ANÁLISIS DE UN ESQUEMA METODOLÓGICO PARA DETECTAR Y PREVENIR CRYPTORANSOMWARE A SISTEMAS OPERATIVOS WINDOWS 10 EN ESTACIONES DE TRABAJO.

JOHNATAN MAZO RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
MEDELLÍN - ANTIOQUIA
2021

ANÁLISIS DE UN ESQUEMA METODOLÓGICO PARA DETECTAR Y PREVENIR CRYPTORANSOMWARE A SISTEMAS OPERATIVOS WINDOWS 10 EN ESTACIONES DE TRABAJO.

JOHNATAN MAZO RAMIREZ

MONOGRAFÍA DE OPCIÓN DE GRADO PARA OBTENCIÓN DEL TÍTULO DE: INGENIERO DE TELECOMUNICACIONES

ASESOR

CARLOS EDUARDO VELÁZQUEZ VILLADA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
MEDELLÍN - ANTIOQUIA
2021

AVAL

Se certifica que el presente trabajo fue desarrollado por Johnatan Mazo Ramírez, bajo la supervisión y aprobación del asesor y jurado asignados.

_____

Asesor asignado: Carlos Eduardo Velázquez Villada

_____

Jurado Asignado: Andrés Quintero Zea

Medellín, 23 de julio del 2021

AGRADECIMIENTOS

Agradezco inicialmente a mi familia, especialmente a mi madre quien estuvo allí apoyando todo este proceso educativo y valores, impartiendo todo este conocimiento y ayuda, para mi persona es un gran ejemplo por seguir.

GLOSARIO

- **MALWARE:** El significado es software malicioso, el cual está construido y diseñado para modificar estaciones de trabajo sin autorización, servidores o usuarios algunos ejemplos pueden ser: virus, botnets, rootkits o ransomware.

- **RANSOMWARE**: Este puede ser un programa o software con el que se busca cifrar o secuestrar información de la víctima por medio de las estaciones de trabajo, servidores o dispositivos móviles exigiendo a cambio un bien común como dinero, información u otro tipo de divisas para poder recuperar la información por medio de una llave de descifrado.

- **CRYPTORANSOMWARE:** Este tipo de ransomware es de alta criticidad y masiva difusión permitiendo cifrar una parte de información de la víctima y puede ser de difícil recuperación sin la clave ligada a este ransomware.

- **CIBERCRIMINAL:** Es la persona o grupo que busca acceder sin autorización, con fines de actividades maliciosas, infectando los sistemas de información. Puede tener como objetivo ganar dinero de forma ilegal en el mundo cibernético.

- **CIBERSEGURIDAD:** Esta área busca prevenir y proteger las estaciones de trabajo, servidores, dispositivos de red, móviles y sistemas de información de ataques de cibercriminales.

- **VARIANTE:** Es un elemento u objeto que tiende a variar a partir de una raíz.

- **DETECTAR:** Consiste en captar la presencia de una cosa, objeto o persona.

- **PREVENIR:** Consiste en implementar medidas de control o tomar algunas precauciones advirtiendo futuros daños, amenazas, peligros o riesgos.

RESUMEN

Durante la última década (2011-2020), el malware conocido como Ransomware ha crecido como una amenaza de ciberseguridad para empresas, empleados y personas. Este crecimiento está relacionado con los métodos que se utilizan en la detección y prevención de malware, los cuales pueden llegar a ser deficientes e insuficientes, además, los vectores y variantes del Ransomware van cambiando y actúan de forma diferente hacia un objetivo específico. Por esto se hace difícil analizar y comprender la gran cantidad de variables personalizables por los cibercriminales dependiendo del funcionamiento del software malicioso.

En esta monografía se analizarán los siguientes trabajos: "Estudio sobre el malware Ransomware" de Carlos Estrada (Estrada Cola, 2018) y "Elaboración de recomendaciones de buenas prácticas a partir del estudio de los principales tipos de malware ransomware que han atacado en Ecuador a las estaciones de trabajo con sistema operativo Windows mediante análisis dinámico y estático" de Jennyfer Alexandra Andrade Valdez y Giovanny Paúl Galarza Zurita (Andrade Valdez & Galarza Zurita, 2019) donde se tomaron 5 muestras de variantes de Cryptoransomware como : CTB-locker, Crytowall, VaultCrypt, WannaCry y Petya que fueron simuladas y analizadas en un entorno controlado para conocer el periodo de vida de un Ransomware.

En este estudio se analiza una propuesta para actualizar y verificar un esquema metodológico para detectar y prevenir algunas variantes de cryptoransomware de sistemas operativos Windows 10 en estaciones de trabajo con base al trabajo de (Andrade Valdez & Galarza Zurita, 2019) donde se realizan unas recomendaciones de buenas prácticas dependiendo del tipo de ransomware al que se exponen algunos entornos controlados con sistema operativo Windows 7 en estaciones de trabajo a partir de este trabajo se presentan algunos métodos actuales y se plantea una medida de eficacia en el momento de la detección y prevención del malware con su variantes más comunes.

Los trabajos a los cuales se hace referencia (Andrade Valdez & Galarza Zurita, 2019) y (Estrada Cola, 2018) recopilan, caracterizan los métodos y variantes más comunes de las variantes de Cryptoransomware por medio de un estudio aleatorio de CTB-locker, Crytowall, VaultCrypt, WannaCry y Petya.

Con base en el comportamiento de estas variantes de ransomware y basado en el marco esquemático y metodológico de (Andrade Valdez & Galarza Zurita, 2019) para detectar y prevenir las afectaciones causadas por el ransomware, se hacen recomendaciones para el análisis dentro de un equipo con software de Microsoft como Windows 10 más comúnmente utilizado por las empresas y personas, de uso masivo comercialmente.

Finalizando esta monografía se plantean unas recomendaciones para el estudio del esquema metodológico que se realiza en el trabajo (Andrade Valdez & Galarza Zurita, 2019) referente a la detección y prevención del Cryptoransomware y lograr así una mayor eficacia con ayuda de patrones comportamentales establecidos. Se espera que con la implementación de este esquema metodológico sea posible mejorar la respuesta para detener y prevenir este tipo de malware cambiante y común en los sistemas operativos más recientes.

Palabras Clave: Cryptoransomware, malware, ransomware, cibercriminal, método, ciberseguridad y variante.

SUMMARY

Over the past decade (2011-2020), the malware known as Ransomware has grown as a cybersecurity threat to businesses, employees, and individuals. This growth is related to the methods used in the detection and prevention of malware, which can become deficient and insufficient, in addition, the vectors and variants of Ransomware change and act differently towards a specific objective. For this reason, it is difficult to analyze and understand the large number of variables customizable by cybercriminals depending on the operation of the malicious software.

This monograph will analyze the following works on (Study on Ransomware malware by Carlos Estrada and Angela M. Garcia) and (Preparation of good practice recommendations based on the study of the main types of ransomware malware that have attacked the workstations with windows operating system using dynamic and static analysis by Jennyfer A. Andrade) where 5 samples of Cryptoransomware variants were taken such as: CTB-locker, Crytowall, VaultCrypt, WannaCry and Petya. Significant that were simulated and tested in a controlled environment to know the life span of a Ransomware.

This study analyzes a proposal to update and verify a methodological scheme to detect and prevent some variants of cryptoransomware of Windows 10 operating systems on workstations based on the work of (Andrade Valdez & Galarza Zurita, 2019) where they are carried out Some good practice recommendations depending on the type of ransomware to which some controlled environments with Windows 7 operating system are exposed on workstations. From this work, some current methods are presented and a measure of effectiveness is proposed at the time of detection and prevention of malware with its most common variants.

The works referred to (Andrade Valdez & Galarza Zurita, 2019) and (Estrada Cola, 2018) collect, characterize the most common methods and variants of Cryptoransomware variants by means of a random study by CTB -locker, Crytowall, VaultCrypt, WannaCry and Petya.

Based on the behavior of these ransomware variants and based on the schematic and methodological framework of (Andrade Valdez & Galarza Zurita, 2019) to detect and prevent the effects caused by ransomware, recommendations are made for analysis within a computer

with Microsoft software such as Windows 10 most commonly used by companies and people in mass commercial use.

At the end of this monograph, a more detailed analysis is proposed, perfecting the study of the methodological scheme that is carried out in the work of (Andrade Valdez & Galarza Zurita, 2019) regarding the detection and prevention of Cryptoransomware and thus achieve greater efficiency with the help of established behavioral patterns. It is hoped that with the implementation of this methodological scheme it will be possible to improve the response to stop and prevent this type of malware that is so common today in the most recent operating systems and that is mutating.

Keywords: Cryptoransomware, malware, ransomware, cybercriminal, method, cybersecurity and variant.

Contenido

Lista de Ilustraciones

Lista de tablas

INTRODUCCIÓN

Desde la aparición del internet en los años 80 hasta la actualidad y la tecnología como herramientas de comunicación se ha hecho muy popular y utilizada globalmente presente en la vida cotidiana de cada persona compartiendo información y accediendo a una gran cantidad de datos que se tienen de forma masiva generado por las actividades diarias, sociales, empresariales y del mercado. Sin embargo, la aplicabilidad de estas nuevas tecnologías trae consigo diferentes tipos de amenazas dentro de un entorno cibernético desde la década de los 90 se vuelve más generalizado los virus y malware afectando a los usuarios con daños severos a las estaciones de trabajo.

La creación del software malicioso conocido desde sus inicios como malware ha evolucionado en las últimas décadas mutando con algunas variaciones como el Ransomware que se encarga de cifrar y secuestrar la información de un usuario o empresas que tienen en su poder bases de datos con la información financiera, personal o de mercado de muchas personas con un fin intencionado de sacar algún tipo de ganancias por parte de los cibercriminales. Existen dos principales tipos de ransomware como lo son Cryptoransomware y Cryptolocker donde se caracterizan por cifrar o bloquear gran parte de la información o dispositivos con algoritmos especializados que solo con ingresar una llave pública o privada se pueden descifrar, pero esta normalmente es suministrada por los delincuentes.

Normalmente para este tipo de ataques se han tomado bastantes precauciones y controles, pero es necesario e importante no solo reconocer la estructura que los componen sino también analizando el comportamiento de cada tipo de ransomware. Las técnicas y análisis que se han tomado como referencia para combatir los ataques de ransomware que cifra la información de los usuarios y empresas consta de un estudio dinámico del código fuente del malware permitiendo obtener información de su funcionamiento desde las conexiones, registros y comandos que se puedan modificar en cierto tipo de sistema operativo. Al estar en auge y el incremento de estas amenazas se han desarrollado varias herramientas especializadas que ayudan a entender con facilidad el desarrollo y despliegue del ransomware algunas de estas

son: wireshark, Depency Walker, Pestudio, Pebrowser, Pexplorer e IDA pro todas estas herramientas en su gran mayoría open source deben simularse en un entorno aislado y controlado dentro de una máquina virtual impidiendo el paso del ransomware contenido para el análisis.

Teniendo en cuenta el impacto de las amenazas recurrentes como lo son el ransomware y que existe una aceptación del riesgo por parte de los usuarios y empresas que son víctimas de este tipo de ataques se ve reflejado una descentralización sobre el conocimiento y esquemas de la detección de ciberamenazas por parte de los equipos de ciberseguridad al no seguir algunos lineamientos de la asegurabilidad de la infraestructura y plataformas TI. Así como la prevención también juega un rol importante, aunque se tengan muchas herramientas para defender y analizar malware se pretende mejorar la metodología esquemática que se tiene con respecto a la valoración del ransomware específicamente el cryptoransomware unificando los marcos de detección y prevención que existen por parte de las entidades gubernamentales y sin ánimo de lucro.

Durante este trabajo se analiza el estudio del esquema metodológico que realizan y proponen los autores de las investigaciones sobre ransomware (Andrade Valdez & Galarza Zurita, 2019) referente a la detección y prevención del Cryptoransomware y lograr así una mayor eficacia con ayuda de patrones comportamentales establecidos. Se proponen recomendaciones para detener y prevenir este tipo de malware en Windows 10.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad se pueden encontrar un sin fin de soluciones de ciberseguridad que permiten identificar y evitar algunos eventos e incidentes que se pueden producir hacia un objetivo como las empresas y personas por medio de malware, aun así, las infraestructuras tecnológicas seguirán siendo un foco bastante susceptible a algunas amenazas y brechas de seguridad que surgen día a día como son ataques dirigidos con Phishing o malware personalizado a afectar algunos sectores como sector financiero e infraestructuras críticas.

De acuerdo con esto se ve reflejada una aparición reciente de diferentes tipos de malware más sofisticados con técnicas mejoradas para encapsular u ocultar estos ataques mediante técnicas de ofuscación para poder eludir la seguridad perimetral de las empresas o estaciones de trabajo en donde esta detección se hace por medio de firmas o inteligencia artificial. Estas nuevas variantes han generado una mayor dificultad a la hora de detectar y prevenir los diferentes tipos de malware, en específico el ransomware y los 2 tipos en el que se derivan como el Cryptoransomware y Cryptolocker que logran cifrar la información dentro de estas infraestructuras tecnológicas. Todo esto genera la necesidad de diseñar y desarrollar nuevas metodologías de análisis para optimizar los procesos de prevención ante una inminente amenaza cibernética.

En función de lo detallado anteriormente, la siguiente monografía propone un análisis del esquema metodológico en cuanto a la detección y prevención de Cryptoransomware durante la evolución del ciclo de vida por medio de etapas o fases. Dependiendo del análisis a todo este esquema y metodología se diseñará un esquema metodológico para proponer controles adecuados para esos programas maliciosos que se pueden presentar con el análisis de algunas variantes de CryptoRansomware como CTB-Locker, Crytowall, VaultCrypt, WannaCry y Petya recolectados dentro de los trabajos de (Andrade Valdez & Galarza Zurita, 2019) y (Estrada Cola, 2018) enfocado en los sistemas operativos Windows 10 que hoy en día son los más vulnerables por su gran repertorio comercial e implementación.

