransomware as a Service, ofreciendo un servicio rápido, personalizado y altamente configurable. [AA1] Las víctimas que son afectadas por este ransomware, sufren el cifrado de todos sus datos y archivos, existiendo la posibilidad de que se complemente con la técnica de doble extorsión, en la que se publican los datos anteriormente citados en el foro del grupo. [AA2]

Al comienzo, este malware pedía a sus afiliados un 25% de los beneficios obtenidos de cada víctima, disminuyendo esta cifra en los clientes con mayor volumen, alcanzando ser uno de los ransomware más agresivos dirigidos a personas o empresas. Esta familia prohibió incluir a su sistema de afiliados de cualquier país perteneciente a la CEI,

además de ser muy crítico con cualquier usuario con personas de distinto habla que el ruso.

Con el objetivo de infectar a las víctimas, al principio este malware utilizaba campañas de phishing mediante correos electrónicos que contienen una imagen “comprometedora” adjunta con los que intentan estafar al usuario o archivos Excel con macros maliciosas. Posteriormente, utilizó técnicas más innovadoras como la compra de credenciales de acceso débiles en servicios de acceso remoto, ya sea RDP o redes VPN.

Avaddon, ha sido desarrollado utilizando el lenguaje de programación C++ y el entorno software “Microsoft Visual C++” en sus diferentes versiones, sin usar técnicas de empaquetado ni de ofuscación. Por otro lado, el malware utiliza técnicas para dificultar el análisis y no ser detectado de manera sencilla por los motores antivirus, para ello utilizan anti-VM o anti-debugging, en la cual se adjuntan strings cifradas y encapsuladas en objetos.

En el proceso de infección, este ransomware utiliza comandos en la consola de Windows para eliminar las copias de seguridad y shadow, impidiendo a la víctima recuperar el control de la máquina. [AA4]

Las organizaciones que han sido víctimas de ataques de esta variante son muy variadas, perteneciendo la mayor parte al sector de los servicios. Las organizaciones de la fabricación o la alta tecnología son las actividades más afectadas, seguidas de los servicios financieros.

En febrero de 2021, el estudiante español Javier Yuste publicó una herramienta de descifrado gratuita y Open Source en el portal GitHub, que permitía a los usuarios infectados por el ransomware Avaddon recuperar sus archivos, en el caso de que las víctimas no hayan apagado la computadora. La herramienta recorre la memoria RAM del sistema infectado en búsqueda de datos e información con la que se pueda recuperar la clave de cifrado original y posteriormente descifrar los archivos sin necesidad de pagar el rescate.

Varios días después de publicar la herramienta de descifrado, el ransomware fue modificado, incluyendo mejoras en el código y técnicas para anular las funciones de la herramienta. En señal de disculpas, el grupo modificó los contratos a los usuarios afiliados, por lo que se observó un aumento de la actividad del malware. [AA5]

En junio de 2021, el grupo Avaddon ha cerrado la operación, dejando de trabajar como Ransomware as a Service y entregando las claves de descifrado de las víctimas. La empresa BleepingComputer recibió un correo anónimo cuyo emisor se hacía pasar como agente del FBI el cual contenía una contraseña y un archivo ZIP protegido, incluyendo una carpeta con las claves de descifrado de las víctimas. La empresa Emsisoft publicó un descifrador gratuito para esta variante ransomware en la que se incluían 2934 claves de descifrado, donde cada una pertenece a una víctima específica. [AA6]

### 3.2.2 Proceso de desarrollo

#### 3.2.2.1. Identificación de las muestras

Los ejemplares seleccionados para el estudio de la familia ransomware Avaddon ha sido un conjunto de 9 muestras adquiridas de la fuente publica “ANY RUN”, siendo clasificados teniendo como referencia la primera fecha de aparición en la página “VirusTotal”, pudiendo ser de ayuda para observar las modificaciones temporales que realizaban los grupos para alterar los comportamientos y no ser detectados.

Se hará una búsqueda en la página “VirusTotal” de cada una de las muestras, obteniendo la información de relevancia que se incluye en la tabla, compuesto por el hash SHA-256, primera fecha de aparición y varios nombres con los que se denominan entre los motores de búsqueda de antivirus.

Nombre de la muestra	SHA-256	Primera vez subido a VirusTotal	Nombre	Nombre (Microsoft)
Avaddon_1	05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2	04/06/2020	“Trojan.GenericKD.46205682”	“Trojan:Win32/Ui-se!MSR”
Avaddon_2	9c9c4f20e4be9403e80e4f4bc09dcdcabdffcfd061950d7a226fa19b220e6d3bd	06/06/2020	“Gen:Heur.Mint.Titirez.VuW@IWozZSmG”	Undetected
Avaddon_3	4f198228806c897797647eacce0f92d4082476b82781183062a55c417c0bb197	09/06/2020	“Trojan:Win32/Ui-se!MSR”	“Gen:Vatiant.Ransom.Avaddon.2”
Avaddon_4	d1c1dfa0117fc595419464578959feb4c459ab99a498e0cb66cee626ceff6835	10/06/2020	“Trojan.GenericKD.46205682”	“Trojan:Win32/Ui-se!MSR”
Avaddon_5	4fd72c550987c7638e727c9d84b4940692bf94e101d3f5746bc4a8f377e49b37	23/06/2020	“Gen:Heur.Mint.Titirez.1.23”	“Trojan:Win32/Obfuscator.SL!MTB”
Avaddon_6	194d34ae7ddcfa9918c1230cda4615d275baf0bb1a2bb2e0c2c5fb70a87ff4fa	24/06/2020	“Gen:Heur.Mint.Zard.52”	“Trojan:Win32/C-hapak.DEB!MTB”
Avaddon_7	cc95a8d100f70d0fbf4af14e852aa108bdb0e36db4054c3f60b3515818a71f46	31/08/2020	“Trojan.Ransom.CDZ”	“Ransom:Win32/Avaddon.C!MTB”



