ESPECIALIZACIÓN EN CIBERSEGURIDAD

ANÁLISIS ESTÁTICO Y DINÁMICO DEL RANSOMWARE MEDIANTE EL EMPLEO DE SANDBOXING PARA LA GENERACIÓN DE INFORMES DETALLADOS

DIANA PAOLA SUAREZ CARDOZO

Universidad® Católica de Manizales
VIGILADA MINEDUCACIÓN
Obra de Iglesia de la Congregación
Hermanas de la Caridad Dominicas de La Presentación de la Santísima Virgen

Análisis Estático Y Dinámico Del Ransomware Mediante El Empleo De Sandboxing Para La Generación De Informes Detallados

Trabajo de grado presentado como requisito para optar al título de *Especialización en Ciberseguridad*

Modalidad de grado: Monografía

Jhon Cesar Arango

Diana Paola Suarez Cardozo

UNIVERSIDAD CATÓLICA DE MANIZALES

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESPECIALIZACIÓN EN CIBERSEGURIDAD

MANIZALES, CALDAS

2024

Resumen

El avance constante en el desarrollo de software, hardware y redes de comunicación ha dado lugar a un mundo en el que las personas están interconectadas de manera continua. Sin embargo, esta interconexión también ha propiciado la creación de técnicas criminales que explotan las vulnerabilidades en equipos y redes para llevar a cabo acciones delictivas, como el robo o secuestro de información personal y financiera. Estos ciberdelincuentes buscan obtener beneficios económicos, lo que convierte estos actos en un proceso rentable para ellos.

En este contexto, el análisis de malware desempeña un papel fundamental. Permitiendo evaluar en detalle la funcionalidad y el impacto del malware, lo que a su vez facilita el desarrollo de medidas de protección más sólidas y efectivas. Este proceso se vuelve esencial para contrarrestar las amenazas para proteger tanto a individuos como a organizaciones.

En el presente estudio, se llevará a cabo un análisis específico del malware de tipo Ransomware, dado el auge que ha tenido en los últimos años al ser de los más usados para ataques cibernéticos. Con el análisis del Ransomware se tiene como finalidad mostrar su funcionamiento interno e impacto, lo que contribuirá a entender la forma en que este opera para así fortalecer las estrategias de seguridad cibernética y mitigar futuros riesgos.

Palabras clases: software, análisis, malware, vulnerabilidad.

Abstract

The advancement in software, hardware, and networks communications has allowed people to be continuously interconnected. However, this interconnection has also led to the emergence of criminal techniques that exploit vulnerabilities in equipment and networks to carry out unlawful actions, such as theft or the abduction of personal and financial information. These cybercriminals aim to gain economic benefits, turning these acts into a profitable process for them.

In this context, malware analysis plays a crucial role, allowing for a detailed evaluation of malware functionality and impact. This facilitates the development of more robust and effective protective measures. This process becomes essential in countering threats and protecting both individuals and organizations.

In the present study, a specific analysis of Ransomware malware will be conducted, given its surge in recent years as one of the most widely used for cyber-attacks. The purpose of analyzing Ransomware is to demonstrate its internal workings and impact, contributing to an understanding of how it operates. This, in turn, will strengthen cybersecurity strategies and mitigate potential future risks.

Key words: software, analysis, malware, vulnerabilities.

Contenido

Lista de Tablas

Lista de Figuras

1. Introducción

Los grandes avances de la tecnología han dado lugar a la aparición en el mercado de dispositivos cada vez más veloces, con capacidades mejoradas. Esta evolución tecnológica ha llevado consigo la creación de herramientas, tanto a nivel de software como de hardware, diseñadas para beneficiar a la sociedad en general, a organizaciones, comunidades específicas y diversos sectores aumentando las redes de intercomunicación a nivel global.

Sin embargo, este progreso tecnológico también ha dado lugar a una modalidad delictiva que se vale de la tecnología como medio para cometer actos criminales. La ciberdelincuencia es un fenómeno que ha proliferado junto con los avances tecnológicos. Los delincuentes, aprovechando la creciente conectividad de la sociedad y la dependencia de la tecnología en la vida moderna, han desarrollado nuevas formas de ataque y explotación de vulnerabilidades.

Estos actos delictivos pueden variar desde el robo de datos personales y financieros hasta el secuestro de sistemas informáticos mediante ransomware, propagación de virus y la realización de estafas en línea. Esto plantea desafíos significativos para la seguridad cibernética y la protección de datos, lo que ha llevado a la necesidad de que tanto individuos como organizaciones adopten medidas más sólidas de seguridad para mitigar las amenazas que se derivan de esta creciente modalidad de delincuencia tecnológica.

El malware, termino asociado a software malicioso, ha experimentado un desarrollo gradual que está relacionado con estos avances tecnológicos y el crecimiento exponencial de dispositivos tecnológicos susceptibles de sufrir ataques por parte de este tipo de software cuando se da el aprovechamiento de una vulnerabilidad.

En sus primeras etapas de desarrollo, el malware se originó a partir de investigaciones destinadas a estudiar cómo un software podría propagarse dentro de una red de computadoras.

Un ejemplo notable de esta época es el software Creeper, del cual hablaremos en detalle más adelante. Estas investigaciones también incluyeron pruebas de software en computadoras con el objetivo de automatizar tareas específicas, pero a menudo resultaban en comportamientos inesperados. Además, se exploraban las características de las computadoras para implementar software con fines específicos, que en primera instancia no se diseñaban con la intención de causar daño en el sistema en el que se ejecutaba.

Con el tiempo, estos estudios iniciales evolucionaron para incluir un análisis más profundo del comportamiento de este software malicioso, con el propósito de buscar formas de eliminarlo o remediar los cambios que generaba en el sistema víctima. Esto marcó el surgimiento de los primeros estudios de análisis de malware y la implementación de los primeros programas antivirus, diseñados para detectar y eliminar el software de los ordenadores 'infectados'.

El término malware, engloba diversas variantes de software malicioso que realizan diferentes comportamientos al explotar vulnerabilidades y atacar tanto a la víctima como a la red a la que está conectada. A lo largo de los años, la naturaleza de las amenazas ha evolucionado significativamente, pasando desde los primeros tipos de software con impactos más reducidos llegando a ataques más destructivos que junto con la ingeniería social tienen mayor alcance. Entre los tipos de malware existente, el ransomware ha tenido un mayor crecimiento en los últimos años debido a sus consecuencias en las redes de las víctimas y a las ganancias económicas que genera para los atacantes.

En respuesta a esta creciente ola de ataques y al desarrollo de software malicioso cada vez más sofisticado, el análisis de malware desempeña un papel crucial, dado que permite a las empresas desarrolladoras de soluciones de ciberseguridad y a las organizaciones en general comprender en detalle cómo funciona y qué impacto tiene este software. Esto, a su vez, facilita la

elaboración de planes de seguridad efectivos. El análisis de malware se define como un proceso exhaustivo que tiene como objetivo identificar y comprender el comportamiento, las intenciones y el impacto del software malicioso en sistemas informáticos y redes, con el fin de detectar y mitigar estas amenazas.

Este análisis puede llevarse a cabo de manera manual en un entorno de pruebas aislado o mediante el uso de dispositivos especializados, como el sandbox. En este estudio en particular, se hará uso del sandbox, una herramienta que permite descomponer, examinar y clasificar el malware sin la necesidad de infectar un dispositivo real. Esta técnica resulta fundamental para desarrollar soluciones de seguridad efectivas destinadas a proteger sistemas informáticos y redes contra este tipo de amenazas, sin poner en riesgo sistemas en producción.

Este estudio se enfocará en el análisis del ransomware WannaCry, el cual en el año 2017 infectó ordenadores en más de 150 países ante un ataque masivo. Este ransomware logró su expansión aprovechando una vulnerabilidad en los sistemas operativos Microsoft Windows que no habían sido actualizados. La elección de WannaCry como objeto de estudio se debe a que es uno de los ransomware que ha tenido un mayor impacto a nivel global en los últimos años llegando a afectar organizaciones en Colombia. Este malware se caracteriza por la forma en que opera, generando un fuerte impacto en los ordenadores que infecta, lo que lo convierte en un tema de estudio relevante y de interés. Adicionalmente se tendrá en cuenta otro tipo de ransomware para ampliar el conocimiento sobre este tipo de amenazas.

2. Objetivos

2.1 Objetivo General

Realizar un estudio del ransomware, empleando un enfoque combinado de análisis dinámico del software mediante el reporte de un sandbox y análisis estático, con el propósito de comprender su funcionamiento y evaluar su impacto. A partir de esto desarrollar y presentar una plantilla estructurada para la generación de informes basados en los resultados obtenidos de los análisis.

2.2 Objetivos Específicos

- Analizar el funcionamiento e impacto del ransomware mediante el análisis dinámico del software usando el reporte de un sandbox, complementado con el análisis estático para lograr una mejor comprensión del código.
- Proponer medidas preventivas eficientes y eficaces basadas en los hallazgos del análisis estatico y dinamico del ransomware.
- Desarrollar y presentar una plantilla para la creación de informes basados en los resultados obtenidos del análisis estatico y dinamico del ransomware.

3. Descripción del Problema

El malware es un término que se utiliza para describir cualquier tipo de software malicioso diseñado para causar daño en dispositivos programables, servidores y redes (*What is malware?*, s/f). Este software malicioso puede ser creado con una variedad de propósitos (*¿Qué es el malware?*, 2020), siendo los principales el robo de datos personales y financieros, el control de múltiples máquinas para lanzar ataques de denegación de servicio, así como la infección de computadoras con el fin de encriptar o apropiarse de su información para obtener ganancias.

Tanto los usuarios finales como las grandes corporaciones son víctimas de millones de ataques constantemente. Los delincuentes examinan las vulnerabilidades de los sistemas y utilizan técnicas de ingeniería social para engañar a los usuarios y lograr sus objetivos.

En la actualidad, con millones de computadoras conectadas a Internet, el malware ha experimentado un crecimiento significativo y se ha propagado de diversas maneras. Puede infiltrarse a través de sitios web falsificados donde los usuarios ingresan su información, mediante correos electrónicos que contienen enlaces falsos o archivos infectados, así como a través de código malicioso en aplicaciones que aparentan ser legítimas. La ingeniería social también se utiliza para aumentar la probabilidad de que un usuario acceda a estos programas.

Los principales tipos de malware y que son más utilizados en la actualidad para los ataques empleados, son el virus, gusanos, troyanos, el ransomware, entre otros. En este estudio se va a trabajar principalmente sobre el ransomware.

Dada la gran cantidad de malware potencialmente peligroso que circula en línea y la necesidad de contar con múltiples capas de protección contra posibles ataques, el análisis de malware se ha vuelto fundamental en la seguridad de las redes. Este análisis implica examinar en un entorno controlado archivos, correos electrónicos, enlaces y otros elementos que, después de

pasar por diversos controles, ingresan a la red. El objetivo de este es reducir el riesgo de un posible ataque.

El análisis de malware, como se define en Sikorski & Honig[1], se refiere al proceso de descomponer o examinar el malware con el objetivo de comprender su funcionamiento, identificarlo y desarrollar estrategias para combatirlo o eliminarlo. Este tipo de análisis se lleva a cabo con el propósito principal de obtener información detallada sobre cómo ocurrió la intrusión en la red, identificar todas las posibles máquinas y archivos infectados, y determinar las vías a través de las cuales se realizó la intrusión. Además, el análisis de malware busca identificar formas efectivas de mitigar los riesgos asociados a este.

Cuando uno o varios nodos de la red se infectan debido a un ataque de malware, se requiere realizar el análisis del malware para limitar la propagación de la infección y/o eliminar el malware de la red. Este análisis se puede llevar a cabo de manera estática o dinámica, evaluando el comportamiento del malware en la red. Esto proporciona el conocimiento necesario para tomar las medidas adecuadas, comprendiendo cómo se comporta el malware y cuáles son sus componentes para después establecer políticas de seguridad que se adapten a la estructura del malware, lo que permite eliminarlo de los nodos afectados y prevenir posibles ataques futuros del mismo tipo de malware.

[1] Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The hands-on guide to dissecting malicious software.

4. Planteamiento del Problema

¿Cómo el análisis de malware ayuda en la generación de medidas que permitan fortalecer la seguridad de las redes y además aumentar el conocimiento de los equipos implicados en la seguridad para mitigar futuras amenazas?

5. Justificación

El propósito de este trabajo es llevar a cabo la revisión de análisis de reportes de un sandbox sobre ransomware dado que el sandbox es una herramienta que permite realizar un análisis más rápido y seguro, sin riesgo de infectar ningún ordenador con archivos maliciosos pero que generalmente los reportes utilizan un lenguaje muy técnico sobre el análisis del software malicioso.

Los sandbox son herramientas utilizados en el área de seguridad informática, lo cuales permiten realizar pruebas en un entorno aislado antes de comprometer la red principal de una empresa. En este estudio, el sandbox proporciona tanto un análisis dinámico como estático del malware, lo que permite identificar el funcionamiento y el impacto del Ransomware cuando ingresa al sistema de la víctima.