OBJETIVOS

Objetivo General

Analizar un esquema metodológico soportado con controles de análisis de malware para detectar y prevenir ataques generados por las variantes de Cyptoransomware a sistemas operativos Windows 10 en una estación de trabajo.

Objetivos Específicos

- Describir los criterios y variantes de las familias del Cryptoransomware para la elección y usabilidad dentro de un esquema metodológico que aborda controles para detectar y prevenir malware.
- Con base en el esquema metodológico existente, proponer un modelo que pueda reunir una acción eficaz detectando y previniendo ciberamenazas por un ataque por CryptoRansomware dentro de las estaciones de trabajo.
- Proponer trabajo futuro como la validación del esquema metodológico propuesto usando muestras y pruebas seleccionadas de las variantes de Cryptoransomware como CTB-Locker, Crytowall, VaultCrypt, WannaCry y Petya.

JUSTIFICACIÓN

El mundo de la tecnología y el mundo cibernético han cambiado gran parte de nuestro día a día, facilitando y permitiendo controlar varios aspectos de este.

Este uso masivo de la tecnología e informática está en diversas áreas del sector industrial como lo son: sector de la medicina, financiero, multimedia y redes sociales. Estos sectores tienen algo en común manejando grandes cantidades de datos e información que se almacena en la nube, servidores, teléfonos inteligentes, dispositivos IoT y estaciones de trabajo. Teniendo en cuenta esto, podemos buscar y encontrar varios cientos de archivos con información bastante relevante como son: historiales médicos, facturas, cuentas de cobro, personales, financieros, cuentas de bancos, planos y estructuras militares y de construcción.

La información y datos almacenados se han transformado en un activo tangible muy valioso para las personas y sociedad, colocamos como ejemplo: Una empresa de arquitectura puede perder sus diseños y planos de proyectos o edificios donde han sacrificado sumas de dinero y tiempo, también podemos ver el caso de un hospital que sufra una fuga de información del estado de salud de los pacientes, y así podemos ver muchos casos y aplicarlo a varios sectores de las industrias impactando notoriamente en la imagen, confianza y económicamente.

Los cibercriminales aprovechan y están conscientes de esta mina de oro de información de vital importancia para las empresas, empleados y personas. Saben que algunos de estos sectores por desconocimiento de controles de seguridad o implementación de medidas accedan al pago en dado caso que se pierda, daña o caiga en malas manos este activo tan importante. Uno de los métodos que utilizan los cibercriminales más conocidos se llama Ransomware el cual puede presentar a través de diferentes tipos de ataque y con estas técnicas permitiría apoderarse o capturar esta información, una de las técnicas más utilizadas se llama Cryptoransomware el cual cifra toda la información dentro de un equipo y pide recompensas bastantes altas en dinero o criptomonedas para descifrar o recuperar dicha información.

El malware es una amenaza para todas las infraestructuras de tecnología y más utilizando técnicas como el Ransomware donde tiene un papel importante ya que se utilizan comúnmente por los cibercriminales con o sin experiencia y esto puede ser bastante crítico para las empresas en todo el mundo. Lo que se pretende con este trabajo con modalidad de monografía es analizar los modelos esquemáticos y metodológicos para detectar y prevenir este tipo de Ransomware estudiados en los trabajos de investigación de (Andrade Valdez & Galarza Zurita, 2019) sobre las variantes de Cryptoransomware que analizaron en estaciones de trabajo Windows 7 para abordar la necesidad que tienen las empresas de proteger su información y optimizar desde las áreas de tecnología un análisis efectivo y una respuesta ante este tipo de incidentes tan graves para una empresa, empleado o persona del común que sufre un ataque de esta índole, actualizando algunas de sus recomendaciones para el sistema operativo Windows 10.

MARCO CONCEPTUAL Y TEÓRICO

A continuación, se presentan los conceptos generales en relación con el tema de malware enfocado en su tipo como lo es el Ransomware y sus variantes a la que se le hace mención en el trabajo de grado. Estos conceptos permitirán definir cuáles pueden ser los componentes más relevantes para determinar un esquema metodológico para detectar y prevenir cuando ocurra un incidente de seguridad con este tipo de malware. De igual forma se pretende describir otros conceptos de trabajos que actualmente sirven de guía y orientación referente a los temas relacionados como objeto de estudio complementando este trabajo de grado.

Definiciones

1.1 Ransomware

La idea detrás del ransomware, una forma de software malicioso es simple: bloquear y cifrar la estación de trabajo de la víctima o los datos del dispositivo, luego exigir un rescate para restaurar el acceso.

“En muchos casos, la víctima debe pagarle al ciberdelincuente dentro de un período de tiempo determinado o corre el riesgo de perder el acceso para siempre. Y dado que los ataques de malware a menudo son implementados por ladrones cibernéticos, pagar el rescate no garantiza que se restablezca el acceso”. (Grace, 2021)

1.2 Precios y pago de rescate

Los precios del rescate varían según la variante del ransomware y el precio o los tipos de cambio de las monedas digitales. Gracias al anonimato percibido que ofrecen las criptomonedas, los operadores de ransomware comúnmente especifican los pagos de rescate en bitcoins.

Las variantes de ransomware recientes también han incluido opciones de pago alternativas como iTunes y tarjetas de regalo de Amazon. Sin embargo, debe tenerse en cuenta que el pago del rescate no garantiza que los usuarios obtengan la clave de descifrado o la

herramienta de desbloqueo necesaria para recuperar el acceso al sistema infectado o los archivos alojados.

1.3 Infección y comportamiento de ransomware

Los usuarios pueden encontrar esta amenaza a través de una variedad de medios. El ransomware se puede descargar en los sistemas cuando usuarios involuntarios visitan sitios web maliciosos o comprometidos. También puede llegar como una carga útil, ya sea caída o descargada por otro malware. Se sabe que algunos ransomware se entregan como archivos adjuntos de correos electrónicos no deseados,
descargados de páginas maliciosas a través de publicidad maliciosa, o lanzados por kits de explotación en sistemas vulnerables.

Una vez ejecutado en el sistema, el ransomware puede bloquear la pantalla de la computadora o, en el caso del cripto-ransomware, cifrar archivos predeterminados. En el primer escenario, un
"La imagen de la pantalla o la notificación se muestra en la pantalla del sistema infectado, lo que evita que las víctimas utilicen su sistema. Esto también muestra las instrucciones sobre cómo los usuarios pueden pagar el rescate. El segundo tipo de ransomware evita el acceso a archivos de archivos potencialmente críticos o valiosos como documentos y hojas de cálculo". (TrendLabs, 2017)

1.4 Tipología de Ransomware

Los ataques de ransomware se pueden implementar de diferentes formas. Algunas variantes pueden ser más dañinas que otras, pero todas tienen una cosa en común: un rescate. A continuación, se muestran siete tipos comunes de ransomware.
Para todos aquellos que no están familiarizados con el ransomware que acecha en el panorama cibernético actual, ¡aquí hay un poco de conocimiento compartido!
El ransomware es un tipo de malware que ingresa a un sistema informático o red a través de

medios fraudulentos y bloquea el acceso a los archivos cifrándolos hasta que se pague un rescate exigido a los piratas informáticos a cambio de una clave de descifrado.

Ahora, llegando a las variantes de ransomware, básicamente son solo dos conjuntos de ransomware. “El primero es un malware que encripta archivos que bloquean el acceso a la víctima hasta que se le paga en criptomoneda. El segundo tipo de ransomware no cifra los archivos, pero bloquea el acceso de la víctima a los archivos hasta que se pague un rescate.

A medida que los piratas informáticos se vuelven sofisticados, el tercer tipo de ransomware ha surgido en una nota reciente que es un malware que no solo encripta archivos hasta que se paga un rescate, sino que los elimina automáticamente después de un período de tiempo estipulado o si la víctima niega pagar el rescate”.

Las variantes de ransomware observadas hasta ahora son Cryptolocker, WannaCry, Bad Rabbit, Cerber, Crysis, CryptoWall, GoldenEye, Jigsaw y Locky. (Goud, 2019)

- **Cryptoransomware:**

Esta forma de ransomware puede causar mucho daño porque encripta cosas como sus archivos, carpetas y discos duros. Uno de los ejemplos más familiares es el destructivo ataque de ransomware WannaCry de 2017. Apuntó a miles de sistemas informáticos en todo el mundo que ejecutaban el sistema operativo Windows y se extendió dentro de las redes corporativas a nivel mundial. Se pidió a las víctimas que pagaran un rescate en Bitcoin para recuperar sus datos.

- **Locker-ransomware:**

Es conocido por infectar su sistema operativo para bloquear completamente su computadora o dispositivos, haciendo imposible el acceso a cualquiera de sus archivos o aplicaciones. Este tipo de ransomware suele estar basado en Android.

- **Scareware:**

Es un software falso que actúa como un antivirus o una herramienta de limpieza. Scareware a menudo afirma haber encontrado problemas en su computadora, exigiendo dinero para resolverlos. Algunos tipos de scareware bloquean su computadora. Otros inundan tu pantalla

con molestas alertas y mensajes emergentes.

- **Doxware:**

Es comúnmente conocido como software de fuga o extorsión, amenaza con publicar la información robada en línea si no paga el rescate. A medida que más personas almacenan archivos confidenciales y fotos personales en sus computadoras, es comprensible que algunas personas entren en pánico y paguen el rescate cuando sus archivos han sido secuestrados.

- **RaaS:**

También conocido como "Ransomware como servicio", RaaS es un tipo de malware alojado de forma anónima por un pirata informático. Estos ciberdelincuentes se encargan de todo, desde la distribución del ransomware y la recogida de pagos hasta la gestión de descifradores, software que restaura el acceso a los datos, a cambio de su parte del rescate.

- **Ransomware de Mac:**

Los sistemas operativos Mac fueron infiltrados por su primer ransomware en 2016. Conocido como KeRanger, este software malicioso infectó los sistemas de los usuarios de Apple a través de una aplicación llamada Transmission, que pudo encriptar los archivos de sus víctimas después de ser lanzada.

- **Ransomware en dispositivos móviles:**

"El ransomware comenzó a infiltrarse en dispositivos móviles a mayor escala en 2014. ¿Qué sucede? El ransomware móvil a menudo se envía a través de una aplicación maliciosa, que deja un mensaje en su dispositivo que dice que se ha bloqueado debido a una actividad ilegal." (Camelo, 2019)

1.5 ¿Quiénes son los objetivos de los ataques ransomware?

Ransomware puede extenderse a través de Internet sin objetivos específicos. Pero la naturaleza de este malware de cifrado de archivos significa que los ciberdelincuentes también

son capaces de elegir sus objetivos. Esta habilidad de segmentación permite a los ciberdelincuentes ir tras aquellos que pueden, y son más propensos a, pagar rescates más grandes.

Aquí hay cuatro grupos objetivo y cómo cada uno puede verse afectado.

- Grupos que se perciben como que tienen equipos de seguridad más pequeños. Las universidades entran en esta categoría porque a menudo tienen menos seguridad junto con un alto nivel de intercambio de archivos.

- Organizaciones que pueden y pagarán rápidamente. Las agencias gubernamentales, los bancos, las instalaciones médicas y grupos similares constituyen este grupo, porque necesitan acceso inmediato a sus archivos, y pueden estar dispuestos a pagar rápidamente para obtenerlos.

- Empresas que contienen datos confidenciales. Los bufetes de abogados y organizaciones similares pueden ser blanco de ataque, porque los ciberdelincuentes banco en las controversias legales que podrían derivarse si los datos que se mantienen para el rescate se filtran.

- “Negocios en los mercados occidentales. Los ciberdelincuentes van por los pagos más grandes, lo que significa dirigirse a las entidades corporativas. Parte de esto implica centrarse en el Reino Unido, los Estados Unidos y Canadá debido a una mayor riqueza y uso de computadoras personales”. (Fruhlinger, 2020)

1.6 Formas de Distribución de un Ransomware

- **Phishing Emails**

El método más común para que los piratas informáticos propaguen ransomware es a través de correos electrónicos de phishing. Los piratas informáticos utilizan correos electrónicos de

phishing cuidadosamente elaborados para engañar a la víctima para que abra un archivo adjunto o haga clic en un enlace que contiene un archivo malicioso.

Ese archivo puede venir en varios formatos diferentes, incluidos PDF, archivo ZIP, documento de Word o JavaScript.

“En el caso de un documento de Word, el atacante suele engañar al usuario para que "habilite macros" al abrir el documento. Esto permite al atacante ejecutar un script que descarga y ejecuta un archivo ejecutable malicioso (EXE) desde un servidor web externo. El EXE incluiría las funciones necesarias para cifrar los datos en la máquina de la víctima”. (Goud, 2018)

- **Remote Desktop Protocol**

Un mecanismo cada vez más popular en el que los atacantes infectan a las víctimas es a través del Protocolo de escritorio remoto (RDP). “Como su nombre lo indica, el Protocolo de escritorio remoto se creó para permitir que los administradores de TI accedan de forma segura a la máquina de un usuario de forma remota para configurarla o simplemente para utilizar la máquina. Normalmente, RDP se ejecuta en el puerto 3389”. (Challita, 2018)

- **Malicious URLs**

Los atacantes también utilizan correos electrónicos y plataformas de redes sociales para distribuir ransomware insertando enlaces maliciosos en los mensajes. Durante el tercer trimestre de 2019, casi 1 de cada 4 ataques de ransomware utilizó el phishing por correo electrónico como vector de ataque, según cifras de Coveware.

“Para animarle a hacer clic en los enlaces maliciosos, los mensajes suelen estar redactados de una manera que evoca un sentido de urgencia o intriga. Al hacer clic en el enlace, se activa la descarga de ransomware, que encripta su sistema y retiene sus datos para obtener un rescate”. (Emsisoft Malware Lab, 2021)

- **MSPs and RMMs**

Los ciberdelincuentes con frecuencia se dirigen a los proveedores de servicios administrados (MSP) con ataques de phishing y explotando el software de monitoreo y administración remota (RMM) comúnmente utilizado por los MSP.

