

Indice de contenidos

Indice de figuras

Indice de tablas

Glosario de terminos

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, siendo los ejemplares de “REvil” y “Avaddon” cuyos grupos son “” y “” respectivamente, adquiridos de fuentes públicas.

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

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 para obtener la importancia

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 las ejemplares ransomware as a service escogidas, siendo “REvil” y “Avaddon” las familias escogidas para la elaboración del proyecto.

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

- Estudiar el contexto general del problema.
 -

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:

CAPITULO 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 elabora un breve estudio sobre la repercusión en la sociedad, incluyendo una revisión general del Ransomware as a Service.

Se agrega información útil como los principales grupos creadores de estos softwares maliciosos, así como su forma de actuar, herramientas de cifrado que utilizan, prototipos de empresa objetivo por estos ataques y los métodos de extorsión.

1.1. El contexto del problema

En los últimos años, los ataques ransomware han tomado gran importancia en nuestra sociedad, siendo una grave amenaza a nivel mundial.

Según un estudio realizado por la empresa británica Sophos, de las 5000 compañías de 26 países diferentes, un 51% de las compañías que habían sido víctimas de un ataque ransomware, recuperando sus datos prácticamente todas, ya sea por copias de seguridad (56%) o pagando el rescate (26%). [1]

Aprovechando la época de pandemia, estos grupos han incrementado sus cifras de ataques, aumentando en 2020 un 485% el volumen de ataques respecto 2019, y en 2021 un 150% respecto al año anterior. [2][3]

Se estima que fue en 2018 cuando se encuentra por primera vez este grupo, colaborando con GrandCrab. 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]?

Avaddon se vio por primera vez a principios de 2020, obteniendo una versión optima en junio. 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]

1.2. El estado de la cuestión

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 y que exige el pago de un rescate para poder acceder a ellos.” [7]

En 1989, fue reconocido el primer ransomware, “AIDS (Aids Info Desk)” o “PC CyborgTrojan”, escrito por el Dr. Joseph Popp, 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 llegaba a 90. Para obtener el acceso al dispositivo, el

usuario tendría que para 189 dólares a PC Cyborg Corp., en un apartado de Correos en Panamá Popp. [8]

Con la expansión del uso de Internet en los últimos 20 años 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 ofrece 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 programa, proporcionando en algunos casos soporte 24 horas al día. [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 5 ataques de ransomware más importantes hasta la actualidad han sido realizados por los principales grupos RaaS, en los que destacan [10]:

- DarkSide: A principios de mayo la empresa Colonial Pipeline Company fue víctima de un ataque ransomware, en la que cerro el suministro de combustibles a sureste de Estados Unidos, haciendo entrar en pánico a la población. Se trata del ataque con mayor repercusión del 2021, en el que la empresa pagó un rescate de 4.4 millones de dólares.
- REvil: Este grupo llevó un ataque contra el mayor proveedor de carne de vacuno del mundo, interrumpiendo completamente los servicios de venta de su carne. La empresa pago un rescate de 11 millones de dólares.
- Ransomware desconocido: en marzo se produjo un ataque contra el sistema de escuelas públicas de Buffalo, perdiendo décadas de material didáctico, expedientes y solicitudes de admisión. Además, dejó inutilizados los servicios como el jurídico y el contable.
- Evil Corp:
- Wizard Spider sobre Health Service Executive de Irlanda (HSE).

1.2.4. cuáles son sus hidden sites en TOR

1.2.5. como actúan estos grupos

1.2.6. qué herramientas de cifrado usan y como son de efectivas

Dado que la forma de actuar de los ransomware es encriptando los datos y archivos de la víctima para que no puedan ser utilizados. Los mecanismos en esta acción pueden ser muy varios, dependiendo de la simetría y el algoritmo escogido.

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

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. Inicialmente, 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 quíntuple: Intimidan y presionan a las empresas con vender información confidencial a competidores o usuarios interesados en la víctima.

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 identifica la planificación de tareas e hitos seguidos para llevar a cabo el desarrollo del proyecto.

La planificación seguida durante el proyecto ha sido el marco de trabajo Scrum, recogiendo las tareas en una pila que podrá ser modificada a lo largo de proyecto.