Avaddon_8	cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3	20/10/2020	“Gen:Heur.Ransom.REntS.Gen.1”	“Ransom:Win32/Avaddon.C!MTB”
Avaddon_9	fc42cbd5939fcb8b6851021497041c80acd81ce7a43b952ab7807d5a05d2ed97	21/05/2021	“Gen:Variant.Ransom.Avaddon.3”	“Ransom:Win32/Avaddon.MK!MTB”

Para realizar el estudio y posteriormente una comparación con el conjunto de ejemplares, se seleccionará como modelo la muestra 1, aunque las tareas seguidas en los procesos de análisis han sido equivalentes. Esta muestra ha sido elegida como referencia gracias a la cantidad de información y detalles que nos proporcionan las diferentes herramientas en los análisis estáticos y dinámicos, facilitando su estudio.

#### 3.2.2.2. Detalles generales

La primera muestra de la familia “Avaddon” a analizar se observó por primera vez a principios de junio de 2020, siendo detectada por gran cantidad de motores de búsqueda de antivirus, 61 de 71 para ser exactos.

Las muestras han sido desarrolladas como un fichero de imagen ejecutable para máquinas de 32 bits, sin utilizar técnicas de empaquetado ni ofuscación para dificultar la detección del malware. En la mayoría de casos, se usa “Microsoft Visual C++” en diferentes versiones para modificar el malware y seguir incrementando su funcionalidad.

Una vez publicada la herramienta de descifrado desarrollada por Javier Yuste, el grupo realizó importantes modificaciones en el malware para solucionar las brechas que había encontrado este usuario, creando una segunda versión del ransomware mucho más robusta. El resto de modificaciones realizadas al malware no han sido de gran relevancia, ya que no se observan grandes cambios entre las diferentes muestras, variando elementos poco relevantes como las carteras de criptomonedas, ransomware Leaks...

#### 3.2.2.3. Procedimiento de infección

Este malware emplea los métodos de infección tradicionales, utilizando el correo electrónico para contactar con sus víctimas y adjuntando ficheros dañinos, aparentemente en forma de imagen, siendo en realidad un JavaScript, que se ejecuta produciendo el contagio del sistema y posteriormente encriptándolo.

Por otro lado, este malware ha incorporado una técnica más actual en sus métodos de infección denominada “dediks”, en la que los autores compran el acceso de diferentes equipos en los cuales se pueda ejecutar el código malicioso. [PIA]

#### 3.2.2.4. Análisis estático

Se denomina “análisis estático” al estudio realizado sobre una muestra sin detonar, es decir, sin ejecutar la función establecida dependiendo del tipo de archivo o componente a analizar, estudiando elementos como el código ensamblador, dominios, dependencias, cabeceras, etc... [AE1]

Las herramientas utilizadas en este proceso permiten extraer información sin necesidad de ejecutar la muestra, ya que la información está disponible para el usuario de manera inmediata y puede servir como base para guiar la investigación.

En este proceso se obtendrá información de gran importancia para comprender el comportamiento y funcionamiento del malware, realizando tareas de identificación del binario, obtención de strings, técnicas de anti detección o anti ingeniería inversa y debuggers.

Antes de comenzar el análisis estático, es de gran utilidad conocer los detalles más generales de la muestra a analizar, para ello emplearemos las herramientas online “VirusTotal” e “HibridAnalysis”.

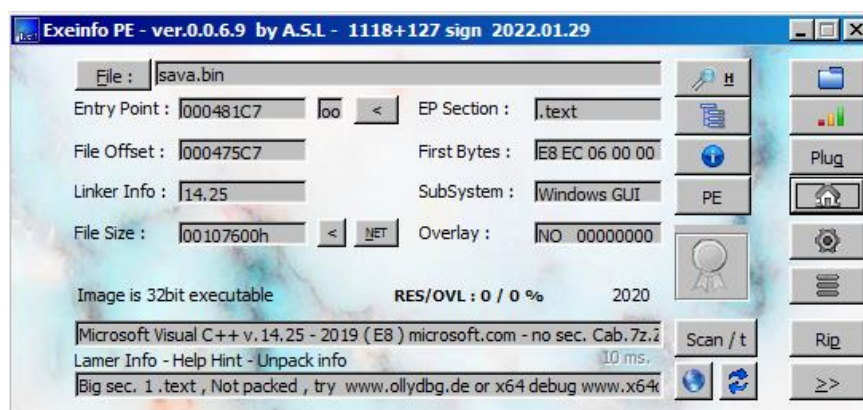
La herramienta “HxD” nos permitirá obtener el formato del archivo gracias a un conjunto de valores formados por el valor numérico con el que se identifica el formato de un archivo, denominado “Magic Number”, el texto del archivo y el PE Header. En ciertas ocasiones los grupos intentan ocultar la verdadera extensión del fichero con el objetivo de dificultar la detección del software malicioso e infectar a las víctimas. En el caso de esta muestra los valores que toman estos elementos son:

- Magic Number: MZP (4D 5A). Este identificador de formato nos indica con los dos primeros valores (MZ) que se trata de un archivo ejecutable.
- Texto del archivo: “This program cannot be run in DOS mode”. Este texto informa al usuario que el archivo ejecutable no es compatible con plataformas MS-DOS de 16 bits.
- PE Header: PE (50 45).