"Un ataque exitoso a un MSP puede potencialmente permitir que los ciberdelincuentes implementen ransomware en toda la base de clientes del MSP y ejerzan una inmensa presión sobre la víctima para que pague el rescate. En agosto de 2019, 22 ciudades de Texas fueron atacadas con ransomware que se propagó a través de herramientas MSP. Los atacantes exigieron 2,5 millones de dólares para desbloquear los archivos cifrados". (Emsisoft, 2019)

- **USB drives and portable computers**

Las unidades USB y las computadoras portátiles son un vehículo común de entrega de ransomware. La conexión de un dispositivo infectado puede provocar que el ransomware cifre la máquina local y se propague potencialmente por la red.

- **Network propagation**

Si bien las cepas más antiguas de ransomware solo eran capaces de cifrar la máquina local que infectaron, las variantes más avanzadas tienen mecanismos de auto propagación que les permiten moverse lateralmente a otros dispositivos en la red. Los ataques exitosos pueden paralizar organizaciones enteras.

Algunos de los ataques de ransomware más devastadores de la historia incluían mecanismos de propagación automática, incluidos WannaCry, Petya y SamSam.

1.7 Funcionamiento del ransomware

Ransomware no es especialmente complicado en términos de programación. Las funciones de cifrado existen de forma nativa en equipos basados en Windows y Unix como macOS y Linux. Algunos atacantes optan por empaquetar su propio marco de cifrado para evitar la detección por el software AV, pero hay un montón de proyectos de código abierto que los

atacantes pueden utilizar. Lo que es más, con la aparición de ransomware-as-a-Service como Cerber RaaS y Shifr Raas, los atacantes pueden simplemente comprar malware listo para usar para distribuir a las víctimas. Los informes indican que los portales para acceder a este tipo de servicios incluso están rompiendo con foros exclusivos de Dark Net para abrir sitios web a los que cualquier aspirante a hacker puede acceder.

Una vez que un atacante tiene un proyecto ransomware en la mano, sólo tienen que decidir cómo distribuirlo. Al igual que con otras formas de malware, vectores de infección típicas dependen de las víctimas de ingeniería social en la descarga de un archivo infectado ya sea desde un sitio web o a través de un correo electrónico de phishing. “A menudo, se utiliza un archivo adjunto de MS Office o un archivo PDF malicioso que, al ser abierto, ejecuta código oculto que a su vez descarga la carga útil de malware. En otros casos, el ransomware podría ser la carga útil entregada por un script en un sitio web maliciosamente elaborado o descargado por un instalador de software falso”. (De Groot, 2020)

1.8 Ciclo de vida del ransomware

Con el fin de entender lo que hay que buscar, primero debemos entender las etapas del ataque típico ransomware.

Etapa 1: Campaña

Hay una variedad de canales de entrega para ransomware, pero un correo electrónico de phishing es el más popular. Supongamos que recibe un correo electrónico de un minorista en línea, indicando que se le cobró de más y se le debe un reembolso. Usted hace clic en el enlace, ¡sin darse cuenta de que la dirección URL está errada o contiene errores tipográficos, y BAM! El ataque ransomware está en marcha.

Etapa 2: Infección

En esta etapa se descarga el código malicioso y comienza la ejecución de código. En este punto su sistema ha sido infectado con ransomware, sin embargo, ninguno de sus archivos

está encriptado todavía. El cifrado es un cálculo matemático reversible que es una tarea intensiva de CPU. En un ataque ransomware típico, sus efectos no se producen inmediatamente porque toma tiempo para el malware para determinar el alcance de los datos para cifrar.

Es importante tener en cuenta que, en este punto, todos los controles de detección automatizada han fallado. El firewall, el proxy, la solución antivirus y el sistema de detección de intrusiones han permitido la infección.

Etapa 3: Escenificación

En esta etapa, el código malicioso garantiza la conectividad con su servidor de comando y control (C2). Un servidor C2 es controlado por el atacante y se utiliza normalmente para enviar comandos al sistema comprometido. Sin embargo, con ransomware, la comunicación con el C2 se da para principalmente obtener la clave de cifrado. En este punto, se realizan varios cambios en los sistemas y se establece la persistencia. El atacante ahora "posee" el sistema.

Etapa 4: Escaneado

Aquí es cuando las cosas comienzan a ralentizarse un poco. En primer lugar, el malware analiza su equipo local para encontrar archivos para cifrar. Esto puede tardar segundos a minutos. También puede buscar datos almacenados en la nube, que se sincronizan a través de carpetas y aparecen como datos locales. A continuación, busca recursos compartidos de archivos. Esto puede tardar horas dependiendo de la cantidad de recursos compartidos que tenga en su red. El objetivo es investigar qué datos están disponibles y determinar qué nivel de permisos tiene el usuario comprometido (por ejemplo, lista, escritura, eliminación).

Etapa 5: Cifrado

Una vez que todos los datos se inventarían, el cifrado comienza. El cifrado de archivos local puede producirse en minutos; sin embargo, el cifrado de archivos de red puede tardar muchas horas. Esto se debe a que en la mayoría de los ataques ransomware, los datos en los recursos

compartidos de archivos de red se copian y cifran localmente. A continuación, los archivos cifrados deben cargarse y los archivos originales eliminados. Este proceso le da algo de tiempo. Supongamos que tiene un recurso compartido de archivos de 25 GB. Va a tomar el equipo local un tiempo para cifrar esos datos y luego subirlo.

Estado 6: Día de pago

Una vez que haya llegado a esta etapa, sus datos se han ido, y el atacante está exigiendo el pago. Y ahora está en modo de recuperación.

Ransomware es particularmente insidioso. Aunque ransomware a menudo viaja a través de correo electrónico, también se puede aprovechar de las puertas traseras o vulnerabilidades.

1.9 Cómo detectar ransomware

Por desgracia, si usted no ha podido evitar ransomware, su primer signo podría ser una unidad cifrada o bloqueada y una nota de rescate.

"Si ejecuta su malware y comprobador de virus con frecuencia con definiciones actualizadas de virus y malware, su software de seguridad puede detectar el ransomware y alertarle de su presencia. A continuación, puede optar por poner en cuarentena y eliminar el ransomware. Tener un plan de recuperación ante desastres

La detección proactiva de ransomware incluye respuesta activa a incidentes, continuidad del negocio y un plan para la recuperación ante desastres". (Celiktas, B., & Karacuha, E.,2018).

- ✓ Un plan es esencial y debe ser la piedra angular de la estrategia de seguridad de una empresa.
- ✓ Configure un plan de comunicación que detalle quién debe ponerse en contacto con quién.
- ✓ Determine qué equipo necesitaría alquilar o comprar para mantener las operaciones

en marcha. Planifique que su hardware actual no esté disponible durante días.

- ✓ Escriba instrucciones explícitas sobre dónde se almacenan los datos y cómo recuperarlos.
- ✓ Implementar una política de copia de seguridad regularmente para evitar que ransomware cause pérdida de datos.
- ✓ Implemente un servicio de recuperación ante desastres.
- ✓ Proporcione números de teléfono para ponerse en contacto con los proveedores que pueden restaurar los sistemas que proporcionan para usted.
- ✓ Prevenir un ataque ransomware con preparación
- ✓ Las empresas deben permanecer vigilantes en la era actual de violaciones de datos y ataques ransomware.
- ✓ Aprenda los pasos adecuados para prevenir, detectar y recuperarse de ransomware, y puede minimizar su impacto en su negocio. Utilice estos consejos para mantener seguros los activos de información de su organización y detener un ataque ransomware antes de que comience.
- ✓ Use un proveedor de centros de datos y proveedores de confianza. Realice la diligencia debida para asegurarse de que son confiables. (Estrada Cola, 2018)

1.10 Métodos de Detección y Prevención para Ransomware

El cripto-ransomware es una amenaza desafiante que cifra los archivos de un usuario mientras oculta la clave de descifrado hasta que la víctima paga un rescate. Este tipo de malware es un negocio lucrativo para los ciberdelincuentes, que genera millones de dólares al año. “La propagación del ransomware está aumentando a medida que la protección tradicional basada en la detección, como antivirus y anti-malware, ha demostrado ser ineficaz para prevenir ataques. Además, esta forma de malware está incorporando algoritmos de cifrado avanzados y ampliando la cantidad de tipos de archivos a los que apunta. Los ciberdelincuentes han encontrado un mercado lucrativo y nadie está a salvo de ser la próxima víctima”. (Gonzalez & Hayajneh, 2017)

Finalmente, hay varios pasos críticos que puede tomar para defender su sistema contra futuros ataques de ransomware. Muchas de estas son las mejores prácticas de seguridad de TI que también protegerán contra cualquier número de otras amenazas.

1. **Manténgase actualizado sobre los parches de seguridad.**

Dentro de esta definición se ve reflejado los objetivos del ransomware, tanto WannaCry como NotPetya solo afectaron a los sistemas que no habían instalado el parche de seguridad de Windows más reciente. Si bien muchos de los usuarios tratan las actualizaciones de seguridad como una interrupción y una molestia, estos ataques son un recordatorio aleccionador de cuán importantes son las actualizaciones de seguridad para la salud de nuestros sistemas de TI.

Dicho eso hay formas de administrar sus actualizaciones para que no interrumpan a los trabajadores durante las horas críticas de trabajo. La recomendación es priorizar las actualizaciones para que los parches de seguridad se apliquen de inmediato. Mientras tanto, otras actualizaciones del sistema pueden posponerse hasta el cierre del día y ejecutarse a una hora determinada, como las 3:00 am, cuando es poco probable que los usuarios estén trabajando.

2. **Mantener copias de seguridad regulares y seguras.**

Las copias de seguridad de datos periódicas son fundamentales para las empresas en muchos aspectos. Después de todo, el ransomware es solo uno de los riesgos que enfrenta su empresa por la pérdida de datos. Las copias de seguridad de datos mantienen los activos de su empresa a salvo de cortes de energía, fallas del sistema y equipos perdidos o dañados.

En el caso de un ataque de ransomware, seguramente estará agradecido de tener una copia de seguridad reciente a mano. Esto se gestiona fácilmente trabajando con su equipo de TI para crear un cronograma de modo que las copias de seguridad puedan realizarse automáticamente. También debe tomar precauciones para asegurarse de que sus copias de seguridad tampoco estén en riesgo de infección.

3. **Cree alertas de detección de ransomware.**

A diferencia de la mayoría del malware, que puede acechar sin ser detectado dentro de un sistema durante meses, el ransomware funciona rápidamente y requiere monitoreo en tiempo real para ser derrotado. La buena noticia es que existen varias formas de detectar ransomware antes de que pueda dañar su sistema.

Un programa anti-ransomware puede detectar estos archivos en su computadora y ponerlos en cuarentena antes de que comiencen a cifrar sus datos. Sin embargo, este no es un sistema infalible. La lista de extensiones de archivo de ransomware conocidas se está expandiendo rápidamente, y siempre existe la posibilidad de que la extensión sea algo increíblemente común o nunca visto.

Por suerte, los programas de detección de ransomware también pueden detectar actividades sospechosas y detenerlas antes de que lleguen demasiado lejos. Por ejemplo, el software de detección de ransomware puede notar si muchos archivos están sufriendo cambios de nombre en un período excepcionalmente corto y luego señalar al administrador del sistema de un posible ataque de ransomware. Por ejemplo, el cambio de nombre de los archivos a una velocidad de más de cuatro archivos por segundo es una actividad inusual incluso en una red grande.

4. **Limite el acceso a datos sensibles.**

Los firewalls son otro medio importante de protección contra malware y otros virus. Un firewall puede impedir que los usuarios accedan a ciertos sitios web, y puede bloquear determinadas descargas de archivos según su tipo o su punto de origen. También puede configurar firewalls que aíslen sus sistemas más críticos de otras computadoras en su red. Esto puede contener la propagación del ransomware y limitar su impacto en su organización. También debe configurar sistemas que controlen el acceso de los usuarios a los datos confidenciales. Si menos empleados tienen acceso a datos críticos, es menos probable que se vean comprometidos. Entonces, si un departamento necesita un acceso más amplio a Internet y, por lo tanto, diferentes permisos de firewall, entonces también querrá limitar la forma en

que esas computadoras interactúan con el resto de su sistema.

5. **Capacite a sus empleados en el uso seguro de la computadora.**

‘’Muchos virus, no solo ransomware, ingresan primero a un sistema informático a través de un error humano. Al establecer protocolos de seguridad y capacitar a los empleados en su uso adecuado, puede ayudar a prevenir un brote en su organización’’. (Brightline Technologies, 2017)

METODOLOGÍA

Para este trabajo de grado como monografía se toman las metodologías de algunos trabajos que a continuación se describirán planteando los análisis de las diferentes familias de cryptoransomware.

Elaboración de recomendaciones de buenas prácticas a partir del estudio de los principales tipos de malware ransomware que han atacado en Ecuador a las estaciones de trabajo con sistema operativo Windows mediante análisis dinámico y estático - Andrade Valdez, Jennyfer Alexandra y Galarza Zurita, Giovanny Paul.

Metodología para el análisis de malware que se analizará en esta monografía.

La metodología que se propone en el trabajo de grado de Jennyfer Alexandra Andrade a la cual se hace referencia en este trabajo de grado como base de la monografía propuesta consiste en estudiar y analizar detalladamente el malware con el fin de conocer y comprender su estructura funcional de cada componente.

Durante el análisis planteado de malware se busca aplicar un conjunto de técnicas apropiadas logrando identificar y reconocer los recursos que se utilizan como: modificación dentro del sistema operativo, ataques y masificación por medio de la red, infección y modificación de archivos y otros comportamientos que puedan ser utilizados por el malware con el objetivo de alterar una estación de trabajo.