2.2.1. Identificación de tareas

Las principales tareas identificadas en el desarrollo del proyecto son:

- Tarea 1: Investigación
 -
- Tarea 2: Búsqueda de muestras ransomware
- Tarea 3: Creación y configuración del entorno de pruebas y herramientas.
 - Creación del entorno de pruebas
 - Instalar máquina virtual.
 - Importar máquina virtual principal.
 - Importar máquina virtual nexa.
 - Configuración del entorno de pruebas.
 - Configurar máquina virtual principal.
 - Configurar máquina virtual secundaria.
 - Configuración herramientas
- TAREA 4: ANALISIS ESTATICO DE LAS MUESTRAS
 - Obtener información general de la muestra.
 - Analizar las cabeceras y secciones del binario.
 - Analizar las librerías y strings.

- Analizar las técnicas anti detección y anti ingeniería inversa.
- TAREA 5: ANALISIS DINAMICO DE LAS MUESTRAS
 - Monitorizar CPU, memoria y procesos de ejecución.
 - Analizar
- TAREA 6: ESTUDIO Y EVALUACION DE LAS MUESTRAS
 - Características generales.
 - Procedimiento de infección.
 - Detalles generales.
 - Análisis estático.
 - Análisis dinámico.
- TAREA 7: ELABORACION DEL INFORME TECNICO SOBRE LAS MUESTRAS

2.2.2. Estimación de tareas

INVESTIGACION

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”.

Al iniciar la investigación, se han elegido diferentes muestras ransomware de la misma familia, con el objetivo de observar desigualdades a medida que los grupos ransomware modifican los ejemplares. Posteriormente se llevará a cabo un análisis estático, recolectando información de herramientas online o del estudio de cabeceras o PE.

CREACION ENTORNO VIRTUALIZADO DE PRUEBAS

Para crear el entorno de trabajo deseado se llevará a cabo la virtualización de dos **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.

La máquina secundaria que funcionara como nexos y firewall a la hora de realizar el estudio dinámico de las muestras se trata de “Kali Linux” en la última versión posible, en este caso “2022.2”, descargada de la página oficial.

Se importarán las dos OVA's sin modificar ningún parámetro, es decir, aceptando la configuración estándar que nos proporciona la herramienta.

CONFIGURACION DEL ENTORNO DE PRUEBAS

Una vez creados los servicios virtualizados de manera correcta, es necesario configurar las maquinas con las herramientas y servicios necesarios para llevar a cabo correctamente los análisis estáticos y dinámicos de los ejemplares ransomware.

En el análisis estático no es necesario modificar ninguna configuración de las maquinas virtuales, ya que las pruebas que se realizan a los malware se ejecutan sin detonar la muestra.

Por el contrario, en el análisis dinámico es necesario e indispensable modificar la configuración de las maquinas

Ya que las maquinas deben de tener acceso a Internet, deberán de estar configuradas en modo "Red NAT" de la siguiente forma:

- Crear una nueva red NAT en la maquina
- Cada maquina será conectada a la nueva red NAT anteriormente creada.
- En características avanzadas, seleccionamos la opción "Modo promiscuo" y "permitir todo" permitiendo al equipo visualizar los paquetes de la misma red sin necesidad de que vayan dirigidos hacia él.

HERRAMIENTAS

Antes de llevar a cabo cualquier tipo de análisis de una muestra ransomware, es necesario realizar una recopilación de información general sobre el malware, adquiriendo datos como el hash del archivo, cabeceras, librerías (DLLs) utilizadas...

Ciertas plataformas ofrecen servicios de este tipo, siendo de gran utilidad para entender el funcionamiento y comportamiento del malware a la hora de la infección de un dispositivo.

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... "Los resultados serán compartidos con el remitente y los socios examinadores, mejorando los resultados de los propios sistemas."

ANY RUN

MITRE ATT&CK

ATT&CK se define como “una base de conocimientos 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.”

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.

Los datos que utilizaremos en el estudio de cada muestra de esta herramienta serán las cabeceras del PE Header, y las DLLs con sus respectivas funciones.

PESTUDIO

PE-BEAR

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.

ANTIDETECCION Y ANTIINGENIERIA INVERSA

OBTENCION DE STRINGS

DEBUGGERS

MUESTRAS

El estudio se realizará sobre un conjunto de muestras de dos ejemplares Ransomware as a Service denominados “REvil” y “Avaddon”, adquiridas de la fuente “ANY RUN”

Las diferentes versiones de los ejemplares serán clasificados y estudiados 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. Además, se incluirá información adicional como será el SHA-256 y varios nombres con los que se denominan entre los motores de búsqueda de antivirus.