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Texto decodificado
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	08	01	00	.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°.!.í!.Li!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....\$. ....
00000080	28	7B	2D	2A	6C	1A	43	79	6C	1A	43	79	6C	1A	43	79	({-*l.Cyl.Cyl.Cy
00000090	37	72	40	78	79	1A	43	79	37	72	46	78	C6	1A	43	79	7r@xy.Cy7rFxÆ.Cy
000000A0	37	72	47	78	74	1A	43	79	37	72	45	78	6D	1A	43	79	7rGxt.Cy7rExm.Cy
000000B0	67	75	47	78	7D	1A	43	79	67	75	40	78	74	1A	43	79	guGx}.Cygu@xt.Cy
000000C0	67	75	46	78	F8	1A	43	79	37	72	42	78	77	1A	43	79	guFxs.Cy7rBxw.Cy
000000D0	6C	1A	42	79	B3	1A	43	79	A8	75	4A	78	7E	1A	43	79	l.By³.Cy"uJx~.Cy
000000E0	A8	75	41	78	6D	1A	43	79	52	69	63	68	6C	1A	43	79	"uAxm.CyRichl.Cy
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000100	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	04	00	.....PE..L...

Posteriormente, analizaremos el ejemplar utilizando la herramienta “HashMyFiles”, proporcionando información relativa a los algoritmos de codificación utilizados (MD5, SHA-256, SHA-512...) y datos como el tamaño, extensión o la ruta en la que se encuentra.

“Exeinfo PE” nos permite obtener detalles sobre los métodos y programas utilizados para su creación, observando que fue desarrollado mediante el programa “Microsoft Visual C++ v.14.25 - 2019”, siendo un fichero ejecutable en máquinas de 32 bits. Además, nos indica que el archivo no se encuentra empaquetado, mostrando la opción de utilizar debuggers como pueden ser “OllyDBG” o “64 Debug” en el caso de querer intentarlo.



“PEStudio” es una herramienta que proporciona gran cantidad de información de forma ordenada y clara, permitiendo obtener elementos como hash, IOS, strings, librerías... En la sección de librerías utilizadas de la muestra analizada podemos observar que se forma por un conjunto de 13 DLL’s, detectando 7 de ellas como maliciosas.

c:\users\ieuser\downloads\avaddon

indicators (48) \*

virustotal (61/71)

dos-header (64 bytes)

dos-stub (200 bytes)

rich-header (Visual Studio)

file-header (Jun.2020)

optional-header (GUI)

directories (6)

sections (99.91%)

libraries (13) \*

functions (208)

exports (n/a)

tls-callback (n/a)

.NET (n/a)

library (13)	flag (7)	type (1)	functions (208)	description
mpr.dll	x	implicit	1	Multiple Provider Router DLL
netapi32.dll	x	implicit	2	Net Win32 API DLL
iphlpapi.dll	x	implicit	1	IP Helper API
ws2_32.dll	x	implicit	6	Windows Socket 2.0 32-Bit DLL
rstrtmgr.dll	x	implicit	5	Restart Manager
crypt32.dll	x	implicit	1	Crypto API32
wininet.dll	x	implicit	7	Internet Extensions for Win32
kernel32.dll	-	implicit	144	Windows NT BASE API Client DLL
user32.dll	-	implicit	2	Multi-User Windows USER API Client DLL
advapi32.dll	-	implicit	23	Advanced Windows 32 Base API
shell32.dll	-	implicit	2	Windows Shell Common DLL
ole32.dll	-	implicit	8	Microsoft OLE for Windows
oleaut32.dll	-	implicit	6	oleaut32.dll

De la misma forma, podemos decir que el conjunto de las 13 DLL's que forman el malware, esta formado por 208 funciones, de las cuales 78 de ellas son maliciosas, perteneciendo la gran mayoría a las siguientes librerías: “kernel32.dll”, “user32.dll”, “advapi32.dll” y “ws2\_32.dll”.

### 3.2.2.5. Análisis dinámico

Se denomina “análisis dinámico” al estudio realizado sobre una muestra detonándola, es decir, llevando a cabo la función del archivo que se haya ejecutado. De esta forma se puede observar en primera persona cual es el comportamiento y funcionamiento del malware.

Este estudio es necesario realizarlo en un entorno de pruebas aislado y seguro, para no dañar ninguna unidad importante de nuestro dispositivo anfitrión. [AD1]

Aunque la ejecución de la muestra se llevará a cabo en un entorno controlado, el análisis dinámico se puede realizar de dos formas, dependiendo como se detone la muestra:

- Ejecución en un entorno de pruebas controlado.

La ejecución en un entorno de pruebas controlado se realizará en la máquina virtual Windows 7, configurada anteriormente para que se encuentre aislada y sea un ambiente correcto para el estudio de las muestras.

Antes de detonar cualquiera de las muestras, es necesario modificar la extensión del archivo de origen por “.exe”, convirtiéndolo en un ejecutable y comenzando la infección de la máquina. Además, se iniciarán las herramientas que utilizaremos en el análisis dinámico para comparar los cambios que se producen a nivel de procesos y tareas cuando la muestra malware se ejecuta, siendo el administrador de tareas, visor de eventos, Process Explorer y Autoruns.

La herramienta “Process Explorer” se trata de un administrador de tareas y monitor de procesos que nos permite observar la carga que realiza la ejecución de la muestra malware al dispositivo que se está virtualizando. A la hora de ejecutar la muestra, se observa cómo se crea un proceso que consume alrededor de tres cuartas partes de los recursos de la CPU, en algunos casos bloqueándola por segundos debido a la sobrecarga.