En esta metodología se plantea un conjunto de técnicas divididas en dos agrupaciones teniendo en cuenta las variaciones y la interacción que tenga cada familia de malware componiéndose de la siguiente forma: Análisis estático o análisis dinámico.

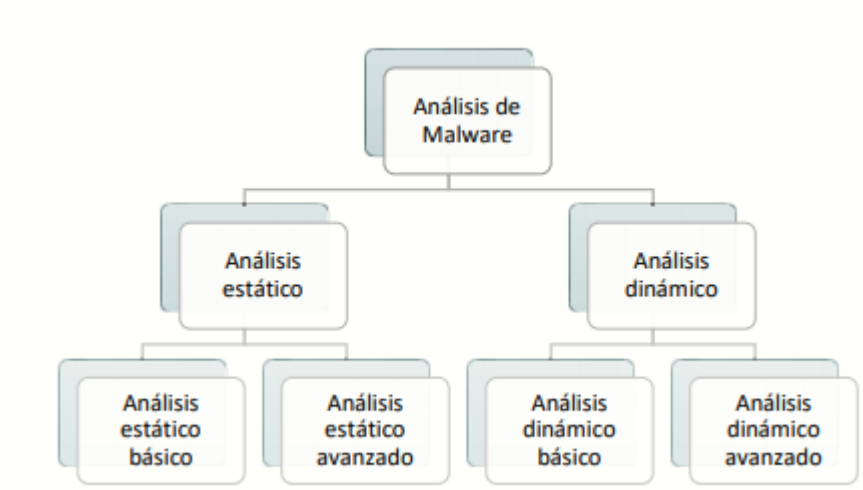


Ilustración 1. *Metodología de análisis de malware. tomado de (Andrade Valdez & Galarza Zurita, 2019)*

Dentro de este análisis se da un resumen sobre los ambientes que se utilizaron en el trabajo de (Andrade Valdez & Galarza Zurita, 2019) basados en la Ilustración 1 Metodología de análisis de malware, donde se inicia generando un ambiente virtual para analizar y ejecutar las evaluaciones de los tipos y variantes de malware enfocado en estaciones de trabajo virtualizadas.

Luego se procede a definir la composición de cada análisis:

- Análisis estático: Para el desarrollo de estas pruebas se deberán tener en cuenta dos subestructuras como lo son un análisis estático básico donde se ejecutan pruebas sin tener interacción directa con la estación de trabajo afectada con malware tratando de utilizar herramientas de antimalware, análisis de hash o código y búsqueda de ejecutables portables temporales y un análisis estático avanzando donde se analiza directamente el malware tratando de realizar varias pruebas complejas como ingeniería inversa que estudia el código cifrado o modificaciones dentro de la estación de trabajo analizando línea a línea el código que lo componen y se logra estudiar de forma tan profunda que se utiliza un lenguaje de máquina.

- Análisis dinámico: En el desarrollo de estas pruebas se recurre a un análisis de código tratando de replicar y examinar los comportamientos y efectos del malware con algunas estrategias como: ejecución del malware de manera controlada. De igual forma se realiza un análisis dinámico avanzado que consiste en conocer la arquitectura del malware con algunas herramientas de programación interactuando con el código del software malicioso.

Para obtener una mayor certeza en la defensa activa en contra de estos métodos y técnicas de ataque de malware y sus variantes no solo teniendo en cuenta los análisis estáticos y dinámicos propuestos en el trabajo anterior sobre el análisis de malware sino también se deberán tener en cuenta otros factores que no depende solo de la estación de trabajo. De igual forma, se debe comprender cuáles deberán ser los activos más relevantes y críticos que se podría vulnerar si hubiera un ataque dirigido por cibercriminales con algunas técnicas y teniendo en cuenta si se lograra materializar o ejecutar una amenaza de ransomware; todo lo anterior es relacionado a cómo elaborar un esquema metodológico donde nos permitiría generar y conservar los principales pilares de seguridad de la información que es: Confidencialidad, Integridad y Disponibilidad.

Iniciando desde la compresión del malware y su forma de ir evolucionando día a día, para tener conocimiento del daño tan grave que podría causar y abordando estos ámbitos se podrían prevenir con una buena preparación de los entornos de manera adecuada y construir los controles necesarios para actuar con mayor eficacia a la hora de combatir de manera activa estas amenazas y evitar materializar un incidente de seguridad mayor.

Diagrama esquemático propuesto en la Ilustración 2, basado en los controles sugeridos en el trabajo de (Estrada Cola, 2018) donde propone varia medidas de seguridad reactivas y pasivas iniciando inicialmente desde una identificación y detección teniendo como objetivo lograr detectar algún intento de infección y ataque por ransomware analizando varios factores con la recopilación de información , correlación de eventos , priorización de eventos , reportar y notificas incidentes y por ultimo documentar, luego sigue una fase de contención teniendo

cono objetivo detener el ataque de ransomware con algunas medidas de seguridad perimetral como firewalls, IDS, IPS y correlacionador de eventos entrando en contacto con la estación de trabajo infectada logrando individualizar y realizar una imagen forense del sistema, la erradicación prosigue donde el objetivo es eliminar los archivos comprometidos y/o restaurar la información cifrada con algunas medidas que iniciarían desde el escaneo por medio de programas de antivirus , antimalware , restauración de imágenes del sistema operativos desde un punto de restauración y realizar un informe forense sobre la imagen generada en la fase de contención , luego de erradicar seguiría una fase de restauración donde se busca restituir y recuperar a un porcentaje mayor del 80 % las estaciones afectadas por el ransomware y poder asegurar desde las copias de información el restablecimiento del servicio en el sistema operativo y por último el tema de capacitación y concientización para los empleados y encargados del área tecnológica para actualizar conocimientos sobre estos tipos de ataques y evitar materializar a futuro este tipo de eventos.

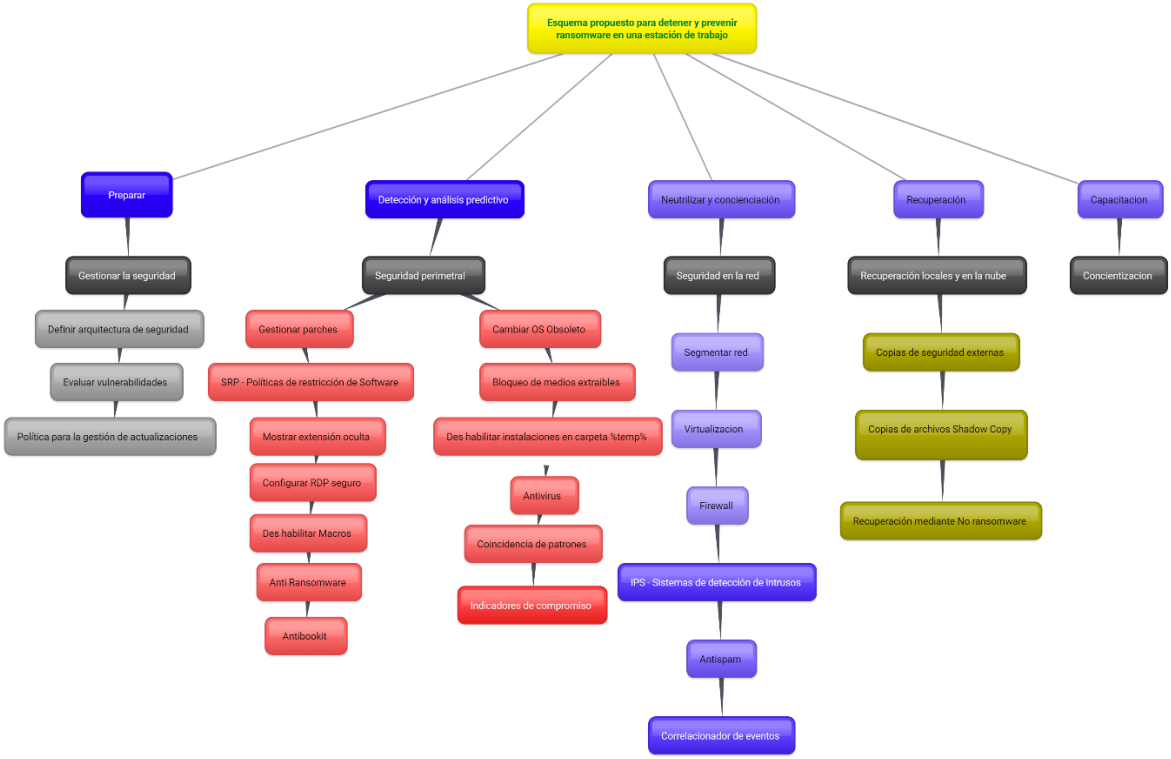


Ilustración 2. *Esquema propuesto para detener y prevenir Cryptoransomware, Fuente propia. Basado en (Estrada Cola, 2018)*

Dentro de la Ilustración 2 Esquema propuesto para detener y prevenir Cryptoransomware, se plantean varias medidas de seguridad dentro del esquema metodológico para proteger y mitigar en mayor medida un ataque por ransomware y sus variantes.

Por consiguiente, se dará una explicación resumida de las medidas utilizadas dentro del esquema.

- **Fase de preparación:**

Durante esta fase se estructura y gestiona la seguridad de la información tratando de preparar al máximo los entornos y unidades de negocio alineados a la asegurabilidad de prevención.

- **Definir arquitectura de seguridad:**

Durante este ítem se busca determinar las decisiones de las unidades de negocio enfocadas en la asegurabilidad del área de TI (Tecnologías de la Información) logrando certificar que la seguridad informática dentro de una infraestructura TI sea lo más coherente definiendo marcos y metodología que ayuden mitigar los riesgos críticos dentro de una organización.

De igual forma se tiene como objetivo como arquitectura la búsqueda y toma de soluciones con roles enfocados a identificar, adquirir, diseñar, aplicar, implementar y desplegar nuevas tecnologías que ayuden a asegurar los entornos y plataformas tecnológicas.

- **Evaluar vulnerabilidades**

Durante la evaluación de las brechas de seguridad y vulnerabilidades realiza una revisión sistemática de las debilidades de seguridad en un sistema de información. Evaluando si el sistema es susceptible a vulnerabilidades conocidas, asignando niveles de gravedad a esas vulnerabilidades y dando recomendaciones, soluciones o planes de mitigación, si es necesario y cuando sea necesario.

- **Política para las actualizaciones de seguridad**

Se deberán aplicar actualizaciones de seguridad y abordar las vulnerabilidades en un plazo de 30 días, o mitigaciones equivalentes, o dispensación aprobada formalmente. En muchos casos, habilitar las actualizaciones automáticas es la mejor opción. Los sistemas deben comprobarse periódicamente para confirmar que las actualizaciones necesarias están siendo instalados

- **Fase de detección y análisis predictivo**

Durante esta fase se desarrollará una estrategia de detección y análisis predictivo con ayuda de algunos dispositivos y plataformas de seguridad perimetral que ayudarán a la identificación y detección temprana de algunas ciberamenazas las cuales se describirán a continuación.

- **Gestionar parches de seguridad**

La gestión de parches es el proceso que ayuda a adquirir, probar e instalar varios parches (cambios de código) en aplicaciones y herramientas de software existentes en una estación de trabajo, lo que permite a los sistemas mantenerse actualizados sobre los parches existentes y determinar qué parches son los adecuados evitando a futuro intrusiones o materialización de alguna vulnerabilidad.

- **Política de restricción de software**

Estas permiten aplicar la configuración de seguridad a un GPO (Directiva de grupo) para lograr reconocer el software y revisar la capacidad para ejecutarse en una estación de trabajo, sitio, dominio o unidad organizativa local. Las políticas de restricción de software controlan la capacidad de los programas para ejecutarse en un sistema.

- **Anti- ransomware**

Los recursos anti-ransomware son soluciones integrales que mantienen la seguridad de la estacion de trabajo y protegen los datos confidenciales que se transmiten a través de una red o se almacenan en dispositivos locales. Las herramientas anti-ransomware a menudo

incluyen múltiples componentes, incluidas herramientas anti-spyware y phishing, así como soluciones antivirus para virus prominentes, que están aislados e identificados por recursos de seguridad. Estas pueden emplear análisis, estrategias, software gratuito o herramientas con licencia para detectar rootkits, gusanos, troyanos y otros tipos de software potencialmente dañino

- **Anti-bootkit**

Los bootkits son una forma avanzada de rootkits que toman la funcionalidad básica de un rootkit y la amplían con la capacidad de infectar el registro de arranque maestro (MBR) o el registro de arranque por volumen (VBR) para que el kit de arranque permanezca activo incluso después de reiniciar el sistema. Los bootkits están diseñados para no solo cargarse desde el registro de inicio maestro, sino que también permanecen activos en la memoria del sistema desde el modo protegido hasta el inicio del sistema operativo y durante el estado activo de la computadora.

- **Antivirus**

El software antivirus es un tipo de utilidad que se utiliza para escanear y eliminar virus de una estación de trabajo o servidor. Si bien existen muchos tipos de programas antivirus, su propósito principal es proteger las computadoras de los virus y eliminar cualquier virus que se encuentre.

- **Coincidir patrones**

En general, los antivirus actuales proporcionan el uso de técnicas de coincidencia de patrones en datos a nivel binario para la detección de virus. Con este fin, se utilizan técnicas de coincidencia de patrones para trazar un mapa de los paquetes entrantes e identificar las partes de los paquetes entrantes que coinciden con las firmas de virus.

- **Indicadores de compromiso**

Los indicadores de compromiso son firmas o artefactos de datos únicos que se correlacionan fuertemente con la existencia de una amenaza a la seguridad o una intrusión en la red que debe abordarse.

- **Limitar configuraciones avanzadas en estaciones de trabajo**

Una de las ramas dentro de esta fase es la de configurar un buen entorno con las configuraciones correctas que nos permita asegurar de manera más efectiva las estaciones de trabajo como medidas preventivas, las cuales se describirán como buena práctica.