Este tipo de análisis es de gran importancia para las organizaciones en casos en los que existan dudas sobre la seguridad de un archivo o cuando se sospecha que un ordenador en la red puede estar infectado cuando se ha realizado la descarga de un archivo con un alto potencial de riesgo o a comportamientos inusuales que se detecten en la red.

Dado que existen numerosos tipos de malware, este tipo de análisis por medio de sandbox también ayuda a identificar el tipo específico de malware presente en el archivo. Además, es crucial que los investigadores comprendan las diferencias entre estos tipos de

malware para analizar su comportamiento con mayor facilidad y definir estrategias efectivas para combatirlo.

Normalmente, después del análisis de malware, se generan firmas de seguridad. Estas firmas pueden clasificarse principalmente en dos categorías, como se menciona en Sikorski & Honig, 2012[2]:

Firmas basadas en Host: También conocidas como indicadores, se utilizan principalmente para detectar los cambios realizados por el malware en el ordenador de la víctima.

Firmas de red: Estas firmas se emplean para detectar código malicioso en el tráfico de red. Aunque no siempre requieren un análisis de malware previo para su generación, su eficacia puede aumentar significativamente si se crean después de dicho análisis.

Este enfoque integral en el análisis de malware y la generación de firmas de seguridad contribuye a fortalecer las defensas cibernéticas de una organización y a proteger su red contra amenazas potenciales.

Dado que los informes de los sandbox pueden presentar la información en un lenguaje técnico, en este estudio se propone desarrollar una plantilla que simplifique la comprensión de dichos informes mediante un análisis detallado. El objetivo principal es facilitar la creación de documentos no técnicos que aborden las generalidades en las que se presenta la información, contribuyendo así a una mejor comprensión del comportamiento del malware. Esta iniciativa cobra relevancia, ya que no solo los profesionales en seguridad informática necesitan comprender el funcionamiento del malware, sino que también es esencial que esta información sea accesible para cualquier persona.

[2] Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The hands-on guide to dissecting malicious software.

6. Contexto Geográfico

Este estudio se enfoca en el análisis del Ransomware WannaCry, utilizando el informe resultante de un sandbox. WannaCry es un ransomware de cifrado que, como su nombre sugiere, cifra los datos de la computadora de la víctima después de aprovechar una vulnerabilidad, exigiendo luego un rescate para descifrar la información.

En 2017, este malware tuvo un impacto a nivel global, afectando aproximadamente a 230,000 computadoras en alrededor de 150 países (*¿Qué es el ransomware WannaCry?*, 2023). Este malware aprovecha una vulnerabilidad en los sistemas de Microsoft mediante la explotación del exploit EternalBlue. A pesar de que Microsoft había emitido previamente un parche de seguridad para proteger contra este exploit, los responsables del ataque llevaron a cabo sus acciones en sistemas no actualizados, aprovechando la falta de prioridad que algunas empresas otorgan a las actualizaciones de sus sistemas (*¿Qué es el ransomware WannaCry?*, 2023).

A nivel de Colombia, se estima que más de 20 empresas resultaron afectadas por este malware. En respuesta a esta amenaza, la Policía Nacional emitió comunicados dirigidos a varias empresas estatales, con el propósito de brindar recomendaciones para prevenir futuros ataques de este malware (Colprensa, 2017).

Las consecuencias de los ataques de Ransomware presentan afectaciones a nivel global, como se evidencia en la información previamente mencionada. En este sentido, cualquier empresa se encuentra potencialmente en riesgo si un atacante identifica y explota vulnerabilidades en sus sistemas con el fin de tomar control de sus datos y privar a la víctima de la posibilidad de recuperarlos desde sus ordenadores afectados.

En el contexto global actual, donde las amenazas de Ransomware pueden afectar a organizaciones en cualquier parte del mundo, el análisis de estas amenazas se convierte en una

prioridad crucial para garantizar la seguridad de la información. Comprender y analizar detenidamente el malware es fundamental, ya que proporciona información esencial sobre cómo los sistemas de una organización podrían verse afectados en caso de un ataque. Esto incluye evaluar el potencial impacto en los equipos y recursos, lo que a su vez permite una mejor preparación para enfrentar tales amenazas.

7. Marcos de la Investigación

7.1 Antecedentes

Las primeras manifestaciones de malware se remontan a la década de 1980; sin embargo, su proliferación comenzó a ganar impulso en la década de 1990, coincidiendo con la popularización de los ordenadores con sistema operativo Windows (Belcic, 2023). Antes de que el desarrollo de malware se generalizara, se llevaron a cabo investigaciones sobre diversas vulnerabilidades que podrían afectar a los ordenadores, así como simulaciones para estudiar su comportamiento.

A continuación, se presenta una cronología de eventos relevantes relacionados con el avance del malware desde sus primeros inicios:

- En 1972, Robert Thomas Morris creó Creeper, una de las primeras manifestaciones de software autorreplicante. Aunque algunos no lo consideran un virus, su propósito era demostrar que el software podía replicarse a través de nodos en una red. Cuando infectaba un ordenador, mostraba el mensaje: "I'm a creeper... catch me if you can!" y continuaba replicándose.

  Para eliminar este 'virus', se desarrolló el software Reaper, considerado el precursor de los actuales antivirus (ESET Latinoamérica, 2012).

- En 1981, Richard Skrenta desarrolló Elk Cloner, uno de los primeros virus a gran escala que afectó a ordenadores Apple II. Este virus se instalaba en el disquete y se propagaba a otros discos, pero no causaba daño ("¿Qué es Elk Cloner?", 2022). En lugar de eso, mostraba un poema en la pantalla cuando se iniciaba el disco.

Elk Cloner,

El programa con personalidad,

llegará a todos tus discos,

se infiltrará en todos tus chips.

¡Sí, es el Clonador!

Se pegará a ti como pegamento,

también modificará tu RAM.

¡Que entre el clonador!

- En 1984, Fred Cohen publicó el estudio "Computer Viruses – Theory and Experiment", que proporcionó la primera definición formal de virus informáticos como programas capaces de infectar otros programas, incluyendo versiones evolucionadas de sí mismos (de ESET Latinoamérica, 2012).

- En 1989, se documentó el primer incidente conocido de ransomware, denominado "AIDS trojan". Joseph Popp fue el creador y distribuidor de este malware que se propagó a través de disquetes conteniendo un software capaz de infiltrarse en las computadoras. Una vez en el sistema, el ransomware establecía una regla que, tras 90 reinicios, encriptaba los nombres de los archivos, ocultándolos o cambiándolos de directorio. Posteriormente, aparecía un mensaje solicitando un pago mensual de 189 dólares o una suma única de 379 dólares para descifrar los datos (Amanda, 2021). Como respuesta a esta amenaza, se desarrolló el software AIDSOUT con el propósito de contrarrestar este tipo de ransomware.

- En 1990, Yisrael Radai define por primera vez el software malicioso como ‘malware’ (Belcic, 2023).
- En 1995, con la llegada de Windows 95, se desarrollaron los primeros virus dirigidos específicamente a esta plataforma. El primer macrovirus conocido fue Concept, que infectaba archivos de Microsoft Word ocultándose en las macros del programa (Ramirez, 2020). Este virus fue ampliamente propagado y para 1997 se estima que más de 30.000 ordenadores fueron infectados.
- En 1996, se desarrollaron varios virus, incluyendo Boza, que infectaba archivos de 32 bits en Windows NT y Windows 95. También se destacó el virus Zhengxi, un virus polimórfico que residía en la memoria y ejecutaba droppers, archivos ejecutables diseñados para infectar la máquina. Eugene Kaspersky fue el que descubrió este virus.
- En 2002, se propagó rápidamente el gusano JS/Exploit-Messenger, que aprovechaba una vulnerabilidad en el navegador Microsoft Internet Explorer. Aunque no era dañino, se propagó rápidamente al tomar la lista de usuarios de MSN Messenger y enviar mensajes (Amanda, 2021).
- En 2005, aumentó la proliferación de adware, software que generaba ventanas emergentes de publicidad molesta. El adware 180 Solutions fue el que generó más molestias, ya que afectaba a cualquier usuario con conexión a Internet (*¿Qué es el adware? Los 7 ejemplos más terribles (2023)*, s/f).
- En 2007 se dio una proliferación en cuanto al desarrollo de malware, siendo el phishing una de las principales formas de propagación (Belcic, 2023).

- En 2009, comenzó a popularizarse el uso de ataques con fines económicos y la oferta de servicios para realizar ataques más amplios. El virus Confiquer, que aprovechaba una vulnerabilidad en Windows Server, afectó a aproximadamente el 8% de los ordenadores conectados a Internet en América Latina. A pesar que antes de la proliferación de los ataques Windows ya había sacado el parche de seguridad, solo en Latinoamérica logró afectar aproximadamente al 8% de los ordenadores conectados a internet ("¿Qué es Conficker?", 2022).
- En 2010 el gusano Stuxnet fue capaz de dañar el sistema de centrifugadoras en una planta de energía atómica en Natanz, Iran. Dentro de la investigación realizada, se identificó que el gusano entro a la red por medio de una USB infectada que se conectó a los sistemas que controlaban las centrifugadoras y a travez de una vulnerabilidad de Windows logró expandirse hasta llegar al sistema central haciendo que las centrifugadoras tuvieran comportamientos no esperados haciendo que con el tiempo un 20% porciento de las centrifugadoras quedaran sin funcionamiento (BBC News Mundo, 2015).
- En 2013 el ransomware CryptoLocker se generalizó por medio de campañas de phishing que hacían que las victimas descargaran archivos adjuntos para que después el Troyano que estaba adentro comenzara a encriptar la información de los ordenadores Windows para después solicitar un rescate sobre estos datos (Belcic, 2020).
- En 2016 en software Mirai creado por Paras Jha y Josiah White ataca dispositivos IoT que funcionan con procesadores ARC, logrando ingresar a los dispositivos que tenían configurado el usuario y contraseña por defecto (Cloudflare, s/f), para después crear una red de bot conocida como botnet o zombies para realizar ataques de DDoS.

- Entre el 2017 y 2023 el ransomware comenzó a tomar más fortaleza entre los ataques realizados a grandes organizaciones, como por ejemplo el ransomware wannacry descrito en un apartado anterior.

Estos eventos demuestran cómo el malware ha evolucionado a lo largo del tiempo, pasando de experimentos y pruebas a amenazas masivas que buscan causar daño y obtener beneficios económicos. La creciente importancia del análisis de malware radica en la necesidad de desarrollar contramedidas, parches de seguridad, firmas de seguridad y software de detección y eliminación para protegerse contra estas amenazas en constante evolución.

A lo largo de los años, se ha presenciado un aumento significativo en la frecuencia de los ataques de ransomware. En la actualidad, este tipo de malware ocupa los primeros puestos en las listas de software empleado para llevar a cabo ataques contra organizaciones (Valades, 2022). Esta tendencia se debe, en gran medida, a que el ransomware se ha convertido en una fuente lucrativa para los que hacen uso de este tipo de malware.

En los inicios de los ataques de ransomware, los perpetradores solían cifrar los datos de las organizaciones objetivo y exigían un rescate económico. Esta suma, por lo general, se requería en criptomonedas debido a su difícil rastreo. En caso de que la empresa afectada optara por no cumplir con las demandas, se iniciaba un proceso de negociación, y la empresa se enfrentaba a tener que continuar operando con la pérdida de información o arriesgarse a pagar sin garantías de que fueran restituidos por completo los datos.

En la actualidad, la dinámica ha evolucionado, y si la empresa no satisface las demandas de los atacantes, estos proceden a vender o divulgar la información de la organización afectada en internet (“La evolución del ransomware,” 2023). Esto es aún más perjudicial para la organización, ya que no solo sufre pérdidas económicas, sino que también se expone a que otras

empresas del mercado conozcan sus datos confidenciales. Además, la divulgación de información privada puede dar lugar a demandas legales y afectar negativamente la imagen de la empresa ante sus stakeholders y clientes.

Por otro lado, en investigaciones previas relacionadas con el análisis de malware, se ha abordado el estudio de las técnicas de análisis estático y dinámico del código. Se ha observado que una de las limitaciones de las herramientas que se centran principalmente en el análisis estático para la detección de software malicioso es su incapacidad para detectar eficazmente ciertos programas maliciosos que están diseñados para ocultarse y evitar la detección. Esta táctica se conoce como "ofuscación de código" (Moser et al., n.d.).

La ofuscación de código es una técnica utilizada por los creadores de malware para dificultar la comprensión y el análisis del código malicioso. Al ocultar su funcionalidad real y mezclarla con elementos aparentemente inofensivos, el malware puede evadir las herramientas de análisis estático, que inspeccionan el código sin ejecutarlo (Moser et al., n.d.). Esto representa un desafío para los investigadores y profesionales de ciberseguridad, ya que hace que la detección y el análisis de malware sean más complicados y requieran enfoques adicionales, como el análisis dinámico, que implica la ejecución controlada del software malicioso en un entorno aislado para observar su comportamiento.