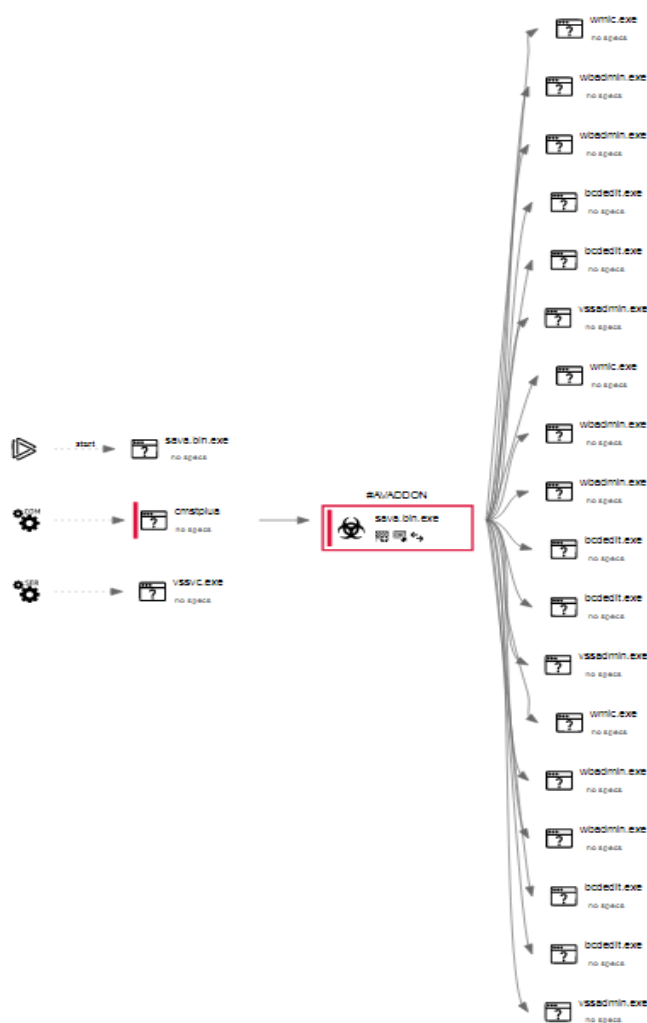


- Ejecución en la nube.

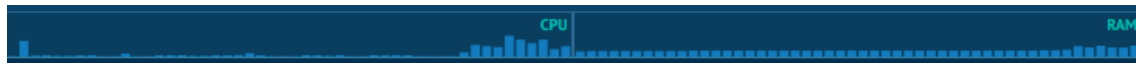
La herramienta online “Any Run” nos permite ejecutar el malware en una maquina online por tiempo limitado, configurando algunos valores de la forma que mayor nos convenga en cada análisis. En nuestro caso, seleccionaremos la misma maquina con la que se han realizado el resto de pruebas, un sistema operativo Windows 7 y una duración de análisis de 60 segundos, el tiempo que proporciona la página para los análisis estándar.

Una vez completado el tiempo de análisis, la herramienta nos proporciona información relevante como los principales procesos realizados, archivos generados y encriptados, rendimiento de RAM y CPU. Además, genera un documento que puede ser descargado con un resumen de toda la información obtenida durante el estudio de la muestra.

La herramienta produce un esquema de ejecución en el cual se muestran los procesos que se llevan a cabo a la hora de la infección, esquematizando cual es el camino que sigue el malware en su ejecución.



De la misma manera se muestran los recursos de CPU y memoria empleados durante todo el proceso, indicando con el color amarillo los periodos en los que se produce un mayor uso de recursos.



## Capítulo 4. Evolución

En este capítulo se describe el proceso empleado para la evaluación del estudio desarrollado. Se define la metodología de evaluación, los casos de prueba y el análisis de los resultados.

### 4.1. REvil

#### 4.1.1. Proceso de evaluación

En esta sección se presenta una evaluación en la que se comparan los diferentes estudios realizados a los conjuntos de muestras en búsqueda de alguna anomalía o información de interés para incluir en el informe del proyecto.

##### 4.1.1.1. Forma de evaluación

La evaluación de la familia ransomware REvil se realizará sobre un conjunto de 9 muestras que se ha seleccionado para llevar a cabo el estudio, perteneciendo a los años 2019, 2020 y 2021, ordenadas teniendo como referencia la primera fecha que aparece en la página “VirusTotal”. Con la recopilación de información de las muestras anteriormente analizadas, se evaluarán y comparará en búsqueda de algún dato o comportamiento significativo que pueda ser incluido en el estudio.

##### 4.1.1.2. Casos de prueba

Para evaluar las diferentes muestras de esta familia se han recopilado los datos e información obtenida de los análisis realizados y posteriormente se comparan todas las muestras seleccionadas en búsqueda de algún detalle que proporcione alguna información al respecto.