- **Mostrar la extensión de los archivos**

Dentro de esta configuración se requiere habilitar la vista de las extensiones ocultas de los archivos para lograr evidenciar que corresponde a un formato común y que no viene enmascarado como normalmente se ve reflejado en los malware.

- **Configuración de escritorio remoto (RDP)**

Durante este ítem se deberá tener buenas prácticas con respecto a la limitación de los escritorios remotos, los cuales son comúnmente atacados por cibercriminales si no se tiene una configuración segura y logran acceder a otras máquinas de forma lateral.

- **Deshabilitar Macros en herramientas ofimáticas**

Las Macros juegan un papel importante por lo que algunos cibercriminales han abusado de estas para insertar condigo malicioso y lograr su objetivo por lo que si las macros no son confiables se deberá deshabilitar esta funcionalidad o restringirla por defecto.

- **Cambiar sistema operativo obsoleto**

Este ítem va muy a la par con el tema de parchar las actualizaciones de los sistemas operativos debido a que muchos cibercriminales aprovechan los sistemas obsoletos para explotar vulnerabilidades conocidas por lo que es de urgencia actualizar siempre a una versión estable o cuando el proveedor realice una actualización de seguridad.

- **Bloquea medios extraíbles**

Esta medida puede llegar hacer un poco extrema, pero es un factor de riesgo que llegaría a ser aprovechado por un cibercriminal que quiere ingresar o sacar información de forma anónima. De igual forma se puede infectar una estación de trabajo, extraer contraseña e información confidencial y dañar un equipo por lo que es un riesgo que se debe evaluar.

- **Fase de neutralización y concienciación**

Durante esta fase se pretende individualizar y tomar medidas preventivas más controladas logrando tener un control de la red con reglas, políticas y dispositivos especializados para tal fin.

- **Segmentar red**

La segmentación de la red brinda protección contra los atacantes que logran traspasar las defensas del perímetro limitando su capacidad para moverse lateralmente dentro de la red. También puede proteger sistemas clave de interferencias accidentales o maliciosas por parte de usuarios internos.

- **Virtualizar**

“La virtualización es el proceso de ejecutar una instancia virtual de un sistema informático en una capa extraída del hardware real. Por lo general, se refiere a la ejecución simultánea de varios sistemas operativos en un sistema informático. Para las aplicaciones que se ejecutan en la parte superior de la máquina virtualizada.”
(Open Source, 2021)

- **Firewall**

“Un firewall es software o firmware que evita el acceso no autorizado a una red. Inspecciona el tráfico entrante y saliente utilizando un conjunto de reglas para identificar y bloquear las amenazas. Los firewalls se utilizan tanto en la configuración personal como en la empresa, y muchos dispositivos vienen con una incorporada, incluidas las estaciones de trabajo con

sistema operativo Mac, Windows y Linux. Son ampliamente considerados un componente esencial de la seguridad de la red.” (Lutkevich, 2017)

- **Sistema de prevención de intrusos**

Un IPS es un sistema de seguridad de red diseñado para evitar actividades maliciosas dentro de una red. A menudo se utiliza en combinación con un sistema de detección de red (IDS) y también puede denominarse sistema de detección y prevención de intrusiones (IDPS).

- **Anti-Spam**

Los métodos que detectan los mensajes de correo electrónico que son anuncios no solicitados, se denominan "spam". Se utiliza un filtro de correo no deseado para detectar el correo no deseado y desviarlo a una carpeta de correo no deseado (buzón de correo no deseado)..

- **Correlacionar eventos**

“La correlación de eventos toma datos de los registros de la aplicación o de los registros del host y luego analiza los datos para identificar las relaciones. Las herramientas que utilizan la correlación de eventos pueden realizar acciones, como enviar alertas de fallas de hardware o aplicaciones, según las reglas definidas por el usuario. El análisis de correlación y de causa raíz ha sido incondicional del monitoreo del desempeño de TI durante algún tiempo. Ambas prácticas ayudan a los departamentos de TI a determinar la causa subyacente de un problema y resolverlo rápidamente para minimizar cualquier impacto y pérdida comercial.”
(Zhang, 2017)

- **Fase de recuperación**

Durante esta fase de recuperación se verán algunas medidas preventivas para contrarrestar los efectos si se llegara a materializar un evento con un ataque de ransomware. Definiendo las siguientes medidas de recuperación.

- **Copias de seguridad externas o en la nube**

El beneficio de una copia de seguridad externa es que los datos están protegidos contra desastres naturales. Por ejemplo, si los archivos originales son demolidos en una inundación o un incendio, aún tiene los datos originales en un lugar seguro.

Dado que todos los datos se almacenan de forma segura en la nube, Los datos están seguros. Las copias de seguridad también serán rápidas y podrá conectarse desde cualquier lugar con una conexión a Internet.

- **Shadow copy**

Al intentar crear copias de seguridad de copias de archivos simples en Windows, un problema común son los archivos bloqueados que pueden alterar la operación. Ya sea que el archivo esté abierto actualmente por el usuario o bloqueado por el propio sistema operativo, ciertos archivos deben estar completamente sin usar para poder copiarlos. Afortunadamente, hay una solución simple: Shadow Copy puede acceder fácilmente a las instantáneas que permiten acceder a copias puntuales de los archivos actualmente bloqueados creados por Windows Restore.

- **Fase de concientización**

La conciencia de la ciberseguridad es la combinación de saber y hacer algo para proteger los activos de información de una empresa. Cuando los empleados de una empresa son conscientes de la ciberseguridad significa que comprenden qué son las amenazas cibernéticas, el impacto potencial que tendrá un ataque cibernético en su negocio y los pasos necesarios para reducir el riesgo y evitar que el delito cibernético se infiltre en su espacio de trabajo en línea.

Para este trabajo de grado se abordan varias fases que permitirán dar solución al análisis que se hará al esquema y metodología propuesto:

Fase 1: Características de Cryptoransomware

Fases para el análisis y desarrollo del trabajo de grado**.**

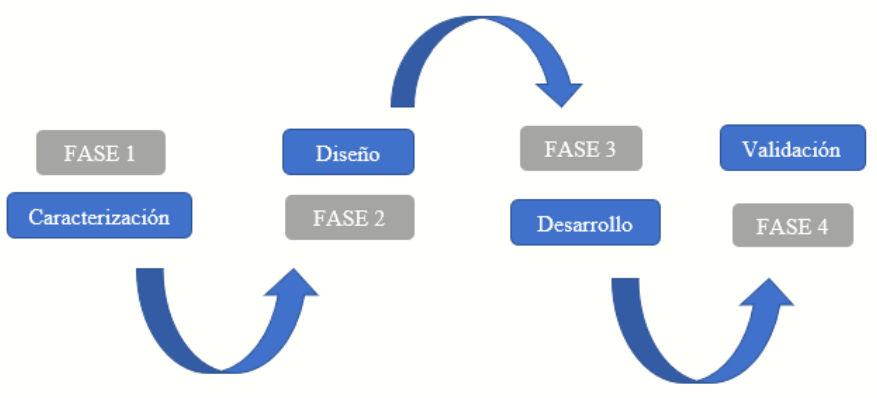


Ilustración 3. *Desarrollo de propuesta, Fuente propia.*

- **Caracterización**

Durante esta fase se tomarán como referencia de los trabajos a analizar 5 muestras de diferentes variantes de tipo Ransomware las cuales están identificadas a continuación: CTB-Locker, Cryptowall, VaultCrypt, WannaCry y Petya definidas en el marco teórico.

"Se tomaron en cuenta 115 muestras reportadas como Ransomware en Ecuador desde el 7 de marzo del 2018 hasta el 21 de agosto del 2018, con lo cual se las clasificó como se muestra en la Ilustración 6." (Andrade Valdez & Galarza Zurita, 2019).

Muestras reportadas en Hybrid Analysis de Ransomware en Ecuador.

Ransomware	Número de muestras reportadas
WannaCryptor	27
Cryptowall	19
Cerber	15
Crysis	14
Locky	12
Satan	10
TeslaCrypt	8
Spora	6
Uiwix	3
CTBLocker	1

Tabla 1. *Muestras reportadas en Hybrid Analysis de Ransomware en Ecuador. Fuente (Andrade Valdez & Galarza Zurita, 2019) .*

‘’La tabla siguiente muestra el valor obtenido en dólares por los ransomwares que trabajan utilizando un modelo de negocio tradicional similar al de CryptoWall. Por las cifras, se puede observar cómo es un negocio bastante lucrativo para los cibercriminales.’’ (Estrada Cola, 2018)

Ransomware	Rescate recibido en Bitcoin	Valor en dólares	Valor en euros
CryptoWall	5.351,2329	2.220.909,12	1.804.055,58
CryptoLocker	1403,7548	449.274,97	364.948,30
DMA Locker	339,4591	178.162,77	144.722,51
WannaCry	47,1743	86.076,76	69.920,58
CryptoDefense	126,6960	63.859,49	51.873,38
NotPetya	4,0576	9.835,86	7.989,72
KeRanger	9,9990	4.173,12	3.389,85

Tabla 2. *Beneficio obtenido con el modelo de negocio tradicional fuente (Estrada Cola, 2018)*

Estas muestras serán consideradas de un alto impacto dentro de los sistemas de informática, se han seleccionado de diferentes fuentes teniendo en cuenta la evolución progresiva del ransomware. Este será enfocado al análisis del malware que durante el tiempo ha venido teniendo una evolución bastante considerable enfocándonos en Windows 10.

Dentro de las variantes que se van a elegir para el desarrollo y análisis. Se caracterizan por medio de comportamientos identificables al momento de la infección. Por lo que la elección de estas interacciones es producto de diferentes fuentes plasmadas en las Ilustraciones anteriores Tabla 1 Muestras reportadas en Hybrid Analysis de Ransomware en Ecuador. Fuente (Andrade Valdez & Galarza Zurita, 2019) y Tabla 2 Beneficio obtenido con el modelo de negocio tradicional fuente (Estrada Cola, 2018) que dan como resultado la identificación de la existencia de algún tipo de malware dentro del sistema operativo.

Dentro de esta fase se desarrollará una estrategia enfocada a la caracterización la cual consistirá en identificar dependiendo el tipo de Cryptoransomware, cual podría ser el comportamiento durante del ataque, analizando el actuar dentro del sistema operativo.

Comportamientos:

1. Capacidad de modificar y cifrar archivos
2. Modificación de claves en Regedit de Windows
3. Creación de directorios temporales para su ejecución
4. Nota y notificación de Cryptoransomware
5. Trafico de red
6. Destruir copias de shadows
7. Autodestrucción y eliminación de rastros digitales luego de intrusión.
8. Registros de dirección IP
9. Búsqueda activa de seguridad perimetral
10. Cambios en registro MBR
11. Modificación en arranque seguro
12. Control de procesos
13. Bloquea procesos del escritorio
14. Cambio en configuración del fondo del escritorio
15. Modificación en restauración del sistema
16. Modificación de las actualizaciones del sistema
17. Modificación de los servicios del sistema
18. Control del administrador de tareas
19. Deshabilitar la restauración del sistema operativo Windows
20. Modificación de los Logs del sistema
21. Posibilidad de inhabilitar seguridad perimetral
22. Control de inicio, reinicio y apagado de la estación de trabajo
23. Expansión por medio de las unidades y red.

Se debe tener en cuenta que este comportamiento se enmarcar en la metodología “MITRE ATT y CK ® siendo una base de conocimientos a nivel mundial accesible de las tácticas del adversario y técnicas basadas en observaciones del mundo real. La base de conocimientos de ATT & CK se utiliza como base para el desarrollo de modelos y metodologías de amenazas

específicas en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad". (MITRE ATT&CK®, 2021)

Estos se califican y se enmarcan dependiendo de su comportamiento y técnica por lo que se evaluará dependiendo de algunos parámetros que se tienen en cuenta según el tipo de gravedad o impacto que pueda tener dentro de los sistemas informáticos.

Medición CVSS

El Common Vulnerability Scoring System (también conocido como CVSS Scores) proporciona una representación numérica (0-10) de la gravedad de una vulnerabilidad de seguridad de la información. Los equipos de seguridad informática suelen utilizar las puntuaciones CVSS como parte de un programa de gestión de vulnerabilidades para proporcionar un punto de comparación entre las vulnerabilidades y priorizar la corrección de las vulnerabilidades.

Calificaciones cualitativas CVSS

A veces es útil, especialmente para fines de discusión con partes interesadas menos técnicas, asignar las puntuaciones CVSS de 0 a 10 a puntuaciones cualitativas. Foro de Equipos de Seguridad y Respuesta a Incidentes (FIRST) asigna los puntajes CVSS a estas calificaciones cualitativas de la siguiente manera:

Puntaje CVSS	Calificación cualitativa
0.0	Ninguno
0.1 – 3.9	Bajo
4.0 – 6.9	Medio
7.0 – 8.9	Elevado
9.0 – 10.0	Crítico

Dentro del resultado final, se obtendrá un porcentaje sobre nivel de compromiso y afectación, teniendo en consideración que el puntaje mayor que se tendrá es de 23 donde aplicaría en

caso de que contenga cada uno de los comportamientos analizados anteriormente descritos donde tendrá un impacto del 100 %. También, se tomará en cuenta la tabla de medición CVSS. Se realiza una extrapolación con relación al porcentaje que se obtiene del comportamiento del malware y la CVSS, podemos tener en cuenta que la escala que se tomará será del 39 % validando la Tabla 3. Escala de CVSS. Fuente propia. con categoría media a partir de las características con mayor afectación, por lo que se pueden considerar de un rango medio, alto y crítico. Por lo que se logrará considerar la fortaleza en la asociación y medición directa con el impacto en los sistemas de forma técnica.