Dada esta limitante, en otros trabajos se hace un análisis de las herramientas usadas para el análisis estático y dinámico de malware y como estos se complementan para un mejor estudio del software que se está analizando dados los diferentes tipos de malware que existen y como estos pueden afectar de diferentes formas los ordenadores según los privilegios con los que cuente al momento de la ejecución, los recursos que utilice y las afectaciones con las que se haya programado para realizar en la maquina víctima (Egele et al., 2012). Entre los métodos que se

pueden utilizar para el análisis se destacan el análisis de los API que se realizan al momento que se ejecuta el software a nivel del usuario, análisis de las funciones ejecutadas a nivel del kernel, análisis en emuladores y máquinas virtuales para ejecutar los programas en un ambiente controlado, y por último, análisis del comportamiento a nivel de red para un mejor acercamiento de los movimientos laterales que puede realizar por lo cual se requiere una red aislada para contar con los dispositivos y accesos necesarios para un mayor análisis.

Entre los métodos destacados para llevar a cabo un análisis integral del malware descrito en Egele et al.,[3] se encuentran:

- Análisis de API: Este enfoque implica el estudio de las API que se realizan durante la ejecución del software a nivel de usuario. El seguimiento detallado de las interacciones del programa con las API proporciona una comprensión más profunda de su comportamiento y puede revelar actividades sospechosas.
- Análisis de funciones ejecutadas a nivel del kernel: Al examinar las funciones ejecutadas a nivel del kernel, se pueden identificar operaciones de bajo nivel que podrían pasar desapercibidas en un análisis superficial. Por ejemplo, esto permite detectar cambios a nivel del núcleo del sistema.
- Análisis en emuladores y máquinas virtuales: Se hace uso de entornos controlados como emuladores y máquinas virtuales lo cual permite ejecutar programas maliciosos en un ambiente aislado y seguro sin afectar la red principal.

[3] Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools.

- Análisis del comportamiento a nivel de red: Esto permite detectar movimientos laterales y comunicaciones sospechosas.

Con esto se busca mostrar que la combinación de estos enfoques de análisis estático y dinámico, junto con la consideración de factores como los privilegios, los recursos y los métodos de propagación, resulta esencial para abordar la complejidad del malware dado que es una estrategia integral con la que se busca garantizar una mejor comprensión del malware y una mayor eficacia en su detección y mitigación.

Por otra parte, En el contexto de este trabajo, que se enfocará en el análisis de los informes generados por los sandbox, resulta crucial resaltar la relevancia de las investigaciones previas que han empleado estas herramientas. Como se mencionó anteriormente, los sandbox desempeñan un papel fundamental al posibilitar un análisis detallado de malware en un entorno virtualizado. Estas herramientas suelen emplear un enfoque dual que incluye tanto el análisis estático, centrado en la evaluación del código, como el análisis dinámico, que implica la ejecución del malware en un entorno virtual. La combinación de estos dos enfoques proporciona una evaluación más detallada de las amenazas, ayudando a comprender y mitigar posibles riesgos de seguridad.

En diversos estudios relacionados con el uso de sandbox, se ha abordado la evolución del malware, que ha desarrollado la capacidad de detectar y diferenciar cuando son ejecutados en entornos virtualizados o en las máquinas de las víctimas. Este fenómeno permite a las amenazas camuflarse y limitar sus funciones para eludir la detección (Liu et al., 2022). Como respuesta a este desafío, se han propuesto varias técnicas, herramientas y ambientes que dificultan al malware identificar con facilidad si está siendo ejecutado en un entorno controlado (Inoue et al., 2009).

Adicionalmente, se han llevado a cabo un análisis de las vulnerabilidades asociadas principalmente a los sandbox públicos o los Public Malware Sandobox Analysis System (Public MSAS en inglés). Estos sandbox públicos presentan una vulnerabilidad dado que, al hacer uso de una red pública, los creadores de malware o cualquier usuario pueden interferir en la conexión (Yoshioka et al., 2010). Esto les permite montar o cambiar un código diferente, evitando así la detección del verdadero malware.

7.2 Marco Normativo

En el contexto de este trabajo de grado, que se enfoca en el análisis de ransomware para acceder de manera no autorizada a sistemas de individuos u organizaciones con el propósito de bloquear y robar datos privados, es relevante destacar la Ley 1273 de 2009 en Colombia. Esta legislación establece sanciones para actividades que atentan contra la disponibilidad, integridad y confidencialidad de los sistemas informáticos[4]. Algunos de los artículos más relevantes para este estudio son los siguientes:

1. Artículo 269A: Este artículo penaliza la interceptación ilegal de datos informáticos.
2. Artículo 269B: Se refiere a la manipulación de datos informáticos y establece sanciones para quienes lo lleven a cabo.
3. Artículo 269C: Penaliza la introducción de virus informáticos y otros programas maliciosos.
4. Artículo 269D: Establece sanciones para el acceso abusivo a un sistema informático ajeno.

[4] Ley 1273 de 2009 - Gestor Normativo. (2009). Gov.co.

5. Artículo 269E: Penaliza la obstrucción al funcionamiento de un sistema informático.
6. Artículo 269F: Establece sanciones para la utilización de software malicioso.

Estos artículos proporcionan un marco legal en Colombia para la persecución y sanción de actividades relacionadas con ransomware y otros ataques informáticos.

La normativa internacional ISO 27001, definida como "el estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI)" (GlobalSuite Solutions, 2023), destaca la necesidad de que las organizaciones aseguren la protección contra software malicioso, dado el riesgo inherente que los sistemas de información enfrentan. Este tipo de amenazas puede materializarse en formas que van desde el robo y daño de información hasta la destrucción de datos o la inutilización de sistemas.

Con el objetivo de mitigar estos riesgos, la norma ISO 27001 establece la obligación de implementar controles efectivos para la protección, detección y recuperación en casos de incidencias de seguridad[5]. Subraya la importancia de combinar métodos técnicos avanzados, como el uso de sandbox y otros programas especializados en el análisis de malware, con campañas de concientización dirigidas a los usuarios que interactúan con los sistemas. Esta combinación estratégica busca abordar tanto las vulnerabilidades técnicas como los aspectos Que recaen en las personas que hacen uso de las herramientas tecnológicas.

[5] GlobalSuite Solutions. (2023, March 20). ¿Qué es la norma ISO 27001 y para qué sirve?

7.3 Marco Teórico-Conceptual

7.3.1 Malware

El término "malware" proviene de la combinación de las palabras en inglés "malicious" y "software", lo que se traduce como "software malicioso". Este hace referencia a programas diseñados con la intención de llevar a cabo diversas acciones perjudiciales en el sistema en el que se ejecutan. Estas acciones suelen incluir el bloqueo del uso de la computadora víctima, la encriptación de información, el daño a archivos o programas, la generación de tráfico para causar perjuicio en la red mediante ataques de denegación de servicio, la propagación a través de la red infectando más computadoras, y la afectación de componentes de hardware como los discos, entre otras acciones según el propósito para el cual esté diseñado el programa (Avast, 2023).

El desarrollo de este tipo de programas ha experimentado un aumento significativo a medida que el uso de computadoras se ha generalizado y se ha expandido el acceso a internet. Esto ha convertido a la red en un medio propicio para la distribución de malware, permitiendo llegar a un mayor número de posibles afectados y generando beneficios para los perpetradores, como el robo de datos personales y financieros.

Algunos tipos de malware son:

- Ransomware: En un ataque de ransomware, el software malicioso bloquea el acceso a la máquina o encripta la información almacenada en la computadora de la víctima, exigiendo un pago, conocido como "rescate", para restaurar el acceso o descifrar los datos (“Los 6 tipos de malware”, 2022).

- Gusanos informáticos: Los gusanos informáticos son un tipo de software que tiene la capacidad de propagarse por sí mismo a través de múltiples computadoras

sin requerir interacción del usuario para su funcionamiento (*¿Qué es el malware?*, 2020).

- Troyanos: Los troyanos son programas maliciosos que se camuflan como aplicaciones benignas, pero, una vez instalados, realizan diversas funciones dañinas en la computadora, como el robo de datos o el espionaje de actividades ("Los 6 tipos de malware", 2022).

- Spyware: El spyware es un tipo de software que monitorea las actividades del usuario y recopila información, como actividades de navegación, contraseñas y datos financieros, así como otra información personal sensible (*What is malware?*, s/f).

- Malware sin archivo: El malware sin archivo es una variedad de malware que no deja rastro de su instalación, lo que dificulta su detección. Puede permanecer en la computadora indefinidamente y robar información sensible basándose en las acciones del usuario (*What is malware?*, s/f).

- Adware: El adware son programas que generalmente se instalan junto con aplicaciones gratuitas y muestran anuncios no deseados de manera constante (*¿Qué es el malware?*, 2020). Además, recopilan información sobre las actividades de navegación del usuario.

Frente a la diversidad de tipos de malware y la necesidad de contrarrestar sus efectos, se cuenta con programas diseñados para detectar y prevenir sus acciones. Entre los primeros productos desarrollados con este propósito se encuentran los antivirus. Aunque estos programas son eficaces, pueden tener un porcentaje de falla en la detección dado a la capacidad que tienen los programas de malware para no ser detectados conocido como el polimorfismo y metamorfismo, además del malware de día cero.

En relación con los mecanismos de detección de malware, se pueden mencionar los siguientes sacados del trabajo de Vinod & V. Laxmi[6]:

- Detección basándose en firmas, Este método implica identificar el malware a través de un conjunto de binarios reconocidos en su código. Aunque es preciso para detectar malware básico, su eficacia disminuye frente a variantes polimórficas y metamórficas, que tienen la capacidad de cambiar y modificar sus funciones.
- Detección basada en especificaciones, En este enfoque, el programa pasa por una fase de entrenamiento donde aprende el comportamiento de software posiblemente dañino. Examina los programas en busca de comportamientos indicativos de malware. Sin embargo, esta técnica puede ser limitada dado las especificaciones con que se entrene.
- Detección basada en el comportamiento, Este tipo de detección resulta más efectivo para malware que muta su código, ya que las acciones que realiza tienden a ser consistentes. Para llevar a cabo el análisis, se requiere recopilar datos estáticos y dinámicos del comportamiento del programa, interpretar el análisis y

[6] Vinod, P., & V. Laxmi, M. S. G. (2009). Survey on Malware Detection Methods.

compararlo con la firma del comportamiento para determinar si el código es malicioso.

7.3.2 Análisis Estático y Dinámico de Malware

El análisis estático y dinámico de malware constituye una actividad esencial en la investigación y comprensión de los procesos generados por software malicioso. Su objetivo principal es proporcionar respuestas a tres preguntas clave:

1. ¿Cómo opera el malware?
2. ¿Cómo puedo detectarlo?
3. ¿Cuál es la mejor manera de eliminar la amenaza generada?

El Dr. Ali Hadi[7] destaca la importancia de enfocarse en procesos específicos que contribuyan a abordar estas preguntas fundamentales. Este enfoque selectivo evita la pérdida de tiempo en el análisis de procesos no relevantes para la identificación de los aspectos críticos del código malicioso. Asimismo, subraya la necesidad de implementar únicamente los métodos de análisis necesarios, evitando el abordaje indiscriminado de todos los posibles enfoques. Esta estrategia garantiza una investigación eficiente y precisa para comprender, detectar y eliminar las amenazas de manera efectiva.

El análisis estático implica el estudio del software sin ejecutarlo. Este enfoque se lleva a cabo mediante la revisión de la estructura del archivo y las funciones utilizadas. En un nivel más avanzado, se puede profundizar examinando detalladamente las funciones a bajo nivel, descomponiendo el archivo en sus partes más importantes utilizando la ingeniería inversa (Hadi, n.d.).

[7] Hadi, A. Understanding malware analysis with Dr. Ali Hadi. INE, Inc.

En el contexto del trabajo realizado por Sikorski & Honig[8], se describen diversas técnicas para extraer información mediante el análisis estático básico:

- Identificación del formato del archivo. Analizar el formato del archivo proporciona información preliminar sobre las posibles acciones que el programa puede llevar a cabo. Por ejemplo, en sistemas Windows, los archivos PE (Portable Executable), DLL, entre otros.

- Escaneo de archivos con programas antivirus. Realizar un escaneo de archivos utilizando diferentes programas antivirus permite comprender cómo estos detectan posibles amenazas. Es importante destacar que esta técnica tiene limitaciones, ya que los antivirus pueden no detectar malware de día cero, es decir, código malicioso nuevo que aún no ha sido identificado ni investigado.

    - Uso de hashing. Emplear funciones criptográficas de hashing, transforma un bloque de datos en una serie fija única de caracteres (Donohue, 2014). En los archivos los más usados son el MD5 y sha-1. Cuando se identifica el hash de un archivo este después puede ser usado para verificarlo en programas como VirusTotal o en internet para saber si ha sido detectado anteriormente como malicioso.

- Análisis de 'strings' o cadenas de texto. La identificación de cadenas de texto dentro del código revela funciones y otra información relevante. Por ejemplo, en programas para Windows, ciertas funciones típicas de este sistema operativo pueden ser detectadas

[8] Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The hands-on guide to dissecting malicious software.

fácilmente. También se puede observar la presencia de DLL (Dynamic Link Library), que contienen código ejecutable.