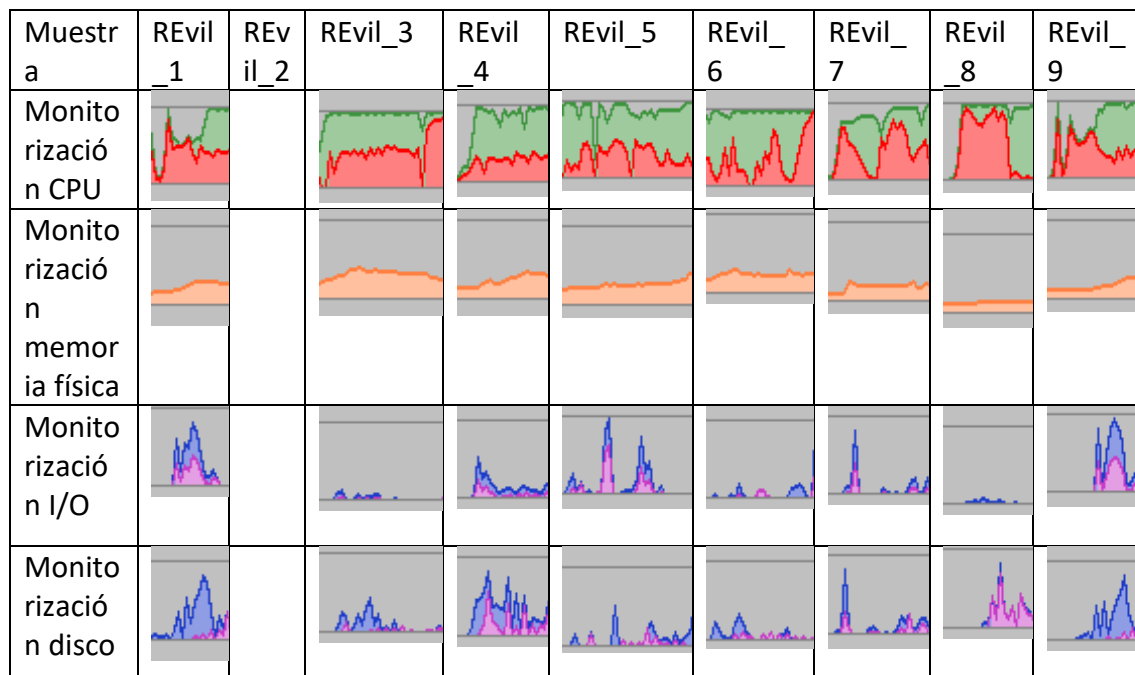
En la Tabla 4.1. se encuentra la puntuación recopilada por la página “VirusTotal” en la que se numeran la cantidad de motores de búsqueda de antivirus que reconocen la muestra como maliciosa.

Muestra	Numero de motores de búsqueda de virus
REvil_1	59/70
REvil_2	51/61
REvil_3	60/70
REvil_4	58/69
REvil_5	59/67
REvil_6	62/70
REvil_7	53/68
REvil_8	60/67
REvil_9	50/69

De los procesos llevados a cabo durante el análisis dinámico se obtiene información relevante que se muestra en las siguientes tablas.



En la Tabla 4.2. se muestran las gráficas del software “Process Explorer”, en el cual se observan los recursos consumidos por el malware en el proceso de infección del dispositivo.



Al intentar detonar la muestra numero dos para observar su comportamiento, observamos que al tratarse de una DLL no se puede ejecutar, por lo que no se puede visualizar el comportamiento de este ejemplar.

En la tabla 4.3. se muestran las extensiones que utiliza cada muestra para cifrar los archivos y datos que se encuentran en el dispositivo, además de la dirección web a la cual tienen que acceder las víctimas para realizar el pago del rescate.

Muestra	Extensión de archivos
REvil_1	fq73a8
REvil_2	
REvil_3	e768ejo218
REvil_4	
REvil_5	1467jq6d27
REvil_6	2d1sa
REvil_7	md1k2rb1
REvil_8	z9z24ksgk
REvil_9	r61a8

Se observa que todas las muestras cifran con una extensión diferente, siendo esta generada de manera aleatoria, formado por una cadena de varios dígitos combinando caracteres alfanuméricos y siendo agregado al final de la extensión de origen.

#### 4.1.2. Análisis de resultados

Utilizando los casos de pruebas citados anteriormente, se estudian los resultados y se desarrolla una evaluación del malware en el que se exponen los detalles más importantes a tener en cuenta.

En la tabla 4.1. se observa que se trata de una muestra reconocida por la mayoría de motores de búsqueda de virus como maliciosa. La muestra 2 observamos que pese a ser una muestra antigua, no es reconocida por la totalidad de estos motores. Por otro lado, la muestra 9 se encuentra en el mismo caso anteriormente citado, suponiendo que en el caso de esta muestra se puede deber a que se trata de un ejemplar relativamente actual.

Respecto al compilador empleado para desarrollar el código de las muestras incluyendo funcionalidad o modificando su comportamiento para no ser detectado, podemos decir que en las muestras escogidas se observan diferentes softwares utilizados para este proceso. El compilador más usado para llevar a cabo esta tarea es “Microsoft Visual C++”, empleado por la mayoría de las muestras escogidas, seguido del ensamblador denominado “TASM/MASM/FASM” y “Borland Delphi”, siendo esta la muestra tomada como modelo para realizar el informe del ransomware. Por otro lado, de las muestras 2 y 8 no se conoce el compilador utilizado para su desarrollo.

La tabla 4.2 muestra mediante gráficos la monitorización del equipo durante la ejecución de cada una de las muestras. Se observa que, en todos los ámbitos, ya sea CPU, I/O o lectura y escritura de disco se produce un consumo de recursos del 100%, en algunos casos llegando a bloquear el dispositivo para completar las funciones que se están ejecutando.

La tabla 4.3 muestra la extensión que incorpora el malware a los archivos que han sido cifrado, siendo generada de manera aleatoria combinando caracteres alfanuméricos con una extensión diferente en cada muestra.

### 4.2. Avaddon

#### 4.2.1. Proceso de evaluación

En esta sección se presenta una evaluación en la que se comparan los diferentes estudios realizados a los conjuntos de muestras en búsqueda de alguna anomalía o información de interés para incluir en el informe del proyecto.