Clasificación CVSS			Medida orientada al modelo propio	
Calificación	%	Categoría	Características	Cantidad de variantes de compromiso
0	0	Nula	0	3
0.1 – 0.39	10% - 39%	Bajo	10% - 39%	8-3
4.0 – 6.9	40% - 69%	Media	40% - 69%	15-9
7.0 – 8.9	70% - 89%	Alta	70% - 89%	20-16
9.0 – 10.0	90% - 100%	Critica	90% - 100%	23-21

Tabla 3. *Escala de CVSS. Fuente propia.*

Se debe tener en cuenta que los valores generados para evaluar los 23 comportamientos se basan en el puntaje cualitativo CVSS que va del 0 a 10 y en nuestro caso aplicaría de 0 a 23 calculando los porcentajes correspondientes y se logra determinar una categoría.

Fase 2: Diseño de esquema metodológico

- **Diseño**

En esta fase de diseño de un esquema de metodología entra en consideración la fase 1 de caracterización, donde se reunirían toda la clasificación de métodos para detectar y prevenir un caso de ransomware, conciliando un análisis cualitativo y cuantitativo dentro de la información que se puede recolectar de los diferentes motores, bases de datos y bancos de conocimiento de forma general.

Se debe tener en consideración que el esquema metodológico se caracterizará primordialmente en la implementación de algunos controles y metodologías más adecuados para detener y prevenir el ransomware en equipos tecnológicos.

En los métodos para la detección y prevención serán valorados por cada una de las variantes del ransomware hallados en la fase de caracterización, donde se tomarán algunos controles como: políticas y controles generales enfocados al área de TI, red, estaciones de trabajo, seguridad perimetral, recuperación y capacitación. Los cuales fueron explicados uno a uno en el planteamiento de la metodología de la Ilustración 3 Esquema propuesto para detener y prevenir Cryptoransomware, Fuente propia.

- **Políticas y controles enfocados al área de TI**
  - Arquitectura de seguridad
  - Gestión de vulnerabilidades
  - Políticas y controles orientados a la ISO 27002.
- **Estación de trabajo**
  - Antivirus
  - Antiransomware
  - Data Execution Prevention
  - Indicadores de compromiso
  - Tecnología de coincidencia de patrones
  - Gestión de parches de segurida

- **Seguridad perimetral**
  - Correlacionar de eventos – SIEM
  - IPS
  - Virtualizar
  - Segmentar red
  - Firewall
  - Antispam
- **Recuperación**
  - Recuperación local y en la nube
  - Copias de seguridad externas
  - Recuperación medio ante herramientas publicadas en No ransomware
- **Capacitación**
  - Concientización

Fase 3: Desarrollo e implementación de controles

- **Desarrollo**

Dentro de la fase de desarrollo, se clasificarán por medio de caracterizar y revisar la documentación, un grupo de estrategias que permitirán detectar de manera rápida el comportamiento del ransomware. De igual forma, esto ayudará a prevenir un incidente mayor que pueda efectuar este ransomware de tipo cryptoransomware. Por lo que se procederá a elegir y analizar una metodología que cumpla esta función logrando analizar la efectividad y reconociendo las variantes del ransomware. Luego, de lograr identificar este esquema se procede a elegir una de ellas mediante la valoración que se definiría en la fase 1 de caracterización.

De igual forma se validará la implementación de algunos controles de seguridad evaluando el nivel de impacto que tenga cada variante de Cryptoransomware como táctica de ciberseguridad reforzando el modelo del esquema propuesto como recomendación que servirá para el manejo de detección y prevención de incidentes de ciberseguridad. Luego de tener identificado la estructura y características de cada familia del ransomware.

Fase 4: Validar la efectividad del esquema propuesto

Validación

Los aspectos para tener en cuenta durante la fase de validación serán los siguientes, teniendo en cuenta que se propondrá mejorar una metodología para la detección y prevención de malware anteriormente descrita por lo que es necesario incorporar los aspectos de efectividad y eficacia.

Teniendo claros los conceptos, se plantean estos indicadores importantes para medir la efectividad de un proceso para generar una mejora continua.

La base para definir un modelo matemático para evaluar la efectividad en la implementación y su eficacia. Surge por la necesidad de las organizaciones de determinar el nivel de preparación frente a la gestión integrada que se deben tener dentro las organizaciones considerando su grado de madurez. Por lo que se elabora un modelo matemático teórico como instrumento que permitiera su cálculo. (Tecnológico et al., 2010). Por consiguiente, se plantearon las siguientes ecuaciones matemáticas.

Ecuación matemática para el cálculo de la Efectividad Teórica

$$\text{Efect} = \sum_{i=1}^{n} \left(\frac{Peso\ del\ indicador}{Valor\ maximo\ de\ los\ indicadores} \right) = 1$$

Para la fase de validación se utilizaría este método matemático descriptivo teórico para poder determinar y tener una sumatoria clara sobre los controles para detectar y prevenir propuestos en la Fase 2 del diseño del esquema metodológico midiendo la efectividad de estos indicadores propuestos con las siguientes fórmulas matemáticas.

Método para detectar

En este método se clasificarán los controles que anteriormente se habían planteado en el esquema metodológico propuesto en la Ilustración 2 Esquema propuesto para detener y

prevenir Cryptoransomware, Fuente propia. Donde se tendrá un grupo orientado a detectar las ciberamenazas con los comportamientos que puedan presentar las variantes de Cryptoramsonware escogidas: CTB-Locker, Cryptowall, VaultCrypt, WannaCry y Petya

Para definir las variables dentro de las fórmulas matemáticas en el método de detección y prevención se tomarán en cuenta los 26 principales controles expuestos anteriormente en el diseño metodológico propuesto y se definirán 4 áreas (Infraestructura, Arquitectura y Red), (Estaciones de trabajo, Servidores y medios de almacenamiento), (Servicios y aplicaciones) y (Herramientas transversales) dentro del desarrollo metodológico donde surgirán 24 controles derivados de los 26 principales. Los cuales se tomarán como resultado para medir la efectividad del diseño metodológico.

- Esta sería la fórmula para la sumatoria del método para detectar:

  Para esta fórmula se tendrán en cuenta la estimación general de los controles propuestos TD y ∑MD la sumatoria de los controles aplicados para detectar las variantes de Cryptoransomware dentro de 4 áreas (Infraestructura, Arquitectura y Red), (Estaciones de trabajo, Servidores y medios de almacenamiento), (Servicios y aplicaciones) y (Herramientas transversales) propuestas en los resultados del desarrollo de la metodología

∑MD= Sumatoria de los controles aplicados para detectar
TD = Estimación general de los controles para detectar

$$CTD=\frac{\text{Sumatoria de los controles aplicados para detectar } (\sum MD)}{\text{Total controles de detección (TD)}}$$

Método para prevenir

En este método se clasificarán los controles que anteriormente se habían planteado en el esquema metodológico propuesto en Ilustración 3 Esquema propuesto para detener y prevenir Cryptoransomware, Fuente propia. Donde se tendrá un grupo orientado a prevenir las ciberamenazas con los comportamientos que pueda presentar las variantes de Cryptoramsonware.

- Esta sería la fórmula para la sumatoria del método para prevenir:

Para esta fórmula se tendrán en cuenta la estimación general de los controles propuestos TP y ∑MP la sumatoria de los controles aplicados para prevenir las variantes de Cryptoransomware dentro de 4 áreas (Infraestructura, Arquitectura y Red), (Estaciones de trabajo, Servidores y medios de almacenamiento), (Servicios y aplicaciones) y (Herramientas transversales) propuestas en los resultados del desarrollo de la metodología

∑MP= Sumatoria de los controles aplicados para prevenir

TP = Estimación general de los controles para prevenir

$$CTP=\frac{\text{Sumatoria de los controles aplicados para prevenir}(\sum MP)}{\text{Total controles de prevencion } (TP)}$$

Para definir los cálculos de estos porcentajes tanto para detectar como para prevenir se tomarán en cuenta las sumas de los controles que se plantearon en la Fase 1 donde determinaríamos el resultado de la efectividad de la aplicación de cada control cubriendo varias áreas que puedan contrarrestar los efectos de los Cryptoransomware de acuerdo con sus comportamientos.

RESULTADOS

Características del Cryptoransomware en estaciones de trabajo

Teniendo en cuenta la metodología anteriormente descrita se presenta la construcción y desarrollo de las técnicas y controles enfocados en detectar y prevenir software malicioso de tipo ransomware de la familia Cryptoransomware realizando un estudio analítico del análisis de una serie de muestras de los scripts o códigos que componen los diferentes ransomwares tomadas desde el trabajo de (Alexandra & Galarza Zurita, Giovanny Paúl, 2019). Este proceso permite explorar el uso, estructura y funcionamiento de las siguientes variantes: **CTB-Locker, Cryptowall, VaultCrypt, WannaCry y Petya**

De acuerdo con la metodología planteada en el trabajo de (Alexandra & Galarza Zurita, Giovanny Paúl, 2019) para el análisis de algunas variantes de ransomware se tomaron varias muestras de ransomware que serán analizadas a continuación mostrando los comportamientos y analizando con herramientas de malware el impacto causado a una estación de trabajo con sistema operativo Windows 7.

- **CTB-Locker**

Durante el análisis de esta muestra se logra identificar con ayuda de algunas herramientas de detección, cómo los antivirus catalogan el CTB-Locker por su tipo de criticidad y afectación en las estaciones de trabajo.

Nombre	CTB-Locker
Tipo	Crypto
Tipo de cifrado	AES-256
Resumen de descripción	Esto escanea el dispositivo de la víctima por completo y cifra los archivos sensibles de destino.

Síntomas	Cuando la víctima se encuentra infectada, se le mostrará una imagen con un mensaje en varios idiomas indicando que debe realizar el pago mediante Bitcoins.
Distribución	Spam y email.
Muestra	

Tabla 4. *Tabla Resumen de análisis de muestra CTB-Locker fuente propia*

Ilustración 4. *Detección de CTBLocker por Hybrid Analysis tomado de (Alexandra & Galarza Zurita, Giovanny Paúl, 2019).*

Dentro de los resultados se visualiza un impacto crítico reportado por los antivirus evaluando la ejecución de la muestra, hallando extensiones enmascaradas como: pdf.exe. lo que permitió a estas herramientas identificar con facilidad un comportamiento común de los archivos maliciosos.

De igual forma se analiza la ejecución del programa para evidenciar las librería y dependencias que activa dentro del sistema operativo hallando lo siguiente:

“Entre las funciones obtenidas, las siguientes pueden afectar el normal funcionamiento del equipo.

- **GetProcAddress:** Esta función se encuentra en la librería Kernel32.dll. Además de las funciones importadas en la cabecera del archivo, esta función puede importar funciones de otras DLL para llamar a cualquier función no declarada.
- **LoadLibraryA:** Es peligrosa puesto que puede invocar a una librería completa que pudo o no ser llamada al inicio del proceso. Esta función se encuentra en la librería Kernel32.dll.
- **GetCurrentProcess:** Esta función tiene acceso a todos los procesos del equipo y puede alterar cualquiera de ellos. Esta función se encuentra en la librería Kernel32.dll.” (Alexandra & Galarza Zurita, Giovanny Paúl, 2019)

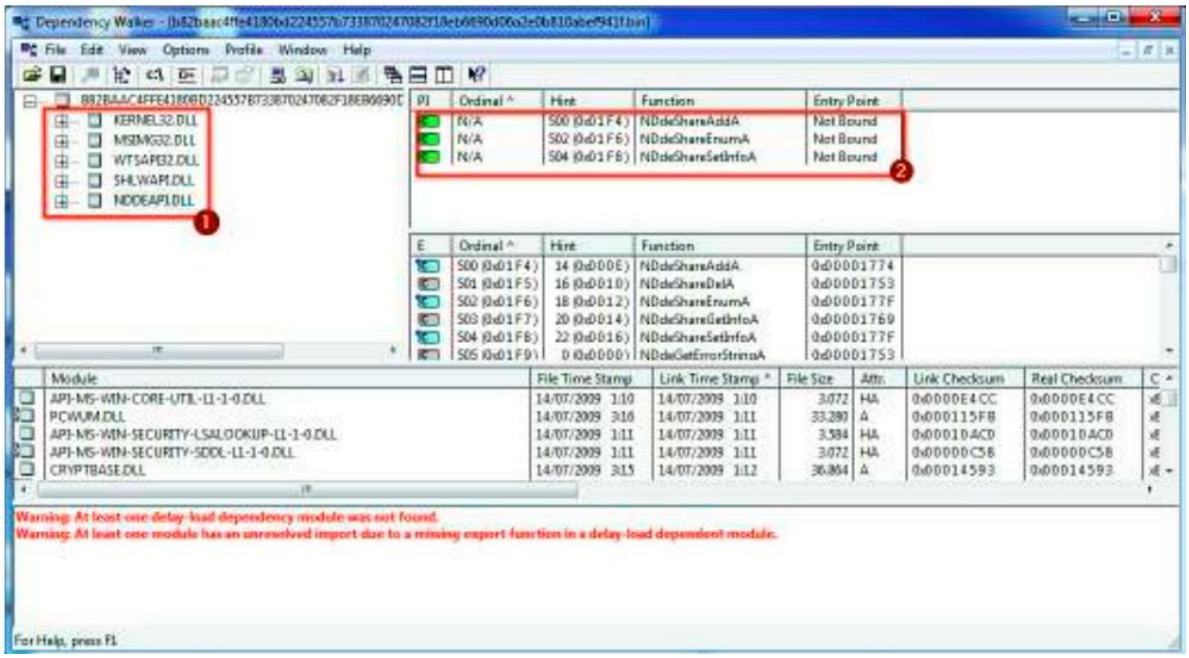


***Ilustración* 5.** *Librerías y funciones de CTBLocker detectadas en Dependencias fuente (Alexandra & Galarza Zurita, Giovanny Paúl, 2019).*