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, análisis dinámico, ejecución en un entorno controlado y en la nube.

3.1. REVIL

3.1.1. Descripción de la solución

3.1.2. Proceso de desarrollo

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

La primera fase se trata de la identificación de las muestras, seleccionando ejemplares que permitan ser analizados. Las siguientes fases son los detalles generales y el proceso de infección, siendo común en todas las muestras, ya que se trata del mismo malware.

Posteriormente se realizará un análisis estático, y otro dinámico. Finalmente, se realizará la ejecución en dos entornos diferentes, uno controlado y otro en la nube.

3.1.2.1. Identificación de las muestras

Los ejemplares escogidos para el estudio de la familia ransomware REvil ha sido un conjunto de 9 muestras, 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.

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/Revil.B”
REvil_3	7227cb2316b9e3b678698609b41ba67958d509fbf37c46cbde714b105b71bd68	27/12/2019	“Win32.Virus.Neshta.D”	“Virus:Win32/Neshta.A”
REvil_4	140f831ddd180861481c9531aa6859c56503e77d29d00439c1e71c5b93e01e1a	17/06/2020	“Gen:Variant.Zusy.306770”	“Ransom:Win32/Sodinokibi!MSR”
REvil_5	14c8e3f1f23d16c2c9a4272cd05d00461d27b372cc5f588b4bbfc6102bbbed708	03/08/2020	“Gen:Variant.Razy.525651”	“Ransom:Win32/Revil.A”
REvil_6	52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85	17/03/2021	“Win32.Trojan-Ransom.Revil.A”	“Ransom:Win32/Revil.A”

REvil_7	ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83	09/09/2021	"Gen:Variant.Ransom.Sodinokibi.66"	"Ransom:Win32/Revil.A"
REvil_8	0c10cf1b1640c9c845080f460ee69392bf aac981a4407b607e8e30d2ddf903e8	29/04/2022	"Trojan.GenericKD.49038346"	"Ransom:Win32/Revil.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 referencia la muestra 3, ya que nos proporciona más detalles de estudio, aunque las tareas seguidas en los procesos de análisis han sido equivalentes.

3.1.2.2. Detalles generales

La primera muestra de la familia malware REvil a analizar trata de finales del primer cuatrimestre del 2019, denominada como "ment.exe" o "noxinikiru.exe", y es detectada en la herramienta "VirusTotal" como maliciosa por 59 de 70 motores de búsqueda de antivirus.

Respecto al tiempo de creación del ejemplar, podemos establecer que el grupo ransomware dedicó un año de trabajo en su desarrollo antes de que saliera a la luz.

Las muestras han sido desarrolladas como un fichero de imagen ejecutable para máquinas de 32 bits, exceptuando la segunda muestra, siendo una DLL que actúa como una librería de imágenes. Teniendo en cuenta esta característica, ninguna de las muestras utiliza un empaquetado para dificultar la detección del malware, en cambio la muestra 2 muestra indicios de poder estar empaquetada, siendo posible desempaquetarlo con "DIE v3".

En la mayoría de casos, se ha utilizado el programa "Microsoft Visual C++" en sus diferentes versiones para incrementar la funcionalidad de las muestras.

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 por primera vez 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

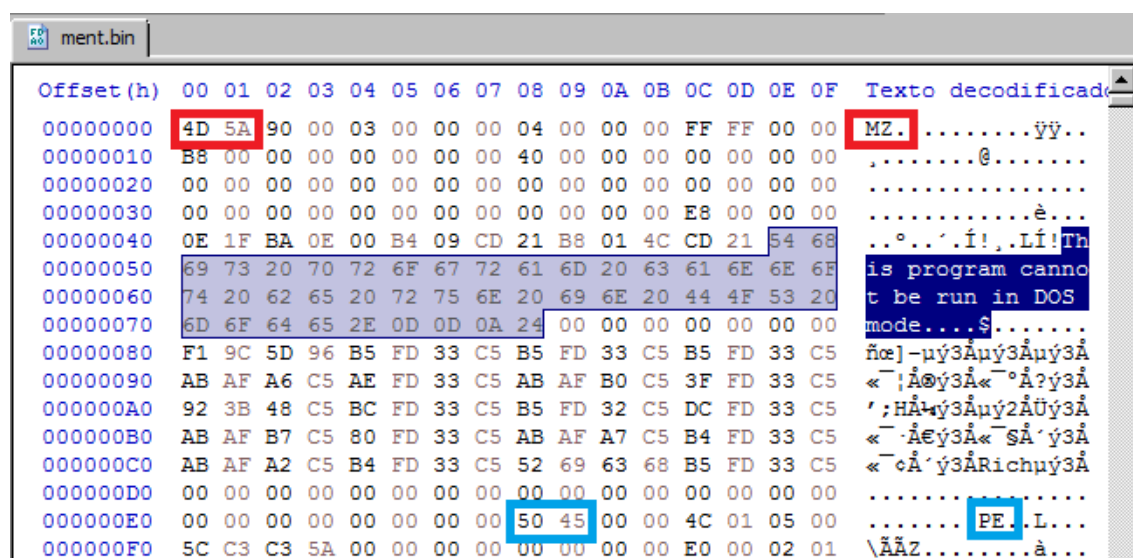
Se denomina “análisis estático” al estudio realizado sobre una muestra sin detonar, es decir, sin ejecutar la función establecida dependiendo del tipo de archivo o elemento a analizar, estudiando el código ensamblador, strings, dependencias, cabeceras, etc... [AE1]