- Detección de técnicas de ofuscación. La ofuscación del código consiste en ocultar partes del mismo para dificultar su acceso. Identificar la presencia de ofuscación se puede lograr al notar la escasez de 'strings', que deberían estar más presentes en el código.

- Análisis de librerías y funciones vinculadas. Examinar las funciones externas llamadas por el código revela la posible reutilización de código por parte de los programadores.

- Exploración de funciones importadas o exportadas. Los programas pueden utilizar funciones importadas o, en ocasiones, exportar funciones para el intercambio de información.

Por otro lado, el análisis dinámico implica examinar el software durante su ejecución. Este proceso se lleva a cabo creando un entorno controlado y monitoreando las acciones realizadas a través de diversas herramientas de seguimiento. En un nivel más avanzado, se puede emplear un depurador para tener un mayor control sobre la ejecución del código (Hadi, n.d.).

Además, también se puede tener un enfoque híbrido compuesto por el análisis dinámico y estático, en el que se ejecuta el software para observar su comportamiento en tiempo real para luego complementar esto con el análisis estático del código para identificar y examinar las partes más relevantes que se encontraron durante la ejecución. La combinación de estos enfoques mejora la capacidad para descubrir y entender la complejidad del malware, así como para desarrollar respuestas y contramedidas más efectivas.

7.3.3 Ransomware

El ransomware, como se explicó anteriormente, es un tipo de malware cuyo propósito principal es bloquear o cifrar los datos de las computadoras que se afectan, impidiendo que se pueda acceder a la información. Posteriormente, los perpetradores exigen un rescate a cambio de la liberación de los datos. Se pueden identificar dos variantes principales de ransomware: el ransomware de bloqueo y el ransomware de cifrado. La distinción entre ambos radica en que el primero se enfoca en obstruir las funciones operativas de la computadora, mientras que el segundo se especializa en cifrar los datos almacenados en la misma. El ransomware de cifrado es la modalidad más prevalente entre los ciberdelincuentes.

El ransomware se ha convertido en una herramienta predilecta para llevar a cabo ataques contra organizaciones. Su crecimiento exponencial ha generado un nuevo mercado en donde empresas desarrollan y comercializan su propio software malicioso, ofreciéndolo a terceros que no necesariamente tienen conocimiento del desarrollo y uso de este software y paga que este sea usado a beneficio de sí mismo. Esta tendencia ha dado lugar a lo que se conoce como Ransomware como Servicio (RaaS). Un ejemplo destacado de esta modalidad es el grupo REvil, que afirmó contar con 60 miembros afiliados entre 2020 y 2021, responsables de la distribución del ransomware (Barbosa, n.d.). La existencia de este mercado negro no solo amplifica la escala de los ataques, sino que también dificulta la identificación y persecución de los perpetradores.

En el trabajo de Kok et al.[9] describen el ciclo de vida del ransomware de la siguiente forma:

1. Creación, En esta fase, se lleva a cabo el desarrollo y perfeccionamiento del código del ransomware. Se busca hacerlo robusto y capaz de ejecutar las acciones planeadas de manera

[9] Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (n.d.). Ransomware, threat and detection techniques: A review.

efectiva. La creatividad y la sofisticación en esta etapa son fundamentales para evadir las defensas de seguridad.

2. Campaña, La distribución del código malicioso tiene lugar en esta etapa, apuntando a víctimas que pueden ser individuos o instituciones. Las técnicas de ingeniería social, como correos de phishing con enlaces maliciosos o archivos infectados, son comúnmente empleadas para alcanzar a los objetivos seleccionados.

3. Infección, Una vez que el malware ha llegado al sistema de la víctima, se ejecuta el payload, permitiendo la instalación del ransomware en el ordenador. Esta fase marca el inicio de la amenaza y su capacidad para llevar a cabo acciones maliciosas.

4. Comando y Control, Después de la infección, el ransomware busca un servidor de comando y control para obtener la clave de cifrado. Este paso es crucial para que el atacante pueda mantener el control sobre el proceso de cifrado y extorsión.

5. Búsqueda, Con la clave de cifrado en su poder, el software malicioso realiza un barrido en busca de archivos críticos, como documentos, backups, contraseñas y bases de datos. El objetivo es identificar los datos más sensibles y valiosos para el usuario o la organización afectada.

6. Cifrado, Una vez que se han identificado los archivos importantes, el ransomware inicia el proceso de cifrado. Este puede adoptar diferentes formas, como cifrado simétrico, asimétrico o híbrido, según la estrategia utilizada por los desarrolladores del malware.

7. Extorsión, Con el cifrado completo, el ransomware despliega un mensaje de rescate, detallando el monto del rescate, los pasos para el pago y el plazo establecido. Este mensaje conlleva la amenaza de eliminar los archivos o divulgar datos confidenciales en línea en caso de no cumplir con las demandas del atacante.

En cuanto a los métodos de pago, los atacantes suelen preferir el anonimato, solicitando rescates en bitcoin debido a su dificultad de rastreo. Además, se utilizan métodos como el envío de mensajes de texto, así como opciones no rastreables, como tarjetas de regalo, PayPal, Ukash cards, MoneyPak, entre otros.

Después de la instalación del payload en el ordenador, Kok et al.[10] Destaca las siguientes funciones que realiza el ransomware lleva a cabo para maximizar su efectividad y dificultar la detección:

- Comprobación de persistencia, El ransomware verifica la persistencia de su presencia en el sistema, asegurándose de que, incluso después de un reinicio del ordenador, el ataque no sea detenido. Esto se logra a menudo mediante la implementación de un ejecutable que se ejecuta como una tarea programada, garantizando la continuidad del malware en el sistema.
- Restricción de la restauración, Con el objetivo de prevenir la restauración del sistema a un estado anterior al ataque, el ransomware puede restringir o deshabilitar las funciones de restauración del sistema.
- Modo sigilo, El ransomware activa el modo sigilo para evitar que la intrusión sea identificada mientras se llevan a cabo las acciones previas al cifrado.
- Mapeo del entorno, Con el fin de adaptarse al entorno específico en el que se está ejecutando, el ransomware realiza un mapeo del ambiente. Este proceso le permite al

[10] Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (n.d.). Ransomware, threat and detection techniques: A review.

malware detectar si está operando en una máquina víctima legítima o en un entorno de pruebas, como un sandbox.

- Enmascaramiento de la comunicación, Para lograr comunicarse con el servidor de comando y control, el ransomware emplea técnicas de enmascaramiento, cifrando o camuflando las comunicaciones para evitar ser detectado por sistemas de seguridad.
- Elevación de privilegios, para aumentar el impacto y alcance en el sistema, el ransomware busca obtener privilegios de administrador con el fin de ejecutar acciones más intrusivas y flograr tener un mayor control sobre el sistema comprometido.

Por otra parte, el ransomware se clasifica principalmente en ransomware de cifrado y de bloqueo. En otras investigaciones, también se hace referencia al ransomware de leakware y de dispositivos móviles. Estos tipos se definen de la siguiente manera:

- Ransomware de cifrado: es el tipo más común de ransomware, en el cual el software cifra todos los archivos o los más importantes que encuentra. Posteriormente, bloquea el acceso a ellos y muestra un mensaje solicitando el rescate (Kaspersky, 2023a).
- Ransomware de bloqueo: en este tipo, se bloquean las funciones principales de los equipos, principalmente a nivel de sistema operativo. En ocasiones, al iniciar el computador, aparece un mensaje solicitando el rescate. Una ventaja de este ransomware es que, en algunas ocasiones, los datos no corren peligro de ser robados (Kaspersky, 2023).
- Leakware / Doxware: en este tipo de ransomware, el software roba la información de la víctima sin necesidad de cifrarla o bloquear el acceso. Luego, chantajea a la víctima con publicar esta información (Anghel & Racautanu, n.d.).

- Ransomware móvil: este ransomware está diseñado específicamente para dispositivos móviles. Normalmente, no cifra la información, ya que los celulares suelen contar con respaldo en la nube, lo que facilita la recuperación de los datos. En cambio, bloquea funciones del dispositivo móvil y busca escalar privilegios (Anghel & Racautanu, n.d.).
- Ransomware de borrado de datos: en este tipo, los atacantes borran la información y luego solicitan un rescate. En algunas ocasiones, no se pide rescate, ya que el objetivo principal es causar daño a la operatividad de la organización víctima, que suele ser de nivel estatal (IBM, n.d.).

7.3.3.1 Familias de Ransomware

El ransomware se clasifica en "familias", que son conjuntos de programas maliciosos que comparten similitudes en su funcionamiento o en su código. Dado el crecimiento del ransomware, para el 2022 se habían identificado 192 familias (González, 2022). En la siguiente tabla, se detallan las características más relevantes de 5 de las familias de ransomware más activas en los últimos años:

Descripción de 5 familias de Ransomware

FAMILIA	*ESTRATEGIA DE PROPAGACIÓN*	*FECHA DE APARICIÓN*	*METODO DE CIFRADO*
Wannacry	Vulnerabilidad Samba Exploit EternalBlue	2017	RSA AES
GandCrab	Correos electrónicos de phishing. Explotación de vulnerabilidades Sitios web comprometidos.	2018	RSA TEA
LockBit	Correos electrónicos de phishing Explotación de vulnerabilidades Acceso remoto a escritorio (RDP)	2019	AES
Clop	Explotación de vulnerabilidades	2019	AES

Alphv BlackCat	Correos de phishing. Explotación de vulnerabilidades. Explotación de credenciales débiles.	2022	AES ChaCha20

Tabla 1. Familias de ransomware.

7.3.3.1.1 Wannacry

Como se ha mencionado anteriormente, Wannacry es un ransomware de cifrado que se volvió reconocido debido al ataque masivo que realizó en el 2017 en el cual los atacantes aprovecharon la vulnerabilidad de SMBv1 (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

, (Microsoft, 2023a)) afectando sistemas como Windows Server 2008, Windows 7, Vista y XP. Los ataques se reliazaron principalmente con el uso del exploit EternalBlue, difundido por el grupo The Shadow Brokers, para obtener acceso remoto a los equipos y cifrar sus datos, exigiendo luego rescates que causaron pérdidas millonarias en numerosas organizaciones a nivel mundial.

Antes de este ataque masivo, Microsoft lanzó el parche de seguridad MS17-010 para proteger los sistemas de esta vulnerabilidad. Sin embargo, debido a la falta de atención en la importancia de la actualización de los sistemas, los atacantes pudieron aprovechar la vulnerabilidad.

Wannacry utiliza el protocolo SMBv1 (Server Message Block), empleado para la comunicación cliente-servidor en la conexión a impresoras, compartir archivos y otros recursos de red (IBM Documentation, 2023). Este ransomware se comporta como un gusano, propagándose a través de la red en busca de sistemas vulnerables, y luego utiliza el backdoor DoublePulsar para instalarse y ejecutarse en los equipos afectados (Latto, 2020).

7.3.3.1.2 GrandCrab

GrandCrab, fue un ransomware que comenzó a propagarse en 2018, fue uno de los pioneros en ofrecer su software a través del modelo de RaaS (Ransomware as a Service) en la dark web. Este malware realizó ataques a organizaciones en América Latina, especialmente en países como Perú 45.2%, México 38%, Ecuador 17.2%, Colombia 9.9% y Brasil 8.7% (Amaya, 2018). En 2019 los creadores anunciaron que el proyecto no iba a seguir siendo ofertado.

Los desarrolladores lanzaron varias versiones de GrandCrab debido a las deficiencias encontradas en las primeras. Por ejemplo, en los primeros ataques, la clave de descifrado se dejaba en un archivo en el sistema comprometido, pero esta táctica fue modificada y protegida en las siguientes versiones para evitar que las víctimas pudieran descifrar sus datos sin pagar el rescate.

Este ransomware utilizaba diversas tácticas de propagación, como campañas de phishing con mensajes diseñados con ingeniería social para persuadir a las personas a descargar archivos adjuntos (Mash, 2019), además de aprovechar exploits para explotar vulnerabilidades en los sistemas informáticos. Una vez que el ransomware se instalaba en el sistema, se alojaba en la carpeta %appdata% e inyectaba el comando nslookup.exe para comunicarse con el C&C (Command and Control) y llevar a cabo el proceso de cifrado en la máquina de la víctima (Espitia, 2019) Posteriormente, los perpetradores solicitaban los pagos de rescate para ser depositados en la billetera DASH

7.3.3.1.3 Lockbit.

Es un ransomare de cifrado que emplea un método de doble extorsión: además de cifrar los datos y exigir un rescate, amenaza con hacer pública la información en caso de no recibir el pago. Este software se ofrece bajo la modalidad de Ransomware como Servicio (RaaS).