- **Cryptowall y VaultCrypt**

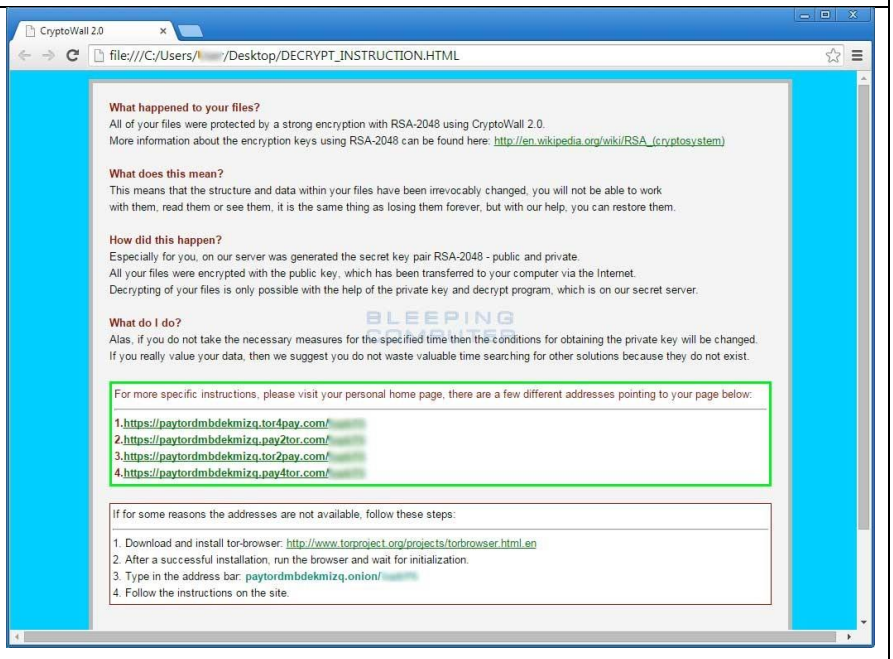
Nombre	Cryptowall y VaultCrypt
Tipo	Crypto
Tipo de cifrado	RSA 2048 y AES
Resumen de descripción	El ransomware, cifra los archivos y lo hace inaccesible y también codifica el nombre del archivo haciendo es difícil de recuperar archivos. La restauración y el retorno al modo anterior también se elimina del sistema de la víctima.
Síntomas	el usuario es engañado haciendo que el usuario abra el correo y descargue el archivo adjunto que contiene el archivo malicioso que ejecuta el ransomware en el sistema de la víctima.
Distribución	Este ransomware utiliza varias técnicas para su distribución como campañas de spam, malvertising, explotar kits.
Muestra	

Tabla 5. *Resumen de análisis de muestra Cryptowall y VaultCrypt fuente propia*

Durante el análisis de esta muestra se logra identificar como algunas herramientas de detección como antivirus catalogan el Cryptowall y VaultCrypt por su tipo de criticidad y afectación en las estaciones de trabajo.

A continuación, observa los resultados

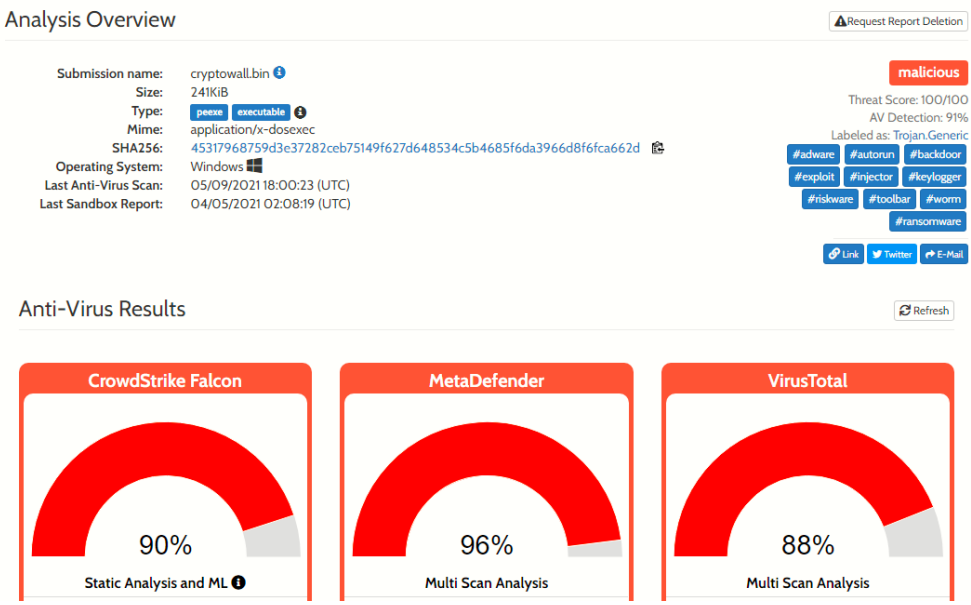


Ilustración 6. *Detección de CryptoWall por Hybrid Analysis tomado de (Alexandra & Galarza Zurita, Giovanny Paúl, 2019).*

Dentro de los resultados se visualiza un impacto crítico reportado por los antivirus evaluando la ejecución de la muestra hallando extensiones enmascaradas como: bin.exe. lo que permitió a estas herramientas identificar con facilidad un comportamiento común de los archivos maliciosos.

De igual forma se analiza la ejecución del programa para evidencia las librería y dependencias que activa dentro del sistema operativo hallando lo siguiente:

“Entre las funciones obtenidas las siguientes pueden realizar cambios no deseados en el equipo:

- **CreateFileMappingA:** Se encuentra en la librería kernel32.dll. Esta función puede crear un identificador para mapear archivos que se cargan en la memoria creando accesos directos a través de las direcciones de memoria.
- **GetProcAddress:** Además de las funciones importadas en la cabecera del archivo, esta función puede importar funciones de otras DLL permitiendo que se invoque a cualquier función no declarada. Esta función se encuentra en la librería kernel32.dll.
- **ControlService:** Esta función se encuentra en la librería advapi32.dll. Se utiliza para iniciar, detener, modificar o enviar una señal a un servicio en ejecución. El malware pude utilizar esta función para manejar su propio servicio.
- **CreateDesktopW:** Esta función se encuentra en la librería user32.dll. Puede ser utilizada por el malware para crear una ventana de escritorio y ser manipulada para mostrar algún mensaje al usuario.” (Alexandra & Galarza Zurita, Giovanny Paúl, 2019)

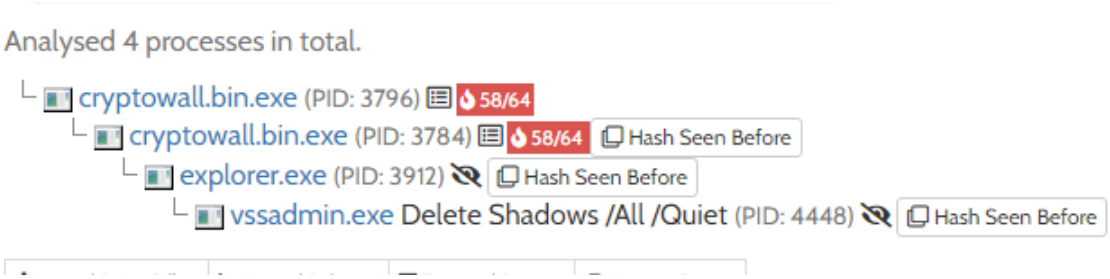


Ilustración 7. *Funciones de CryptoWall detectadas en Dependencias fuente (Alexandra & Galarza Zurita, Giovanny Paúl, 2019).*

❖ **WannaCry**

Durante el análisis de esta muestra se logra identificar como algunas herramientas de detección como antivirus catalogan el WannaCry por su tipo de criticidad y afectación en las estaciones de trabajo.

Nombre	WannaCry
Tipo	Crypto
Resumen de descripción	Este ransomware viene bajo la familia de variantes criptográficas. Instigadores específicos no se encuentran todavía para este ransomware. Más de 150 países se vieron afectados por esta variante de ransomware. Esto también se conoce como WCRY, WANACRYPT0R, WNCRY.
Distribución	Este ransomware se propaga a través de correos de phishing y una vez infectado utiliza la vulnerabilidad SAMBA para propagar dentro de la red.
Muestra	

Tabla 6. *Tabla Resumen de análisis de muestra WannaCry fuente propia*

A continuación, observa los resultados

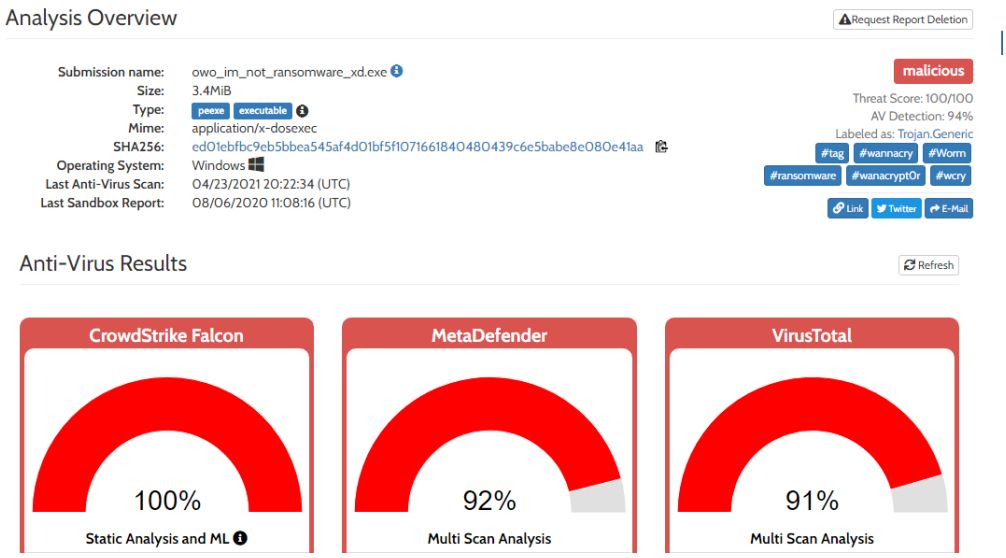


Ilustración 8 *Detección de WannaCry por Hybrid Analysis tomado de (Alexandra & Galarza Zurita, Giovanny Paúl, 2019).*

Dentro de los resultados se visualiza un impacto crítico reportado por los antivirus evaluando la ejecución de la muestra hallando extensiones enmascaradas como: .exe. lo que permitió a estas herramientas identificar con facilidad un comportamiento común de los archivos maliciosos.

De igual forma se analiza la ejecución del programa para evidencia las librería y dependencias que activa dentro del sistema operativo hallando lo siguiente:

“Entre las funciones más interesantes se pueden observar a:

- **CreateProcessA:** Esta función se encuentra en la librería kernel32.dll. Con esta función el malware podría crear nuevos procesos en el equipo infectado.

- **CreateFileA:** Se encuentra en la librería kernel32.dll. Permitiría al malware crear o modificar archivos**.**

- **VirtualAlloc:** Con esta función se puede asignar memoria en un proceso remoto. WannaCry podría utilizarlo para un proceso de inyección. Esta función se encuentra en la librería kernel32.dll.

- **CreateServiceA:** Permite al malware crear y eliminar servicios. Se encuentra en la librería kernel32.dll.” (Alexandra & Galarza Zurita, Giovanny Paúl, 2019)

Ilustración 9. *Librerías y funciones de WannaCry detectadas en Dependencias fuente (Alexandra & Galarza Zurita, Giovanny Paúl, 2019)*

❖ **Petya**

Durante el análisis de esta muestra se logra identificar como algunas herramientas de detección como antivirus catalogan el Petya por su tipo de criticidad y afectación en las estaciones de trabajo.

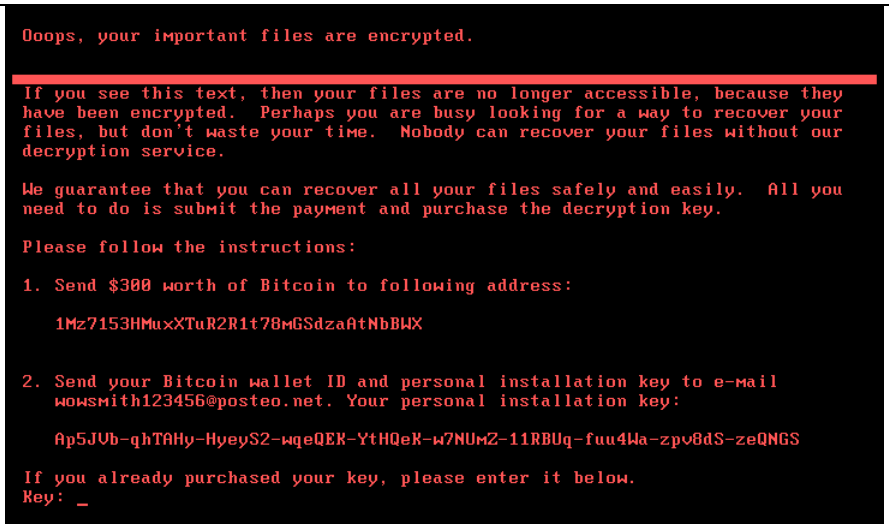
Nombre	Petya
Tipo	Crypto
Tipo de cifrado	RSA y AES
Resumen de descripción	El ransomware, cifra los archivos y lo hace inaccesible y también codifica el nombre del archivo haciendo es difícil de recuperar archivos. La restauración y el retorno al modo anterior también se elimina del sistema de la víctima.
Síntomas	Reiniciará la estación de trabajo. Se observa la pantalla estándar de Windows CHKDSK luego de un bloqueo del sistema. De hecho, el malware ya está trabajando detrás de las escenas para hacer sus archivos inalcanzables
Distribución	Este ransomware utiliza varias técnicas para su distribución como campañas de spam, malvertising, explotar kits.
Muestra	