##### 4.2.1.1. Forma de evaluación

La evaluación de la familia ransomware Avaddon se realizará sobre un conjunto de 9 muestras que se ha seleccionado para llevar a cabo el estudio, ordenadas teniendo como referencia la primera fecha que aparece en la página “VirusTotal”. Con la recopilación de información de las muestras anteriormente analizadas, se evaluarán y

comparará en búsqueda de algún dato o comportamiento significativo que pueda ser incluido en el estudio.

#### 4.2.1.2. Casos de prueba

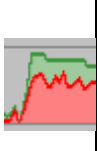
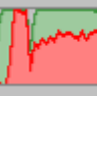
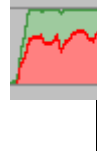

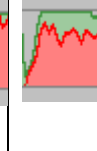
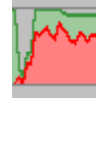
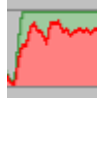
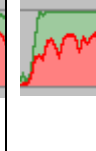
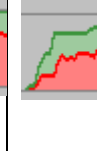
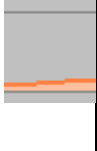



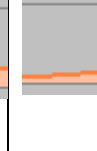


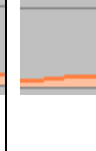
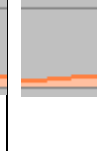
Para evaluar las diferentes muestras de esta familia se han recopilado los datos e información obtenida de los análisis realizados y posteriormente se comparan todas las muestras seleccionadas en búsqueda de algún detalle que proporcione alguna información al respecto.

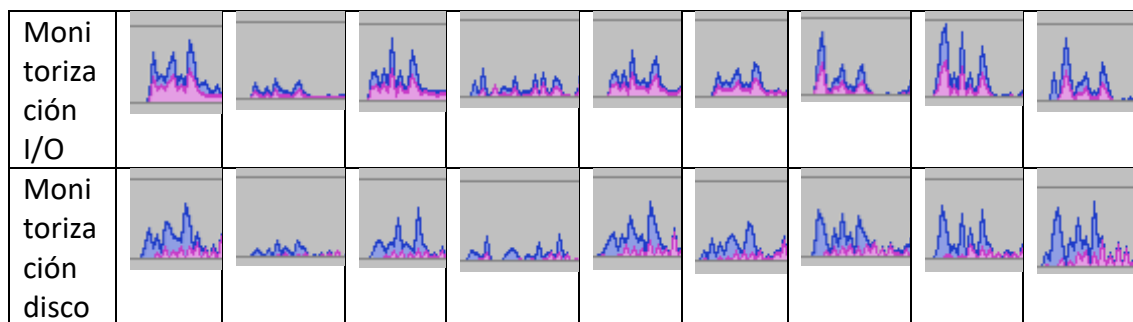
En la Tabla 4.1. se encuentra la puntuación recopilada por la página “VirusTotal” en la que se numeran la cantidad de motores de búsqueda de antivirus que reconocen la muestra como maliciosa.

Muestra	Numero de motores de búsqueda de virus
Avaddon_1	59/70
Avaddon_2	51/61
Avaddon_3	60/70
Avaddon_4	58/69
Avaddon_5	59/67
Avaddon_6	62/70
Avaddon_7	53/68
Avaddon_8	60/67
Avaddon_9	50/69

De los procesos llevados a cabo durante el análisis dinámico se obtiene información relevante que se muestra en las siguientes tablas.

En la Tabla 4.2. se muestran las gráficas del software “Process Explorer”, en el cual se observan los recursos consumidos por el malware en el proceso de infección del dispositivo.

Muestra	Avaddon_1	Avaddon_2	Avaddon_3	Avaddon_4	Avaddon_5	Avaddon_6	Avaddon_7	Avaddon_8	Avaddon_9
Monitoreación CPU									
Monitoreación memoria física									



En la tabla 4.3. se muestran las extensiones que utiliza cada muestra para cifrar los archivos y datos que se encuentran en el dispositivo, además de la dirección web a la cual tienen que acceder las víctimas para realizar el pago del rescate.

Muestra	Extensión de archivos
REvil_1	
REvil_2	
REvil_3	
REvil_4	
REvil_5	
REvil_6	1F2jJ
REvil_7	adCBaDCCac
REvil_8	adCBaDCCac
REvil_9	adCBaDCCac

Se observa que cada muestra cifra con una extensión diferente, siendo establecida en la propia configuración del malware, formado por una cadena de varios dígitos combinando caracteres alfanuméricos y siendo agregado al final de la extensión de origen.

#### 4.2.2. Análisis de resultados

Utilizando los casos de pruebas citados anteriormente, se estudian los resultados y se desarrolla una evaluación del malware en el que se exponen los detalles más importantes a tener en cuenta.