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

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” y “AnyRun”.

Debido a que en ciertos casos se modifica la extensión del fichero para dificultar la detección del software malicioso a las víctimas, la herramienta “HxD” que nos permitirá obtener el formato del archivo gracias a un conjunto de valores formados por el Magic Number, texto del archivo y el PE Header. En esta muestra, los elementos anteriormente citados son:

- Magic Number: MZ (4D 5A).
- Texto del archivo: “This program cannot be run in DOS mode”.
- 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	E8	00	00	00è....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°...í!..Lí!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6E	is program cannot
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	F1	9C	5D	96	B5	FD	33	C5	B5	FD	33	C5	B5	FD	33	C5	file]-uy3Äuy3Äuy3Ä
00000090	AB	AF	A6	C5	AE	FD	33	C5	AB	AF	B0	C5	3F	FD	33	C5	«-;Äuy3Ä«-°Ä?y3Ä
000000A0	92	3B	48	C5	BC	FD	33	C5	B5	FD	32	C5	DC	FD	33	C5	';HÄuy3Äuy2ÄÜy3Ä
000000B0	AB	AF	B7	C5	80	FD	33	C5	AB	AF	A7	C5	B4	FD	33	C5	«-Äuy3Ä«-sÄ'y3Ä
000000C0	AB	AF	A2	C5	B4	FD	33	C5	52	69	63	68	B5	FD	33	C5	«-cÄ'y3ÄRichuy3Ä
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	50	45	00	00	4C	01	05	00PE..L...
000000F0	5C	C3	C3	5A	00	00	00	00	00	00	00	00	E0	00	02	01	\ÄÄZ.....ä...

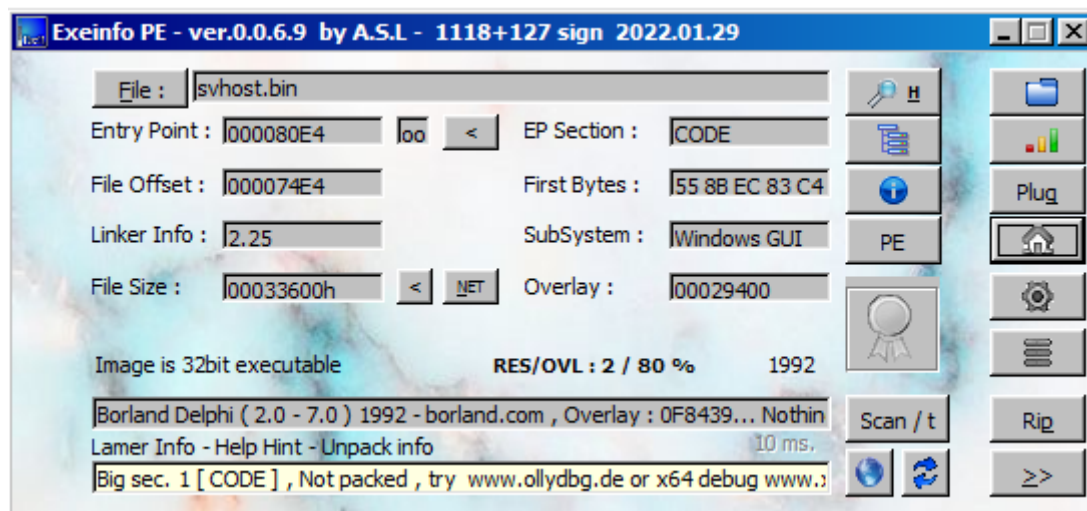
Posteriormente, analizaremos el ejemplar utilizando la herramienta “HashMyFiles”, proporcionando información relativa a los algoritmos de codificación utilizados (MD5, SHA-256, SHA-512...) y datos como el tamaño, extensión o la ruta en la que se encuentra.

```

=====
Filename       : ment.bin
MD5            : 0bb803ea960f1f2c88f4e0cd808c196e
SHA1          : 590053863146f758fcb7a876c02f5d4459aa6a43
CRC32         : e9e5590a
SHA-256       : a91948e235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
SHA-512       : 460f68c551136dc519c3ffaadf18d8536c2914c2bfa0e2d06926664f4b3e493e5e1c2dcd6d826d7637200289ff36b70330bbc0c91187ba8dfc7569d9c9718
SHA-384       : 03d7e5de87157a4e37fea8e27afa473e43e250270ca65912db672f2e959e848cc9db860966e9555b880206cc5018aeecc
Full Path     : C:\Users\IEUser\Downloads\FINAL\REVIL\FINAL\1\ment.bin
Modified Time  : 7/28/2022 12:08:37 PM
Created Time   : 7/30/2022 8:02:39 AM
Entry Modified Time: 7/30/2022 8:02:39 AM
File Size     : 327,168
File Version   :
Product Version :
Identical     :
Extension     : bin
File Attributes : A
=====