En un principio lockbit fue reconocido como ransomware ABCD debido a que esa era la extensión que tenían los archivos después de ser cifrados, en las versiones más recientes los archivos se cifran con la extensión ".lockbit" haciendo que ahora sea reconocido con este nombre (Sanjana, 2024). Los primeros ataques se registraron en 2019, principalmente dirigidos a empresas gubernamentales en países como Estados Unidos, China, India, Indonesia y Ucrania (Kaspersky, 2023b). Aunque los objetivos principales han sido equipos con sistema operativo Windows, también se han reportado variantes que afectan servidores ESXi y el sistema operativo MacOS (Sanjana, 2024).

De manera general, los ataques de lockbit se pueden clasificar en 3 etapas (Kaspersky, 2023b). En la primera etapa de explotación, el ransomware ingresa sin autorización a través de diversas vías, como la explotación de vulnerabilidades, ataques de fuerza bruta o campañas de phishing. Luego, en la etapa de infiltración, utiliza herramientas de pos-explotación para elevar privilegios, moverse lateralmente en la red y desactivar programas de seguridad antes de cifrar los archivos. Finalmente, en la etapa de implementación, el software procede a cifrar los archivos y propagarse a otras máquinas disponibles.

Actualmente, en el tiempo en que se realizó este trabajo, en febrero de 2024 por medio de la operación internacional denominada operación Cronos se realizó el desmantelamiento de la banda criminal donde se arrestaron dos integrantes del grupo de personas vinculadas al ransomware y además fueron intervenidos 34 servidores con los que estos trabajaban (Marquez, 2024).

7.3.3.1.4 Clop

Es un ransomare de cifrado que al igual que lockbit, emplea un método de doble extorsión. Utiliza diversas técnicas para llevar a cabo ataques masivos, entre las que destaca la

explotación de la vulnerabilidad CVE-2023-34362 mediante inyección SQL en la aplicación de transferencia de archivos MOVEit. Durante este incidente, los atacantes desplegaron un Shell web denominado LEMURLOOT para asegurar la persistencia en los servidores web de la víctima y llevar a cabo el ataque (Akamai Security Intelligence Group, 2023).

Otro caso destacado relacionado con este grupo de ransomware ocurrió en 2023, cuando explotaron la vulnerabilidad CVE-2023-0669 del software de transferencia de archivos GoAnywhere MFT mediante una inyección de comandos de autenticación en el License Response Servlet. La vulnerabilidad afectaba a la consola de administración, en donde se identificaron 267 hosts con indicadores de vulnerabilidad. La empresa implementó un parche de seguridad en la versión 7.1.2 para abordar esta vulnerabilidad (Motheram, 2023).

7.3.3.1.5 Alphv BlackCat

El ransomware BlackCat, que opera como RaaS y está programado en el lenguaje Rust, emplea un método de triple extorsión, en donde, además de cifrar los datos y amenazar con su publicación en la red si no se realiza el pago, ejerce presión adicional amenazando con ataques de denegación de servicio (DDoS) para inutilizar los servidores (Valenzuela, 2023).

Las investigaciones sobre este ransomware han revelado que surgió en 2020 bajo el nombre de DarkSide, el cual fue desarticulado tras el ataque al oleoducto Colonial Pipeline. Posteriormente, en 2021, resurgió como BLack-matter, pero a finales del mismo año terminó sus operaciones bajo dicho nombre y en el año 2022, resurgió nuevamente como BlackCat (Vazquez & Gonzalez, 2022). El grupo detrás de este servicio no utiliza un método de propagación único y no se dirige específicamente a un tipo de empresa, habiéndose registrado ataques a múltiples organizaciones, principalmente de alto perfil (HackWise, 2022) lo que lo convierte en un objetivo vigilado de cerca por agencias internacionales.

El ransomware cuenta con diversos métodos de propagación, entre los que se incluye la infiltración mediante el compromiso de credenciales de usuario o a través de campañas de phishing. Una vez dentro del sistema, el ransomware busca comprometer el Active Directory y las cuentas de administrador, utilizando el programador de tareas de Windows para asegurar su persistencia en la red (Vazquez & Gonzalez, 2022). Además, emplea scripts de PowerShell junto con Cobalt Strike para eludir los programas de seguridad. Posteriormente, procede a la exfiltración de los datos y finalmente los cifra utilizando el algoritmo AES.

7.3.4 Herramientas Usadas Para el Análisis de Malware

En este apartado se va a realizar la descripción de las herramientas usadas para la investigación de malware en este trabajo.

7.3.4.1 Sandbox

En términos generales, un sandbox es un entorno de pruebas diseñado para ejecutar programas de manera aislada y controlada (Coppola, 2021). Su utilidad se extiende a diversas finalidades dentro de una organización. Algunos de los usos más comunes incluyen: el desarrollo de software para identificar posibles errores en el código y validar su funcionamiento; análisis de archivos y programas para la investigación de posible malware en estos; investigación en la seguridad de las redes ante posibles ataques; entornos de entrenamiento y simulación ante posibles amenazas de software malicioso (Coppola, 2021).

Los desarrolladores de malware modernos implementan técnicas de evasión conocidas como "métodos antisandbox" o "antisandboxing", para evitar la detección cuando el malware se está ejecutando en un entorno de prueba o en una máquina virtual (“¿Qué es una sandbox?”

2022). Estos métodos están diseñados para identificar señales o comportamientos específicos asociados con los entornos de prueba y, en consecuencia, ocultar o modificar el comportamiento del malware para eludir la detección.

Algunas de las estrategias comunes utilizadas por el malware para evadir la detección en entornos pueden ser la comprobación del entorno comprobando características de hardware, configuraciones o características de red comunes de ambientes de pruebas, también pueden detectar herramientas típicas usadas para el análisis de software y demás.

En el trabajo de Yoshioka et al., 2009[11] se describen tres criterios principales que debe cumplir un sandbox para ejecutar las pruebas:

- Observabilidad, capacidad del sandbox para proporcionar una observación detallada de las acciones realizadas por el malware como el monitoreo de diversas capas, como el sistema operativo, llamadas a API, ejecuciones en la red y otras acciones relevantes. Esta información ayuda en la creación de firmas en sistemas de detección, como IDS/IPS o antivirus.
- Seguridad, Dada la naturaleza del sandbox para ejecutar software potencialmente riesgoso, la seguridad del entorno es de suma importancia. Se deben implementar medidas de seguridad para proteger la red principal contra posibles infiltraciones del malware. Además, es también importante equilibrar la autenticidad del entorno de prueba con la protección de la red, ya que, como se había descrito anteriormente, el malware es capaz de detectar entornos completamente aislados y no ejecutar su código real en estas circunstancias.
- Eficiencia, La eficiencia es una de las principales ventajas de un sandbox, ya que permite la ejecución automática del software y el análisis de su comportamiento en un tiempo

[11] Yoshioka, K., Hosobuchi, Y., Orii, T., & Matsumoto, T. (2010). Vulnerability in Public Malware Sandbox Analysis Systems.

significativamente más corto en comparación con el análisis manual. Además, que este también es capaz de adaptarse a entornos de amenazas en constante evolución, permitiendo una detección y respuesta más ágiles.

8. Metodología

En este trabajo, se llevó a cabo una investigación que siguió dos metodologías clave: la revisión bibliográfica para analizar el estado del arte y la investigación de estudio de caso centrada en el análisis del ransomware WannaCry.

Para abordar el análisis del estado del arte, se llevó a cabo una investigación de la literatura actual relacionada con los temas fundamentales de este trabajo. Se exploraron trabajos que cubren la historia de malware, con un enfoque detallado en el ransomware. Además, se examinaron las herramientas utilizadas en otros estudios para el análisis de malware. Este análisis incluyó una revisión detallada de cómo se ha abordado el análisis de malware en casos anteriores.

En relación al estudio de caso del ransomware WannaCry, se ha realizado el análisis basado en el informe generado por un dispositivo sandbox en el cual, se ejecutaron reglas Yara para llevar a cabo el análisis estático del código. Posteriormente, se procedió con el análisis dinámico en una máquina virtual dentro del mismo sandbox.

Al final de este análisis, se tiene como objetivo obtener una plantilla que funcione como guía para resaltar e identificar las partes más relevantes de un código de ransomware y sus características cuando se ejecuta en un entorno controlado. La intención es utilizar esta plantilla como base para la generación de un informe técnico, el cual permitirá comunicar de manera clara y accesible la información derivada de este análisis del ransomware.

8.1 Analisis del Reporte de un Sandbox

En el reporte descargado del análisis realizado en el sandbox (Anexo A), se identifican las diferentes actividades que realiza el ransomware al momento de infectar la máquina virtual en la que se ejecutan las acciones. A continuación, se presenta la información de este mismo:

1. El sandbox empieza ejecutando las reglas Yara FE_RANSOMWARE la cual busca patrones relacionados a Wannacry en los archivos PE tales como los mensajes de rescate, nombres de archivos, comandos que se ejecutan y URLs.

   En la página 2 del Anexo A, se evidencia que en el análisis estático se identifican variables relacionadas con Wannacry. Se obtienen las siguientes alertas:

   - Malware.Binary, la cual hace referencia a que después de analizar los archivos en su contenido binario, se identificó como malicioso
   - Trojan.Artemis Esto hace referencia a que a nivel general se encontró un archivo que presenta comportamientos a los de un troyano, pero no se puede identificar claramente su funcionamiento
   - InfectionFail.KillSwitch Esto hace referencia a una funcionalidad del malware Wannacry con el cual se identifica si puede ejecutarse en el entorno actual o no, en donde en este caso no se logró ejecutar por lo cual puede ser una falla o variante en el código.

2. Posteriormente, comienza a realizar la ejecución del código en la máquina virtual Windows XP en la que se identifica lo siguiente:

   - PEData High Entropy: esto hace referencia a que el archivo tiene un alto nivel de entropía, es decir, puede contener código que no se identifica como técnicas de ofuscación que son conocidas por ser usada comúnmente en el malware.

- PEData Obfuscation: después de analizar los archivos PE encuentra código de ofuscación.
- PEData known compiler: se detecta que los archivos PE están compilados por un compilador conocido por el sistema.
- Process root for executable binaries: Despues de esto se detecta la ejecución de los archivos PE a nivel root
- Process Query Registry: El malware intenta acceder al registro del sistema, el cual es una base de datos de los archivos Windows donde se encuentra información de los archivos, configuración del sistema, usuarios y demás
- Despues, en la pagina 6 se identifica que se realizan cambios a nivel del registro del sistema, creando y ocultando un archivo en el directorio caché del usuario S-1-5-21-1409082233-688789844-725345543-1003 normalmente usado para guardar temporalmente archivos de internet.
- Entre las páginas 6 a 11, se detecta que el malware corre la función de la API de Windows GetComputerNameW para obtener información de la maquina en la que se está ejecutando.
- Pag 12; se detecta que se realiza el query a la página www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com el cual es un kill switch del malware (Berry et al., 2017), si logra ingresar a la página deja de ejecutar el código, y si falla continua con la ejecución
- Pag 13; el malware comienza a ejecutar cambios a nivel del registro del sistema para lograr persistencia en el servicio del Centro de Seguridad de Microsoft que está asociado con el ejecutable mssecsvc.exe

- Después, el malware busca tener persistencia en el ‘Programador de Tareas’ asociado al ejecutable tasksche.exe con la creación del archivo en una ruta aleatoria que este genera C:\Intel\wfgkyoarrgrrwwo 604\tasksche.exe
- Pag 15 – 24, el malware crea un hilo de tareas en el cual va a comenzar a generar IPs aleatorias dentro de la subred a las cuales va a seguir intentando conectarse durante toda la ejecución del programa. Además, crea un hilo diferente con redes aleatorias a las cuales intentará conectarse. Dado si logra alcanzar alguna conexión a una de las IPs, realiza la explotación de la vulnerabilidad.
- Pag 26 - 27; Regkey Service created in a non-standard manner: se identifica que se genera un nuevo servicio llamando a la función de Windows CreateServiceA la cual “Crea un objeto de servicio y lo agrega a la base de datos del Administrador de control de servicios especificada” (Microsoft, 2023c) creando el servicio "wfgkyoarrgrrwwo604" el cual lo configura para ejecutar el archivo "tasksche.exe" por medio del comando "cmd.exe /c"
- Pag 30; se crea el archivo b.wnry de hash c17170262312f3be7027bc2ca825bf0c en la ruta "C:\Intel\wfgkyoarrgrrwwo604" el cual es la imagen de rescate (BMP)
- Pag 30; se crea el archivo "c.wnry" de hash ae08f79a0d800b82fcbe1b43cdbdbefc en la ruta "C:\Intel\wfgkyoarrgrrwwo604" el cual es el archivo de configuración que contiene la dirección de los servidores C2, las carteras de bitcoin, etc.
- Pag 31; Después, se crea el folder "C:\Intel\wfgkyoarrgrrwwo604\msg" el cual es el directorio en el que se guardan los archivos con el mensaje de rescate en 28 idiomas diferentes.