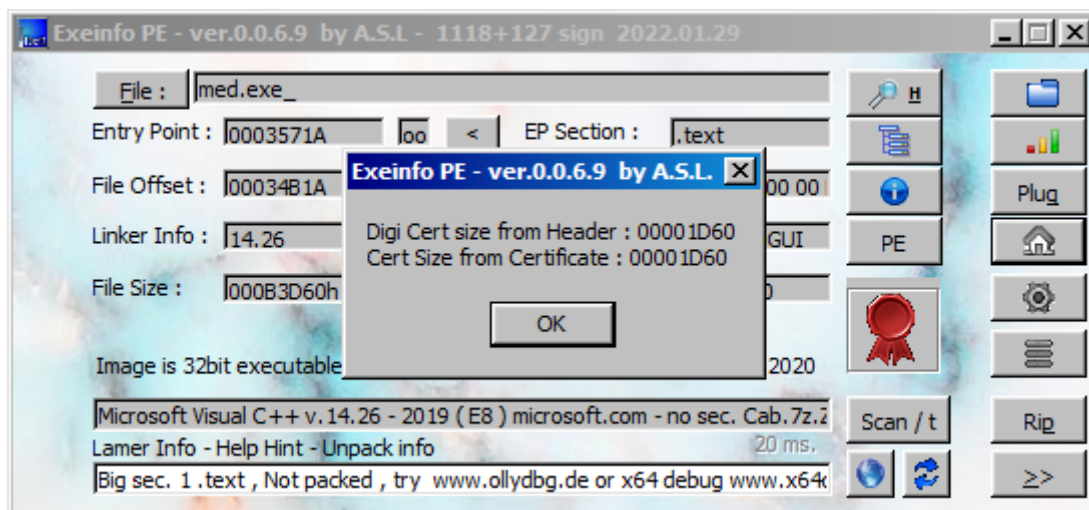
En la tabla 4.1. se observa que se trata de una muestra reconocida por la mayoría de motores de búsqueda de virus como maliciosa. La muestra 2 observamos que pese a ser una muestra antigua, no es reconocida por la totalidad de estos motores. Por otro lado, la muestra 9 se encuentra en el mismo caso anteriormente citado, suponiendo que en el caso de esta muestra se puede deber a que se trata de un ejemplar relativamente actual.

La tabla 4.2 muestra mediante gráficos la monitorización del equipo durante la ejecución de cada una de las muestras. Se observa que, en todos los ámbitos, ya sea CPU, I/O o lectura y escritura de disco se produce un alto consumo de recursos, en

algunos casos llegando a bloquear el dispositivo para completar las funciones que se están ejecutando.

La tabla 4.3 muestra la extensión que incorpora el malware a los archivos que han sido cifrado, siendo establecida en los archivos de configuración de la muestra. Además, se observa que dependiendo de la forma de cifrado que se utiliza en cada ejemplar, la nota de rescate que produce es distinta, en algunos casos con una extensión “.html” que se puede observar mediante un navegador web o “.txt”, observándose desde un editor de texto.

En la muestra 7, se puede observar que los desarrolladores de este ejemplar han incluido un “Certificado X509”, suponiendo que el objetivo buscado por estos usuarios sea que los motores de búsqueda de antivirus y la víctima no lo reconozcan como un malware y así poder infectar el dispositivo con mayor facilidad.



## Capítulo 5. Conclusión

En este capítulo se recogen las aportaciones realizadas durante el proyecto, los trabajos propuestos a futuro y los problemas encontrados durante el desarrollo. Previamente, se ha realizado un estudio del contexto del Ransomware as a Service y el análisis de las muestras seleccionadas, en búsqueda de información relevante con el objetivo de realizar un informe de las variantes analizadas.

### 5.1. Aportaciones realizadas.

Una vez completado el estudio, se puede verificar que se ha logrado cumplir los objetivos establecidos al principio del informe. Se realizó un estudio exhaustivo de las familias Ransomware as a Service seleccionadas, en este caso REvil y Avaddon, dos malware que han tenido gran importancia en los últimos años.

En este informe se ha recopilado tanto información sobre los grupos desarrolladores del malware como la metodología utilizada para llevar a cabo las infecciones en las víctimas, estudiando los métodos de extorsión y las técnicas utilizadas para obtener los beneficios buscados.

### 5.2. Trabajos futuros.

Los trabajos futuros propuestos en este trabajo se centran en mejorar el informe de las muestras ransomware analizadas, buscando ampliar el conocimiento sobre el comportamiento de las muestras.

Como trabajos futuros se proponen mejorar y añadir nuevos estudios a los ya realizados. Las mejoras propuestas a los estudios ya existentes son las siguientes:

- Analizar en profundidad el código ensamblador de las muestras.
- Analizar muestras con una fecha de compilación posterior a las elegidas, observando si el grupo ransomware ha añadido funcionalidad nueva.
- Creación y uso de reglas “Yara” y “Snort” para la detección preventiva de este tipo de variante ransomware.
- Realizar el análisis dinámico en un entorno de pruebas configurado con un sistema operativo Linux, observando si los resultados son los mismos.

### 5.3. Problemas encontrados

En el desarrollo de este proyecto se han presentado distintas dificultades que serán descritas a continuación.

El principal problema a la hora de llevar a cabo el proyecto se trata de la dificultad para encontrar información de calidad sobre el tema escogido, en este caso los Ransomware as a Service “REvil” y “Avaddon”.

Respecto a la selección de muestras para el estudio surgen varios problemas dependiendo de la familia. “REvil” a pesar de haber gran número de muestras diferentes, solo la minoría son válidas para llevar a cabo los análisis y poder ser estudiada. Por otro lado, la familia “Avaddon” padece de un problema parecido, al ser una variante relativamente nueva no se encuentran fácilmente las muestras para analizar.