```

Gracias a la herramienta “Exeinfo PE” podemos obtener detalles sobre los métodos y programas utilizados para su creación, observando que fue desarrollado mediante “Microsoft Visual C++ 9.0 – 2008”, 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.



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.

La ejecución de la muestra se llevará a cabo de dos formas diferentes, dependiendo el entorno en el que se detone:

3.1.2.5.1. Ejecución en un entorno de pruebas controlado.

Las pruebas realizadas en un entorno controlado se desempeñarán de dos formas, aunque las dos se realizarán en la máquina principal anteriormente creada:

La primera, utilizando la herramienta online “Any Run”, que permite ejecutar el malware en una maquina por tiempo limitado, seleccionando la misma maquina con la que realizaremos el resto de pruebas (Windows 7). Nos proporciona información como los principales procesos realizados, archivos generados y encriptados, rendimiento de RAM y CPU...

La ejecución de esta muestra finaliza en 60 segundos, exigiendo al inicio de la virtualización gran cantidad de los recursos de la CPU.

Por otro lado, se detonará la muestra en la máquina virtual denominada como “maquina principal” y configurada para poder realizar un estudio, analizando los procesos de ejecución, identificando y recolectando ficheros cifrados, notas de rescate, buscando herramientas de descifrado...

3.1.2.5.2. Ejecución en la nube.

Por otro lado, en el caso de llevar a cabo la ejecución del malware en la nube se analizarán los procesos de ejecución, IOCs, dominios, carteras de criptomonedas...

3.2. AVADDON

3.2.1. DESCRIPCION DE LA SOLUCION

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, 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.

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/Ulisse!MSR”
Avaddon_2	9c9c4f20e4be9403e80e4f4bc09dcdcabdfcfd061950d7a226fa19b220e6d3bd	06/06/2020	“Gen:Heur.Mint.Titirez.VuW@IWozZSmG”	Undetected
Avaddon_3	4f198228806c897797647eacce0f92d4082476b82781183062a55c417c0bb197	09/06/2020	“Trojan:Win32/Ulisse!MSR”	“Gen:Vatiant.Ransom.Avaddon.2”
Avaddon_4	d1c1dfa0117fc595419464578959feb4c459ab99a498e0cb66cee626ceff6835	10/06/2020	“Trojan.GenericKD.46205682”	“Trojan:Win32/Ulisse!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/Chapak.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”

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, utilizando “Microsoft Visual C++” en diferentes versiones para modificar el malware y seguir incrementando su funcionalidad.

Las 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

3.2.2.5. Análisis dinámico

BIBLIOGRAFIA

- [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.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>
- [6] <https://blog.elhacker.net/2021/04/analisis-ransomware-avaddon-RaaS.html>
- [7] <https://es.malwarebytes.com/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>
- [A1] <https://protecciondatos-lopd.com/empresas/ransomware-as-a-service-raas/>
- [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>

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