- Después en el directorio C:\Intel\wfgkyoarrgrrwwo604\msg comienza a crear los archivos que contienen el mensaje de rescate en diferentes idiomas, en este caso se crearon los siguientes:

Nombre del archivo	Hash
m_bulgarian.wnry	95673b0f968c0f55b32204361940d184
m_chinese (simplified).wnry	0252d45ca21c8e43c9742285c48e91ad
m_chinese (traditional).wnry	2efc3690d67cd073a9406a25005f7cea
m_croatian.wnry	17194003fa70ce477326ce2f6deeb270
m_czech.wnry	537efeecdfa94cc421e58fd82a58ba9e
m_danish.wnry	2c5a3b81d5c4715b7bea01033367fcb5
m_dutch.wnry	7a8d499407c6a647c03c4471a67eaad7
m_english.wnry	fe68c2dc0d2419b38f44d83f2fcf232e
m_filipino.wnry	08b9e69b57e4c9b966664f8e1c27ab09
m_finnish.wnry	35c2f97eea8819b1caebd23fee732d8f
m_french.wnry	4e57113a6bf6b88fdd32782a4a381274
m_german.wnry	3d59bbb5553fe03a89f817819540f469
m_greek.wnry	fb4e8718fea95bb7479727fde80cb424
m_indonesian.wnry	3788f91c694dfc48e12417ce93356b0f
m_italian.wnry	30a200f78498990095b36f574b6e8690
m_japanese.wnry	b77e1221f7ecd0b5d696cb66cda1609e
m_korean.wnry	6735cb43fe44832b061eeb3f5956b099
m_latvian.wnry	c33afb4ecc04ee1bcc6975bea49abe40
m_norwegian.wnry	ff70cc7c00951084175d12128ce02399

m_polish.wnry	e79d7f2833a9c2e2553c7fe04a1b63f4
m_portuguese.wnry	fa948f7d8dfb21ceddd6794f2d56b44f
m_romanian.wnry	313e0ececd24f4fa1504118a11bc7986
m_russian.wnry	452615db2336d60af7e2057481e4cab5
m_slovak.wnry	c911aba4ab1da6c28cf86338ab2ab6cc
m_spanish.wnry	8d61648d34cba8ae9d1e2a219019add1
m_swedish.wnry	c7a19984eb9f37198652eaf2fd1ee25c
m_turkish.wnry	531ba6b1a5460fc9446946f91cc8c94b
m_vietnamese.wnry	8419be28a0dcec3f55823620922b00fa

Tabla 2. Archivos de Wannacry 1.

- Pag 39; se crea el archivo “r.wnry” de hash 3e0020fc529b1c2a061016dd2469ba96 en el directorio "C:\Intel\wfgkyoarrgrrwwo604" el cual contiene la nota de rescate con las instrucciones de pago.
- Se crea el archivo “s.wnry” de hash ad4c9de7c8c40813f200ba1c2fa33083 el cual contiene el cliente de Tor
- Pag 45; crea el archivo “t.wnry” de hash 5dcaac857e695a65f5c3ef1441a73a8f en el directorio "C:\Intel\wfgkyoarrgrrwwo604" el cual contiene el programa de cifrado
- Después se crear el archivo “taskdl.exe” de hash 4fef5e34143e646dbf9907c4374276f5 en el directorio

"C:\Intel\wfgkyoarrgrrwwo604" el cual elimina todos los archivos temporales en el directorio /temp de cifrado que se generan de extensión WNCRYT

- Después, se crea el archivo taskse.exe de hash 8495400f199ac77853c53b5a3f278f3e en el directorio "C:\Intel\wfgkyoarrgrrwwo604" con el cual se ejecutan los programas de cifrado.
- Después, se crea el archivo “u.wnry” de hash 7bf2b57f2a205768755c07f238fb32cc en el directorio "C:\Intel\wfgkyoarrgrrwwo604" el cual es el programa que descifra el ransomware.
- Después, se hace el llamado al ejecutable de Windows C:\WINDOWS\system32\attrib.exe corriendo el comando attrib +h el cual establece el directorio actual como oculto.
- Pag 51; genera los archivos 0000000.pky, 0000000.eky, 0000000.res y 0000000.dky que son los archivos con la llave de cifrado
- Pag 56; el malware empieza el proceso taskdl.exe para borrar los archivos temporales que se generan. Del cual, como otros estudios han analizado[12] y se visualiza en el reporte del sandbox, este proceso se reinicia constantemente.
- Crea el archivo @WanaDecryptor@.exe de hash 7bf2b57f2a205768755c07f238fb32cc el cual es usado para generar una llave de registro, posteriormente la información de u.wnry es copiada en este archivo con el programa de descifrado.

[12] Berry, A., Homan, J., & Eitzman, R. (2017, May 23). WannaCry malware profile.

- Después se crea el archivo 40921695823978.bat, el cual contiene script que sirve para mover y eliminar archivos. El cual se ejecuta creando el proceso en Windows lanzado por el archivo tasksche.exe utilizando el comando "cmd /c 40921695823978.bat"
- PAG 57; Después crea el archivo @Please_Read_Me@.txt el cual contiene la nota de rescate que proviene del archivo r.wnry
- Pag 60, El ransomware comienza a hacer llamados API repetidos de ‘sleep’, el cual es conocido como un método de evasión para no ser detectado.
- Pag 66, el malware comienza el proceso cscript.exe //nologo m.vbs el cual empieza el script de Visual Basic Scripting (VBS) m.vbs con la opción //nologo para que no sea visible el mensaje de inicio del motor de script.
- Pag 67, el malware comienza a buscar los directorios que existen y además a identificar los archivos de extensiones que puede encriptar, dejando a un lado las extensiones .exe .dll y .wncry
- Pag 68 – 82, se visualiza que el malware está ingresando a carpetas admin y de los usuarios para cifrarlos, los cuales se identifican con la extensión wnry y además copia el timestamp de la creación del archivo para crear las llaves de cifrado y descifrado (Berry et al., 2017). En cada directorio que cifra archivos copia please_read_me y @wanncryptor@.exe
- Pag 80, se crea el archivo @wanaDecryptor@.exe.lnk
- Pag 83; borra los archivos m.vbs y 40921695823978.bat
- Pag 92, comienza a borrar los archivos originales de los que ya fueron cifrados
- Pag 120, comienza a borrar los archivos temporales wncrypt del directorio /temp

- En el resto del reporte, se visualiza que el malware continúa realizando el proceso de cifrado, elimina archivos temporales y sobrescribe los archivos de extensión
- 200 – 209 comienza a correr wmiprvse.exe
- 212 se termina la ejecución del ransomware.

8.2 Estructuración de informes técnicos detallados

El presente trabajo de grado se centrará en la estructuración de la información técnica requerida en un informe técnico de malware, así como en su organización a nivel de contenido.

A nivel general, se tendrán en cuenta los siguientes ítem que relacionan diferentes autores[13] [14], referente a como se debe escribir un reporte técnico:

1. Escribir el informe según el público objetivo. Este ítem hace referencia a que en algunos casos los lectores pueden no tener conocimiento previo de los conceptos técnicos de base de los cuales se estarán hablando, por esto se debe explicar de la forma clara y detallada para lograr la comprensión de este.
2. Establecer objetivos claros. Este ítem hace referencia a tener en cuenta el público objetivo para entregar la información específica que se va a entregar, evitando información que no contribuye al entendimiento del tema central.
3. Recuperación de información. En función de los objetivos establecidos, empezar a recopilar material distinguiendo entre el que es relevante y no es referente a los objetivos. Al momento de revisar el material, se prioriza el que es más relevante para los objetivos.

[13] TheIET. (n.d.). A guide to technical reporting.
[14] Guide to Technical Report Writing : Study guides. (n.d.). Sussex.ac.uk.

4. Escritura. Dado que los informes son textos formales, no necesariamente deben redactarse con palabras muy complejas, por el contrario, se debe intentar explicar de forma sencilla para no distraer al lector teniendo en cuenta las normas gramaticales y puntuación. Además, se debe explicar el lenguaje técnico utilizado o evitar usar estas palabras si es posible.
5. Diagramas. Los cuales pueden ser tablas de contenido, gráficos, fotografías, entre otros. Esto con el fin de representar gráficamente cierto contenido.
6. Finalizar el reporte con una conclusión resumiendo del propósito del informe y cuáles fueron los hallazgos
7. Estructura. Este ítem hace referencia a las secciones y sub-secciones que se especificarán en el informe, las cuales pueden variar según el tipo de informe. Para este trabajo se tendrá en cuenta la siguiente estructura:
    a. Título, fecha y nombres de los interesados
    b. Resumen ejecutivo. Descripción de los objetivos y breve descripción del informe
    c. Tabla de contenido
    d. Introducción. En esta se describe el propósito del informe y a quien va dirigido
    e. Descripción del ransomware, abarcando el funcionamiento del mismo
    f. Impacto en la organización
    g. Acciones que se deben tomar
    h. Recomendaciones para la organización
    i. Conclusiones
    j. Referencias/Bibliografía
    k. Anexos

8.3 Informe tecnico

En este apartado se va a definir los apartados del informe técnico teniendo en cuenta lo mencionado en lo descrito en la sección 10.2 Estructuración de informes técnicos detallados. Además, se presentará el formato de presentación del informe y el ejemplo del informe presentando los detalles del ransomware WannaCry.

8.3.1 Título

El titulo debe representar de forma clara y concisa el tema principal del informe, por lo que se sugiere evitar palabras que se usen para atraer al lector, sino ser claro con el tema

8.3.2 Resumen ejecutivo.

Para este ítem, se tiene en cuenta la descripción del o los objetivos que se van a tratar en el informe, una breve descripción de los resultados y/o hallazgos principales obtenidos, y finalmente la conclusión sintetizando lo anterior.

8.3.3 Tabla de contenido

La tabla de contenido, es la lista de las secciones que se van a presentar en el informe. Para el caso de este informe, se presenta de la siguiente forma:

Resumen

1. Introduccion
2. Descripcion del ransomware
3. Impacto en la organización
4. Acciones que se deben tomar
5. Recomendaciones para la organización

6. Conclusiones
7. Referencias
8. Anexos

8.3.4 Introducción.

En este apartado se realiza la introducción del informe, destacando el objetivo de este, una breve descripción del contenido y de los apartados que se ven a mencionar a continuación.

8.3.5 Descripción del ransomware

En este apartado se realiza la descripción del software, abordando sus aspectos técnicos más relevantes y su funcionamiento. Aunque en la bibliografía revisada no se encontró un marco de referencia específico para este apartado, se utilizará como referencia la información recopilada de varios informes relacionados con informes técnicos de malware presentada a continuación

a. Nombre del malware
b. Tipo de malware
c. Familia de Ransomware
d. Fecha de aparición
e. Dispositivos o Sistemas Operativos afectados
f. Metodo de cifrado
g. Comando y Control (C&C)
h. Vector de ataque
i. Vector de propagación
j. Ficheros generados o usados por el malware

8.3.6 Funcionamiento:

En este apartado se describe cómo funciona el ransomware una vez realiza la explotación de un sistema vulnerable.

8.3.7 Impacto en la organización

En este apartado, se identifica cual sería el impacto (bajo, alto, critico) dado la empresa se viera afectada por un incidente de ciberseguridad relacionado a un ataque de ransomware.

8.3.8 Recomendaciones para la organización

En este apartado se pueden describir las acciones preventivas y correctivas a tomar de manera general para un incidente de ciberseguridad y además detallar de manera particular con respecto al tipo de malware que se esté presentando.

8.3.9 Conclusiones

En este apartado, se describe la conclusión referente a lo presentado anteriormente. El siguiente es el texto ejemplo realizado:

8.3.10 Referencias/Bibliografía

En este apartado se hace referencia a la bibliografía usada en que se tomó la información según sea el caso.

8.3.11 Anexos

En este apartado se hace anexan los archivos relacionados al caso, como por ejemplo el reporte del sandbox.

Para la presentación del informe según la información que se definió que este debe llevar, se propone el siguiente formulario para la presentación de la información:

Información del reporte		
No. Reporte	**Versión**	**Fecha dd/mm/aaaa**
Representante de TI		
Resumen		
Tabla de contenido		
Introducción		
Información del archivo		

Nombre	
Tamaño en KB	**Extensión**
MD5	
SHA1	
SHA256	
Descripción del Ransomware	
Tipo de malware	**Nombre del malware**
Familia de Ransomware	**Fecha de aparición dd/mm/aaaa**
Método de Cifrado	**Comando y Control (C&C)**
Dispositivos o Sistemas Operativos afectados	
Vector de ataque	
Vector de propagación	
Ficheros generados o usados por el malware	

Nombre	**Hash**	**Descripción**

Funcionamiento		
Impacto en la Organización		
Recomendaciones para la organización **Medidas preventivas**		
Medidas correctivas		
Conclusiones		
Referencias		
Representante TI		

Firma
Nombre
Fecha

Tabla 3. Formato del formulario

A continuación, se presentará un ejemplo del informe sobre el ransomware WannaCry utilizando el formato de presentación.

Información del reporte		
No. Reporte **1**	**Versión** 1	**Fecha dd/mm/aaaa** dd/mm/aaaa
Representante de TI		
Resumen		
En respuesta a la posible amenaza en que se encuentra la organización sobre incidentes de ciberseguridad, en el siguiente informe se presenta la información sobre el análisis realizado al ransomware Wannacry. Se realizó el análisis de su funcionamiento, vectores de ataque y las vulnerabilidades (CVE) relacionadas a este. Adicionalmente, se presentan recomendaciones para mejorar la seguridad de la organización para minimizar el riesgo de ser víctima de un ataque por este software, en donde se presentan sugerencias relacionadas a medidas proactivas como la actualización de los sistemas y demás.		