## BIBLIOGRAFIA

- [1\*] <https://www.eset.com/es/caracteristicas/ransomware/>
- [1] <https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>
- [2] <https://discoverthenew.ituser.es/security-and-risk-management/2021/04/los-ataques-de-ransomware-aumentaron-un-485-en-2020>
- [3] <https://www.ituser.es/seguridad/2022/02/los-ataques-de-ransomware-aumentaron-un-105-en-2021-y-superaron-los-623-millones>
- [4\*] <https://www.itdigitalsecurity.es/actualidad/2022/03/los-ataques-de-ransomware-han-aumentado-un-253-debido-a-la-guerra-de-ucrania>
- [4] <https://www.welivesecurity.com/la-es/2021/07/05/ataque-masivo-ransomware-revil-comprometio-mas-1000-companias-mundo/>
- ? [5] <https://www.eleconomista.es/tecnologia/noticias/11566335/01/22/Rusia-detiene-a-todos-los-hackers-del-grupo-REvil-responsables-del-mayor-ataque-de-la-historia.html>
- [5\*] <https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/axa-enfrenta-al-ransomware-avaddon>
- [6\*] <https://www.unotv.com/ciencia-y-tecnologia/asi-opera-avaddon-hackers-que-atacaron-a-la-loteria-nacional/>
- [6] <https://blog.elhacker.net/2021/04/analisis-ransomware-avaddon-RaaS.html>
- [7] <https://es.malwarebytes.com/ransomware/>
- [7\*] <https://cybersecuritynews.es/espana-en-el-top-10-de-paises-mas-afectados-por-ransomware/>
- [8] <https://repository.unad.edu.co/handle/10596/35364>
- [9] [https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/#:~:text=Ransomware%20as%20a%20Service%20\(RaaS\)%20is%20a%20business%20model%20between,service%20\(SaaS\)%20business%20model](https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/#:~:text=Ransomware%20as%20a%20Service%20(RaaS)%20is%20a%20business%20model%20between,service%20(SaaS)%20business%20model)
- [10] <https://www.splashtop.com/es/the-5-most-devastating-ransomware-attacks-of-2021so-far>
- [10\*] <https://www.welivesecurity.com/la-es/2021/12/20/ransomware-2021-datos-ataques-grupos-mas-activos/>
- [HS1] <https://www.softwaretestinghelp.com/what-is-dark-web/>
- [A1] <https://protecciondatos-lopd.com/empresas/ransomware-as-a-service-raas/>
- [C1] <https://www.welivesecurity.com/la-es/2016/09/13/cifrado-ransomware-criptografico/#:~:text=El%20ransomware%20criptogr%C3%A1fico%20es%20capaz,acceder%20como%20carpetas%20del%20sistema.>
- [C2] <https://www.redeszone.net/noticias/seguridad/que-archivos-cifra-ransomware/>



- [C3] <https://www.sertecomsa.com/post/2017/06/23/spotlight-en-ransomware-métodos-de-cifrado-de-ransomware>
- [C4] [https://oa.upm.es/38772/1/PFC\\_EDUARDO\\_RUIZ\\_AZOFRA\\_2015.pdf](https://oa.upm.es/38772/1/PFC_EDUARDO_RUIZ_AZOFRA_2015.pdf)
- [C5] <https://hmong.es/wiki/Salsa20>
- [C6] [http://www.dma.fi.upm.es/recursos/aplicaciones/matematica\\_discreta/web/aritmetica\\_modular/rsa.html](http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/rsa.html)
- [C7] <https://protecciondatos-lopd.com/empresas/algoritmo-diffie-hellman/>
- [C8] [https://hmong.es/wiki/Elliptic\\_curve\\_cryptography](https://hmong.es/wiki/Elliptic_curve_cryptography)
- [H3] <https://attack.mitre.org/resources/faq/>
- [RL1] <https://www.theta432.com/post/tactica-cibercriminal-ransom-leaks>
- [RL2] [https://www.hornetsecurity.com/wp-content/uploads/2022/01/Cyberthreat\\_Report\\_2021\\_ES.pdf](https://www.hornetsecurity.com/wp-content/uploads/2022/01/Cyberthreat_Report_2021_ES.pdf)
- [E1] <https://www.bleepingcomputer.com/news/security/ransomware-gangs-target-companies-using-these-criteria/>
- [E2] <https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>
- [E3] <https://assets.sophos.com/X24WTUEQ/at/wpkww9k8xsn3m7j2hrpw5ws/sophos-state-of-ransomware-2021-wpes.pdf>
- [EX1] [3 Key Ransomware Trends in 2022: RaaS, Multi Extortion, IABs | Picus Security \(medium.com\)](https://www.picussecurity.com/3-Key-Ransomware-Trends-in-2022-RaaS-Multi-Extortion-IABs/)
- [IN1] <https://www.incibe-cert.es/blog/sodinokibi-caracteristicas-y-funcionamiento>
- [AE1] <http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2900/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y>
- [DS1] <https://www.secureworks.com/research/threat-profiles/gold-southfield>
- [\*DS2] <https://protecciondatos-lopd.com/empresas/sodinokibi/>
- [DS2] <https://www.pandasecurity.com/es/mediacenter/pandalabs/sodinokibi-infome-ransomware/>
- [DS\*] <https://docplayer.es/206203420-Sodinokibi-informe-malware-jorge-barelles-menes-pablo-cardos-marques-aaron-jornet-sales-javier-munoz-alcazar.html>
- [DS4] <https://www.incibe-cert.es/blog/sodinokibi-caracteristicas-y-funcionamiento>
- [AD1] <http://repository.unipiloto.edu.co/handle/20.500.12277/2900>

[AA1] <https://www.welivesecurity.com/la-es/2021/05/31/ransomware-avaddon-principales-caracteristicas/>

[AA2] <https://news.sophos.com/en-us/2021/05/24/what-to-expect-when-youve-been-hit-with-avaddon-ransomware/>

[AA4] <https://gdata.com.mx/blog/ransomware-avaddon-principales-caracteristicas/>

[AA5] <https://www.zdnet.com/article/free-decrypter-released-for-avaddon-ransomware-victims-aaand-its-gone/>

[AA6] <https://blog.segu-info.com.ar/2021/06/ransomware-avaddon-cierra-su-operacion.html?m=0>

[PIA] <https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5365-ccn-cert-id-28-20-avaddon-1/file.html>