El comprender el funcionamiento del ransomware Wannacry y las mejores prácticas asociadas a la protección ante este software malicioso, permite a la organización estar preparada para mitigar los riesgos asociados y poder enfrentar la situación dado se viera afectado por un incidente de ciberseguridad.

Tabla de contenido

Introducción

En este informe, se describirá el funcionamiento del ransomware Wannacry, que ha tenido un impacto considerable en organizaciones a nivel global, incluyendo empresas en Colombia. Este malware tiene el potencial de provocar pérdidas significativas, por lo que es fundamental contar con la información adecuada para mitigar los riesgos y reducir las posibilidades de sufrir afectaciones. Según lo anterior, el objetivo de este informe es proporcionar información que permita a la organización protegerse de posibles ataques provenientes de este ransomware.

La investigación para este informe se basó en la recopilación de información disponible en Internet sobre el funcionamiento del ransomware, complementada con el análisis del reporte obtenido de un sandbox que ilustra su comportamiento al infectar un dispositivo. Entre los hallazgos más relevantes se destaca la rapidez con la que este software se propaga a través de la red del dispositivo objetivo, lo que subraya la importancia de las etapas de identificación y contención para mitigar los posibles daños y/o perdidas.

Por esto, entre las recomendaciones se encuentra el poder implementar medidas preventivas, como actualizar regularmente el software, mantener copias de seguridad, capacitaciones de personal al respecto de temas de seguridad informática. Además, se sugiere establecer un plan de respuesta a incidentes donde se especifiquen procedimientos para la detección y mitigación de ataques.

En los siguientes apartados, primero se presentará la descripción detallada del ransomware, abordando su funcionamiento y características. Luego, se examinará el posible impacto que este tipo de malware podría tener en la organización en caso de un ataque. Posteriormente, se presentarán las medidas y acciones recomendadas para mitigar los riesgos y proteger la infraestructura de la empresa. Además, se incluirán conclusiones basadas en los hallazgos del análisis. Por último, se proporcionarán las referencias bibliográficas y los anexos pertinentes para complementar la información presentada en el informe.

Información del archivo	
Nombre	
2a1c8a6c-5d48-11ee-a6e4-005056976388.zip	
Tamaño en KB	**Extensión**

11042818	zip

MD5

f645aa2e7577172630cd9bdf4ebceb91

SHA1

c966994c40b3bbfb44a0634365fae91ed34c99a7

SHA256

6c503129a4236a07c2b56a029a5d115b638d5135ce9c467d746dd24a1b0f64f1

Descripción del Ransomware

Tipo de malware	**Nombre del malware**
Ransomware	WannaCry
Familia de Ransomware	**Fecha de aparición dd/mm/aaaa**
WannaCry	2017
Método de Cifrado	**Comando y Control (C&C)**
RSA y AES	Red Tor

Dispositivos o Sistemas Operativos afectados

Windows Server 2008, Windows 7, Windows Vista y Windows XP

Vector de ataque

Explotación de la vulnerabilidad samba SMBv1. Los ataques principalmente se desarrollaron por medio del exploit EternalBlue.

Vector de propagación

Vulnerabilidad de los servidores Windows que no cuentan con el parche de seguridad MS17-010 CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017- 0147, CVE-2017-0148 (Microsoft, 2023ª)

Ficheros generados o usados por el malware

Nombre	**Hash**	**Descripción**
tasksche.exe	84c82835a5d21bbcf75a61706d8ab549	Programador de tareas
@WanaDecryptor@.exe	7bf2b57f2a205768755c07f238fb32cc	software de descifrado.

mssecsvc.exe	db349b97c37d22f5ea1d1841e3c89eb4	servicio del Centro de Seguridad de Microsoft.
r.wnry	3e0020fc529b1c2a061016dd2469ba96	Contiene la nota de rescate con las instrucciones de pago.
s.wnry	ad4c9de7c8c40813f200ba1c2fa33083	Contiene el cliente de Tor
t.wnry	5dcaac857e695a65f5c3ef1441a73a8f	Programa de cifrado
taskdl.exe	4fef5e34143e646dbf9907c4374276f5	Archivo que genera la tarea de Windows que elimina los archivos temporales *.WNCRYT
taskse.exe	8495400f199ac77853c53b5a3f278f3e	Lanza el programa de descifrado
u.wnry	7bf2b57f2a205768755c07f238fb32cc	Programa de descifrado
b.wnry	c17170262312f3be7027bc2ca825bf0c	Imagen del ransomware (BMP)
c.wnry	ae08f79a0d800b82fcbe1b43cdbdbefc	contiene la dirección de los servidores C2, las carteras de bitcoin, etc.
Funcionamiento		

En primer lugar, el malware intenta realizar una consulta a la página www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, la cual actúa como un interruptor de apagado (kill switch) del malware (Berry et al., 2017). Si logra acceder a esta página, detiene la ejecución del código; si falla, continúa con sus acciones.

A continuación, el malware procede a realizar modificaciones en el registro del sistema para asegurar su persistencia, tanto en el servicio del Centro de Seguridad de Microsoft asociado con el ejecutable mssecsvc.exe, como mediante la creación del ejecutable taksche.exe para ganar persistencia en el 'Programador de tareas'.

Posteriormente, el malware genera dos hilos de tareas. En el primero, comienza a generar direcciones IP aleatorias dentro de la subred, mientras que en el segundo hilo, genera IPs aleatorias distintas. Ambos hilos intentan conectarse a estas direcciones IP durante todo el tiempo de ejecución del programa. Si el malware logra establecer conexión con alguna de las direcciones IP, procede a explotar la vulnerabilidad.

A continuación, el software comienza a generar los archivos mencionados en la tabla 3 para iniciar el proceso de cifrado de archivos. También copia los archivos que contienen los mensajes de rescate, el servidor de mando y control (C&C) para conectarse a la red Tor y realizar el pago del rescate, así como el programa de descifrado.

Para llevar a cabo el cifrado de archivos, el malware genera una clave única para cada archivo, que guarda en los archivos 00000000.pky y 00000000.eky. Una vez finalizado el proceso de cifrado, se muestra la siguiente pantalla solicitando el pago por el rescate de los archivos cifrados:

Imagen 1. Mensaje de rescate Wannacry (Berry et al., 2017)

Impacto en la Organización

El impacto en la organización puede ser alto o critico según la cantidad de servicios que se vieran afectados y el tiempo que se tome en recuperar el funcionamiento normal de la empresa.

Recomendaciones para la organización

Medidas preventivas

1. Mantenimiento y actualización de los sistemas: Esto debido a que es esencial contar con los sistemas operativos y software de la organización actualizados para

prevenir ataques por vulnerabilidades conocidas que ya cuenten con protección. Para esto es necesario contar con un plan de procedimientos en el que se establezcan los detalles referentes a esto. Puntualmente para el caso del ransomware wannacry, la vulnerabilidad SMBv1 se encuentra solucionada con el parche de seguridad MS17-010 de Windows.

2. Desarrollo de un plan integral de prevención y respuesta a incidentes de ciberseguridad: Para este punto, se sugiere la elaboración de un plan en el que se detalle las medidas a tomar para prevenir, detectar, responder y recuperarse ante ataques de ransomware. Para esto, adicionalmente es importante identificar los roles y responsabilidades del equipo de respuesta a incidentes.

3. Formación y capacitación de personal: es importante capacitar a las personas que hacen parte de la organización de los riesgos asociados a incidentes de ciberseguridad para que puedan identificar posibles amenazas que principalmente pueden estar relacionadas a correos (phishing) o mensajes de texto con links o archivos que contengan software malicioso.

4. Implementación de soluciones de ciberseguridad avanzadas: esto hace referencia a los dispositivos y software que ayuden a proteger la infraestructura de la organización como firewalls, sistema de detección de intrusos, antivirus, software de filtrado de correos, entre otros.

Medidas correctivas

En caso de un incidente de ransomware WannaCry:

1. Ejecución del plan de prevención y respuesta a incidentes de ciberseguridad: dado la organización se encontrara siendo afectada por un incidente de ransomware es necesario ejecutar el plan de prevención y respuesta a incidentes de ciberseguridad que se debió haber desarrollado con anterioridad.

2. Identificación de buenas prácticas y cosas por mejorar: realizar un análisis del incidente y de cómo fue manejado para identificar qué acciones fueron las más efectivas u cuales se deben mejorar y documentarlo para actualizar el plan construido.

Conclusiones

Dado que WannaCry es un ransomware que fue identificado hace 7 años (en 2017), actualmente existe un parche de seguridad disponible para evitar la explotación de esta vulnerabilidad en los servidores Windows que pueden ser afectados. Sin embargo, considerando que este tipo de software malicioso está en constante evolución, es crucial mantenerse actualizado y estar al tanto de los problemas que han surgido en el pasado. De estos casos, se puede obtener información relevante para abordar vulnerabilidades más recientes, como aquellas que aún no tienen una solución disponible (conocidas como vulnerabilidades de día cero).

Referencias

Representante TI

Firma
Nombre
Fecha

Tabla 4. Ejemplo del informe

9. Resultados y Discusión

En la literatura especializada sobre el malware, se ha observado que inicialmente estos sistemas se desarrollaron como herramientas de prueba en entornos controlados o con el propósito de investigar el funcionamiento del software. Sin embargo, con el tiempo y debido a su gran potencial, se han creado variantes cada vez más especializadas con la intención de causar daños y/o obtener ganancias, principalmente económicas.

Aunque el ransomware no fue inicialmente el tipo de malware más común, su impacto en las actividades de las organizaciones y las posibles ganancias económicas para los perpetradores lo han convertido en una amenaza significativa. Con el paso del tiempo, todas las formas de malware han evolucionado, mejorando sus técnicas de ataque. En el caso del ransomware, se han observado cambios notables en diversos vectores, como por ejemplo, el método de cifrado. Inicialmente, los archivos simplemente eran cifrados, pero en la actualidad existen variantes que eliminan completamente los archivos del servidor atacado.

Otro aspecto relevante es la evolución de las tácticas de extorsión. Anteriormente, los atacantes solicitaban un rescate a cambio de la información cifrada, y una vez realizado el pago, el ataque cesaba. Sin embargo, en muchos casos actuales, se practica la doble extorsión, donde los atacantes amenazan con divulgar la información en una red anónima como Tor, con el fin de ejercer presión sobre la organización atacada para que esta realice el pago. Si esto no se realiza se publica la información ya sea para venderla o solo buscan afectar a la organización implicada.

En el análisis de malware, específicamente del ransomware, se han identificado características clave que se manifiestan al explotar un sistema vulnerable. Por ejemplo, en el caso de WannaCry, que fue el ransomware analizado en este trabajo, se observó su comportamiento en un entorno controlado (sandbox), donde se pudo visualizar cómo logra la persistencia en el

sistema, cómo lleva a cabo el cifrado de archivos y demás para luego exigir el rescate. Este es un ejemplo general de cómo muchos ransomware operan, aunque existen variaciones más específicas en otros casos.

En el análisis del ransomware ejecutado por el sandbox, se identificó la problemática que este contiene un lenguaje técnico el cual requiere que la persona que lea este informe deba saber un profundo conocimiento en el área. Por esto, se realiza un modelo general de la información más relevante del ransomware que puede ser presentada en un informe para una mayor facilidad al momento de entender este tipo de incidentes de ciberseguridad.

10. Análisis de resultados

El malware ha tenido una evolución significativa a medida que se han desarrollado herramientas mas especializadas y que se amplian las redes de comunicación. En un inicio estos se desarrollaron como pruebas para investigaciones hasta llegar a ser el tipo de software que se conoce hoy en día con el cual se busca causar daño a la red en que se introduce para obtener algpun tipo de ganancia o robar información para otros fines.

En este trabajo, se centró principalmente en el malware de tipo ransomware, el cual también ha tenido una evolución significativa, siendo hoy en día de los más usados para atacar organizaciones, causando interrupción en sus actividades comerciales cifrando sus datos para después solicitar un cobro para el rescate de la información.

En cuanto a las técnicas de ataque, se ha observado una mejora constante en la sofisticación del ransomware, especialmente en lo que respecta al método de cifrado. Desde simples cifrados de archivos hasta variantes que eliminan completamente los archivos del servidor afectado.

Además, las tácticas de extorsión han evolucionado hacia la doble extorsión y triple extorsión, donde los atacantes amenazan con divulgar la información cifrada en redes anónimas si no se realiza el pago del rescate y también realizar ataques de DDoS para hacer presión en la organización afectada para que realice el pago del rescate solicitado.

El análisis de malware realizado en este trabajo al ransonware WannaCry a partir del reporte de un sandbox ayudó a identificar características clave sobre su funcionamiento. En el cual se encontraron retos al momento de analizar este reporte dada la forma en que se presenta la información.

Dado esto, se realizó la propuesta de un modelo general en el que se identifican las partes más relevantes del funcionamiento del malware los cuales se presentan en un informe detallado además de otra información relevante para este estudio como medidas preventivas a tomar para minimizar las probabilidades de un ataque de este tipo de ransomware.

11. Conclusiones

Los sandbox son herramientas que ayudan en el análisis de malware, incluyendo el ransomware. Permiten realizar tanto análisis estático como dinámico del malware, lo que proporciona una comprensión de su funcionamiento. Permitiendo identificar los puntos clave que deben abordarse para mejorar la protección relacionada a la ciberseguridad de las organizaciones.

Sin embargo, los informes generados por los sandbox pueden contener información muy técnica y difíciles de entender para aquellos que no están familiarizados con este campo. En este sentido, en este trabajo se llevó a cabo un análisis detallado de un informe de ransomware, con el objetivo de presentar la información técnica de tal forma que sea más fácil de entender.

Durante este proceso, se identificaron las funciones específicas del ransomware y se contrastaron con la información disponible en la literatura. Esto permitió identificar las partes más relevantes del funcionamiento del malware y presentarlas de manera clara y concisa en un informe.

Es importante destacar que, a pesar que se encuentra con facilidad información sobre ransomware y análisis a detalle de estos, se observó una falta de información específicos en la literatura en relación con la creación de informes. Por lo tanto, se recurrió a la información general recopilada y se adaptó según los aspectos que se consideraron más relevantes del ransomware para presentarlo en un informe.

12. Recomendaciones

Para futuras investigaciones, se sugiere ampliar el análisis a otros tipos de ransomware con el fin de identificar variables adicionales que puedan enriquecer el informe final. Este enfoque permitirá una comprensión más completa de las diversas técnicas y tácticas empleadas por el ransomware en la ejecución de los ataques.

Además, se recomienda explorar aspectos específicos relacionados con la elaboración de informes gerenciales centrados en incidentes de ciberseguridad. Dado que la literatura existente sobre este tema es limitada, se abre una oportunidad para investigar y desarrollar un marco conceptual sólido que guíe la generación de informes gerenciales efectivos en respuesta a incidentes de ransomware. Estos informes no solo deben proporcionar una visión detallada del incidente en cuestión, sino también ofrecer recomendaciones estratégicas para mitigar riesgos futuros y fortalecer las medidas de seguridad de la organización.

13. Referencias

Akamai Security Intelligence Group. (2023, June 8). El grupo de ransomware CL0P aprovecha la vulnerabilidad de día cero SQLi de MOVEit (CVE-2023-34362). Akamai.com. https://www.akamai.com/es/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware

Amanda. (2021, December 21). MSN Messenger golpeó el gusano. Krypton Solid. https://kryptonsolid.com/msn-messenger-golpeo-el-gusano/

Amaya, C. G. (2018, August 22). GandCrab: nueva familia de ransomware que crece rápidamente en Latinoamérica. Welivesecurity.com. https://www.welivesecurity.com/la-es/2018/08/22/gandcrab-nueva-familia-ransomware-crece-latinoamerica/

Anghel, M., & Racautanu, A. (n.d.). A note on different types of ransomware attacks. Iacr.org. https://eprint.iacr.org/2019/605.pdf

Avast. (2023, January 19). ¿Qué es el malware y cómo protegerse de los ataques? ¿Qué es el malware y cómo protegerse de los ataques?; Avast. https://www.avast.com/es-es/c-malware

Barbosa, D. C. (n.d.). Ransomware como servicio (RaaS): qué es y cómo funciona este modelo. Welivesecurity.com. https://www.welivesecurity.com/la-es/2022/02/23/ransomware-as-a-service-raas-que-es-como-funciona/

BBC News Mundo. (2015, October 11). El virus que tomó control de mil máquinas y les ordenó autodestruirse. BBC. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Belcic, I. (2020, February 27). Qué es el ransomware CryptoLocker y cómo eliminarlo. Qué es el ransomware CryptoLocker y cómo eliminarlo; Avast. https://www.avast.com/es-es/c-cryptolocker

Berry, A., Homan, J., & Eitzman, R. (2017, May 23). WannaCry malware profile. Mandiant. https://www.mandiant.com/resources/blog/wannacry-malware-profile

Colprensa. (2017, May 15). Ya son 20 empresas colombianas afectadas con virus WannaCry. Elcolombiano.com. https://www.elcolombiano.com/tecnologia/wannacry-afecta-a-20-empresas-colombianas-NF6531294

Coppola, M. (2021, November 18). Sandbox: qué es, para qué sirve y cómo funciona. Hubspot.es. https://blog.hubspot.es/website/que-es-sandbox

de ESET Latinoamérica, L. (2012). Cronología de los virus informáticos: La historia del malware. http://www.eset-la.com/pdf/prensa/informe/cronologia_virus_informaticos.pdf

Donohue, B. (2014, April 10). ¿Qué Es Un Hash Y Cómo Funciona? Kaspersky. https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

Egele, M., Scholte, T., Kirda, E., & Kruegel, C. (2012). A survey on automated dynamic malware-analysis techniques and tools. ACM Computing Surveys, 44(2), 1–42. https://doi.org/10.1145/2089125.2089126

Espitia, D. S. (2019, July 25). GandCrab: historia del ransomware de principio a fin. Telefónica Tech. https://telefonicatech.com/blog/grandcrab-historia-de-principio-a-fin

GlobalSuite Solutions. (2023, March 20). ¿Qué es la norma ISO 27001 y para qué sirve? GlobalSuite Solutions. https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

González, E. (2022, August 10). Identificadas 192 familias de ransomware en todo el mundo. Bit Life Media. https://bitlifemedia.com/2022/08/ransomware-familias/

Guide to Technical Report Writing : Study guides. (n.d.). Sussex.ac.uk. https://www.sussex.ac.uk/ei/internal/forstudents/engineeringdesign/studyguides/techreportwriting

HackWise. (2022, August 2). Peligrosa banda de ransomware hackeó un oleoducto europeo. HackWise. https://hackwise.mx/peligrosa-banda-de-ransomware-hackeo-un-oleoducto-europeo/

Hadi, A. (n.d.). Understanding malware analysis with Dr. Ali Hadi. INE, Inc. https://ine.com/blog/understanding-malware-analysis-with-dr-ali-hadi

IBM. (n.d.). ¿Qué es el ransomware? Ibm.com. https://www.ibm.com/es-es/topics/ransomware

IBM Documentation. (2023, March 24). Ibm.com. https://www.ibm.com/docs/es/aix/7.3?topic=management-smb-protocol

Inoue, D., Yoshioka, K., Eto, M., Hoshizawa, Y., & Nakao, K. (2009). Automated malware analysis system and its sandbox for revealing malware's internal and external activities. IEICE Transactions on Information and Systems, E92-D(5), 945–954. https://doi.org/10.1587/transinf.e92.d.945

Kaspersky. (2023a, April 19). Identificación de ransomware: en qué se diferencian los troyanos de cifrado. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Kaspersky. (2023b, April 19). Ransomware LockBit: lo que necesitas saber. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware

Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (n.d.). Ransomware, threat and detection techniques: A review. Edu.My. Retrieved November 16, 2023, from https://seap.taylors.edu.my/file/rems/publication/105055_5256_1.pdf

La evolución del ransomware. (2023, February 13). KeepCoding Bootcamps. https://keepcoding.io/blog/la-evolucion-del-ransomware/

Latto, N. (2020, February 27). ¿Qué es WannaCry? ¿Qué es WannaCry?; Avast. https://www.avast.com/es-es/c-wannacry

Ley 1273 de 2009 - Gestor Normativo. (2009). Gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Liu, S., Feng, P., Wang, S., Sun, K., & Cao, J. (2022). Enhancing malware analysis sandboxes with emulated user behavior. Computers & Security, 115(102613), 102613. https://doi.org/10.1016/j.cose.2022.102613

Los 6 tipos de malware. (2022, August 18). KeepCoding Bootcamps. https://keepcoding.io/blog/tipos-de-malware/

Marquez, J. (2024, February 20). Adiós LockBit: la banda de ransomware más peligrosa del mundo ha sido desmantelada tras una operación internacional. Xataka.com; Xataka.

https://www.xataka.com/seguridad/adios-lockbit-banda-ransomware-peligrosa-mundo-ha-sido-desmantelada-operacion-internacional

Mash, M. (2019, March 6). Cómo evitar el ransomware GandCrab. Kaspersky. https://www.kaspersky.es/blog/gandcrab-ransomware-is-back/17959/

Microsoft. (2023a, March 1). Microsoft security bulletin MS17-010 - critical. Microsoft.com. https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN

Microsoft. (2023b, July 3). Función CreateServiceA (winsvc.h). Microsoft.com. https://learn.microsoft.com/es-es/windows/win32/api/winsvc/nf-winsvc-createservicea

Microsoft. (2023c, July 3). Función CreateServiceA (winsvc.h). Microsoft.com. https://learn.microsoft.com/es-es/windows/win32/api/winsvc/nf-winsvc-createservicea

Moser, A., Kruegel, C., & Kirda, E. (n.d.). Limits of static analysis for malware detection. Tuwien.ac.at. https://auto.tuwien.ac.at/~chris/research/doc/acsac07_limits.pdf

Motheram, H. (2023, February 16). Día Cero RCE en GoAnywhere MFT [CVE-2023-0669]. Censys. https://censys.com/es/rce-zero-day-in-goanywhere-mft-cve-2023-0669/

¿Qué es AIDS Trojan? (2022, August 11). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-aids-trojan/

¿Qué es Conficker? (2022, August 16). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-conficker/

¿Qué es el adware? Los 7 ejemplos más terribles (2023). (n.d.). SoftwareLab. Retrieved September 29, 2023, from https://softwarelab.org/es/blog/que-es-el-adware/

¿Qué es el malware? (2020, July 10). McAfee. https://www.mcafee.com/es-co/antivirus/malware.html

¿Qué es el ransomware WannaCry? (2023, August 18). www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

¿Qué es Elk Cloner? (2022, August 10). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-elk-cloner/

¿Qué es un virus informático? (2022, June 20). KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-un-virus-informatico/

¿Qué es una sandbox? (2022, August 26). KeepCoding Bootcamps. https://keepcoding.io/ciberseguridad/que-es-una-sandbox/

Ramirez, F. (2020, January 31). Concept, el primer virus de macro. Derecho de la Red; derechodelared. https://derechodelared.com/concept-el-primer-virus-de-macro/

Sanjana. (2024, January 21). Anticipe los ataques ransomware LockBit. ManageEngine Blog. https://blogs.manageengine.com/espanol/2024/01/21/anticipe-ataques-ransomware-lockbit.html

Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The hands-on guide to dissecting malicious software. No Starch Press.

TheIET. (n.d.). A guide to technical reporting. Theiet.org. https://www.theiet.org/media/5182/technical-report-writing.pdf

Valades, B. (2022, March 3). Top 10 de ciberataques en 2021: el ransomware encabeza el ranking. Segurilatam. https://www.segurilatam.com/actualidad/top-10-de-ciberataques-en-2021-el-ransomware-encabeza-el-ranking_20220303.html

Valenzuela, C. G. (2023, February 16). Qué es un ataque de triple extorsión de ransomware, la nueva tendencia entre los ciberdelincuentes. Computer Hoy. https://computerhoy.com/ciberseguridad/ataque-triple-extorsion-ransomware-nueva-tendencia-ciberdelincuentes-1200866

Vazquez, R., & Gonzalez, M. (2022, December 5). ¿Como opera ALPHV el programa de membresías de RaaS? Metabase Q. https://www.metabaseq.com/es/como-opera-alphv-el-programa-de-membresias-de-raas/

Vinod, P., & V. Laxmi, M. S. G. (2009). Survey on Malware Detection Methods. Hack.in 2009.

What is malware? (n.d.). Trellix.com. https://www.trellix.com/en-us/security-awareness/ransomware/what-is-malware.html

Yoshioka, K., Hosobuchi, Y., Orii, T., & Matsumoto, T. (2010). Vulnerability in Public Malware Sandbox Analysis Systems. https://www.researchgate.net/publication/221428311_Vulnerability_in_Public_Malware_Sandbox_Analysis_Systems

Yoshioka, K., Inoue, D., Eto, M., Hoshizawa, Y., Nogawa, H., & Nakao, K. (2009). Malware sandbox analysis for secure observation of vulnerability exploitation. IEICE Transactions on Information and Systems, E92-D(5), 955–966. https://doi.org/10.1587/transinf.e92.d.955

(N.d.). Cloudflare.com. https://www.cloudflare.com/es-es/learning/ddos/glossary/mirai-botnet/

Universidad®
Católica
de Manizales

VIGILADA MINEDUCACIÓN

Obra de Iglesia
de la Congregación

Hermanas de la Caridad
Dominicas de La Presentación
de la Santísima Virgen

Universidad Católica de Manizales
Carrera 23 # 60-63 Av. Santander / Manizales - Colombia
PBX (6)8 93 30 50 - www.ucm.edu.co

;