Tabla 7. *Tabla Resumen de análisis de muestra Petya fuente propia*

A continuación, observa los resultados

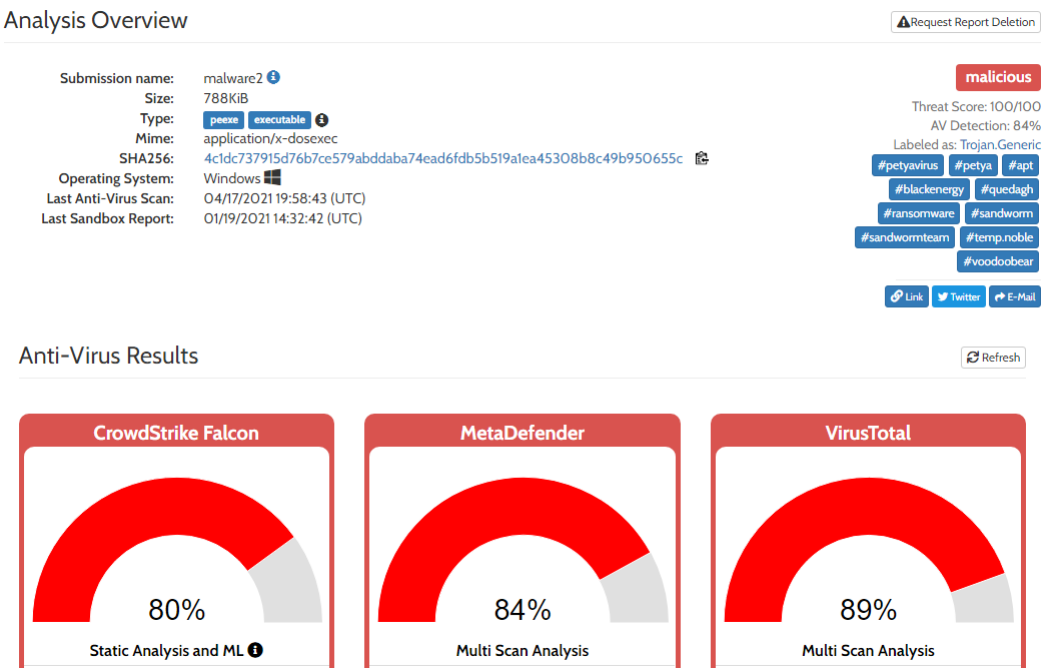


Ilustración 10. *Detección de Petya por Hybrid Analysis tomado de (Alexandra & Galarza Zurita, Giovanny Paúl, 2019).*

Dentro de los resultados se visualiza un impacto crítico reportado por los antivirus evaluando la ejecución de la muestra hallando extensiones enmascaradas como: .exe. lo que permitió a estas herramientas identificar con facilidad un comportamiento común de los archivos maliciosos.

De igual forma se analiza la ejecución del programa para evidencia las librería y dependencias que activa dentro del sistema operativo hallando lo siguiente:

“Entre las funciones más interesantes se pueden observar:

- **CreateProcessA:** Esta función se encuentra en la librería kernel32.dll. Con esta función el malware podría crear nuevos procesos en el equipo infectado.
- **CreateFileA:** Se encuentra en la librería kernel32.dll. Permitiría al malware crear o modificar archivos**.**

- **VirtualAlloc:** Con esta función se puede asignar memoria en un proceso remoto. WannaCry podría utilizarlo para un proceso de inyección. Esta función se encuentra en la librería kernel32.dll.
- **CreateServiceA:** Permite al malware crear y eliminar servicios. Se encuentra en la librería kernel32.dll.” (Alexandra & Galarza Zurita, Giovanny Paúl, 2019)

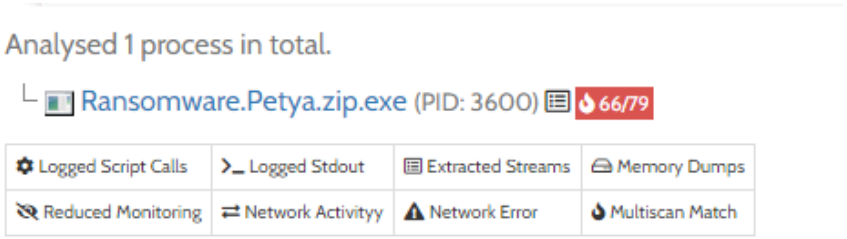


Ilustración 11. *Librerías y funciones de Petya detectadas en Dependencias fuente (Alexandra & Galarza Zurita, Giovanny Paúl, 2019).*

Luego de analizar las 5 variantes de Cryptoransomware a estudiar con respecto a los resultados de los trabajos de estudios de malware se obtiene información con respecto a las características de su funcionamiento, por lo que se procede con la calificación de cada una de estas basados en su comportamiento. Por lo tanto, se contrasta con la lista de comportamientos que tiene comúnmente este tipo de ransomware en una estación de trabajo Tabla 8. Familia de Cryptoransomware vs Posibles comportamientos y porcentaje final fuente propia. dando como resultado un ponderado final con el porcentaje otorgado al contrastar estos dos parámetros comportamentales.

Este análisis va a ir centrado en los criterios basados en cada comportamiento de un cryptoransomware y particularidades como: Método y técnica de entrega, extensión de cifrado, formato, capacidad de eliminar copias de seguridad, validación de comunicación desde el master del comando y control, descifrado y métodos de pago.

Para lograr entender la estructura o ciclo de vida de estas familias de cryptoransomware fue necesario comprender cada característica y alcance que tiene cada una. Para así validar y consolidar la construcción de un esquema para detectar y prevenir ciberamenazas.

Diseño estructural del esquema metodológico

Teniendo en cuenta estos factores y comportamientos se deciden elegir las familias por el alto riesgo e impacto que pueden causar en las estaciones de trabajo con sistema operativo Windows 10.

	Familia				
Posibles comportamientos	CTB-Locker	Cryptowall	VaultCrypt	WannaCry	Petya
Capacidad de modificar y cifrar archivos	X	X	X	X	X
Modificación de claves en Regedit de Windows	X	X	X	X	X
Creación de directorios temporales para su ejecución	X	X	X	X	X
Nota y notificación de Cryptoransomware	X	X		X	X
Trafico de red	X	X	X	X	X
Destruir copias de shadows	X	X	X	X	X
Autodestrucción y eliminación de rastros digitales luego de intrusión.		X	X	X	X
Registros de dirección IP		X			
Búsqueda activa de seguridad perimetral					
Cambios en registro MBR					X
Modificación en arranque seguro					
Control de procesos	X	X	X	X	X
Bloquea procesos del escritorio					
Cambio en configuración del fondo del escritorio				X	
Modificación en restauración del sistema	X	X	X		
Modificación de las actualizaciones del sistema					
Modificación de los servicios del sistema					
Control del administrador de tareas				X	
Deshabilitar la restauración del sistema operativo Windows					
Modificación de los Logs del sistema					
Posibilidad de inhabilitar seguridad perimetral					
Control de inicio, reinicio y apagado de la estación de trabajo					
Expansión por medio de las unidades y red.	X	X	X	X	X
Impacto	39%	48%	39%	48%	43%

Tabla 8. *Variantes de Cryptoransomware vs Posibles comportamientos y porcentaje final fuente propia.*

Los comportamientos plasmados en la Tabla 8 Familia de Cryptoransomware vs Posibles comportamientos y porcentaje final, fueron elegidos en la fase 1 de caracterización del Cryptoransomware para lograr identificar y clasificar el impacto que causan las variantes escogidas como factores comunes reflejados en una estación de trabajo enmarcados por el MITRE ATT&CK®.

Desarrollo e implementación de controles de detección y preventivos de Cryptoransomware

Área	Definición	Enfoque de ciberseguridad	Control de Prevención	Control de Detección
Infraestructura, Arquitectura y Red	Se buscan algunas estrategias que ayudan a mitigar el impacto y riesgos dentro de una infraestructura tecnológica basada en una arquitectura que integre plataformas, redes y demás.	Establecer una arquitectura de ciberseguridad	X	
		Establecer una definición de segmentación y división de red.	X	
		Seguridad perimetral (Firewall/IPS, Proxy y VPN)	X	X
		Implementación de IDS (Sistema de detección de intrusos)	X	X
Estaciones de trabajo , Servidores y medios de almacenamiento	Dentro de las estrategias que se implementaran se enfocaran en los usuarios, servidores, estaciones de trabajo y medios de almacenamiento tanto locales como en la nube.	Seguridad perimetral (Antimalware)	X	X
		Metodología de prevención de ejecución de datos	X	X
		Revisión de sistemas operativos obsoletos y desactualizados	X	X
		Bloqueo de extensiones generadas por ransomware		X
		Visualización de extensiones de archivos ocultos	X	
		Bloqueo de inicio automático de medio extraíbles	X	
		Inhabilitar el inicio y ejecución de archivos temporales sospechosos	X	

		Validar configuración de las políticas de escritorio remoto seguro	X	X
		Validar copias de seguridad y restauración	X	X
		Políticas de prevención de perdida de datos	X	
Servicios y aplicaciones	Se tratarán de incluir las demás plataformas, aplicaciones que cubren las áreas de las herramientas de servicios informativos	Filtros antispam		X
		Filtros de extensiones peligrosas		X
		Validación para instalación de software		X
		Configuración de listas negra y blancas para las aplicaciones	X	
		Inhabilitar macros sin certificado de confianza	X	
Herramientas transversales	Son estrategias centradas a la aplicación de medidas de seguridad a todas las tecnologías.	Evaluar amenazas, brechas de seguridad y vulnerabilidades	X	
		Actualizaciones y parche de seguridad	X	X
		IoC - Indicadores de compromiso	X	
		Implementación de SIEM - Gestión de eventos de información de seguridad	X	
		Capacitación	X	
		Total, de controles de prevención aplicados	20	
		Total, de controles de detección aplicados		12

Tabla 9. *Esquema metodológico para detectar y prevenir Cryptoransomware fuente propia.*

La Tabla 10. Esquema metodológico para detectar y prevenir Cryptoransomware fuente propia. Está basada en los controles de la metodología propuesta.

Metodologías para detectar y prevenir Cryptoransomware

Tomando como referencia la Tabla 10. Esquema metodológico para detectar y prevenir Cryptoransomware, se pueden visualizar los tipos de controles aplicados a algunas plataformas e infraestructuras tecnológicas donde fueron divididas por área o grupo con un foco especifico según lo acordado. Las estrategias allí planteadas fueron clasificadas por su tipo de control siendo preventivo o correctivo previendo un futuro escenario de una infección por alguna familia planteada de Cryptoransomware.

Para cada área específica se ha definido una caracterización, a continuación, se dará una breve descripción:

- **Infraestructura, Arquitectura y Red:**

Dentro de estas áreas se enfoca en proponer algunos controles que buscan mitigar una masificación de ransomware con alguna de sus familias y poder así mitigar el impacto de una crisis por infección desde el área arquitectura de seguridad busca diseñar y elaborar con diferentes tecnologías del mercado. Estas soluciones que puedan ayudar a detectar, prevenir y corregir ciberamenazas. Desde el área de infraestructura tecnológica se pretende asegurar todos los componentes con ayuda de algunos dispositivos de seguridad perimetral como lo son la implementación de Firewall, IPS e IDS que pueden detectar de manera rápida la información maliciosa que ingresa de manera externa. En la parte de red se requiere segmentar o dividir cada componente de la red estableciendo reglas como las ACL que funcionan como permisos para comunicar un segmento de red a otro y tener un mayor control del tráfico interno por lo que esto podría ayudar a detectar cualquier intento de intrusión y poder prevenir cualquier intento de manipulación o propagación por medio de una infección de un ransomware.

- **Estaciones de trabajo, Servidores y medios de almacenamiento**

Dentro de esta área se buscan algunas estrategias apoyadas con ayuda del comportamiento tanto interno como externo de los usuarios pudiendo configurar y aplicar varios controles asegurando las herramientas y dispositivos que se posee, permitiendo analizar e identificar

cualquier tipo de actividad maliciosa o sospechosa apoyado en como los usuarios generan tráfico interactuando con los sistemas, herramientas y dispositivos.

Dentro de área de estaciones de trabajo y servidores se deberán tener en cuenta políticas y controles en cuanto a la restricción de software previendo algún tipo de modificación en los archivos internos del sistema operativo o algún otro programa que pueda afectar o dañar a los sistemas. De igual forma es importante tener en cuenta las aplicaciones de seguridad perimetral como programas antimalware y antivirus que nos permita asegurar y mitigar al máximo los errores humanos a los que están expuestos los usuarios por medio de la difusión del Cryptoransomware y lograr prevenirlo lo más pronto bloqueando su contenido.
Los funcionarios que tiene a cargo la responsabilidad de estos dispositivos dentro del área de TI, por políticas se debe tener un plan de actualización de los sistemas operativos a la última versión estable, aplicaciones, servicios y protocolos obsoletos robusteciendo la seguridad.

- **Servicios y aplicaciones**

Dentro de esta área serán tomadas en cuenta todas aquella aplicaciones y servicios tecnológicos en los que se pueda implementar controles y políticas de seguridad en cuanto al mejoramiento del desarrollo y los ambientes productivos.

Las medidas orientadas a las maquinas sobre el contenido que consumen los usuarios deberá se filtrada evitando la ejecución con extensiones de archivos como .exe, .zip y js o links sospechosos que puedan venir adjuntos en los correos electrónicos. También se tendrán que incorporar listas blancas y negras de las aplicaciones donde no se tengan permitido dentro de una línea base de configuración.

- **Herramientas transversales**

Dentro de esta área se deben abarcar todas la tecnologías y componentes de información que se tienen dentro de la organización con estrategias como el seguimiento y evaluación de vulnerabilidades logrando identificar las brechas de seguridad explotables que pueden inducir a un incidente de ciberseguridad. Para poder minimizar o mitigar las vulnerabilidades

encontradas se podrán programar planes de actualización y parchado de sistemas operativos, aplicaciones, servicios y protocolos inseguros con esto se cubre en mayor medida los ataques aprovechados por los cibercriminales dentro de algunas tecnologías.

En algunas ocasiones se van a materializar algunos ataques que podrían pasar los controles propuestos, cabe resaltar que ningún sistema es seguro. Por lo que sería necesario tener un plan de indicadores de compromisos y análisis por medio de los Sandbox o ambiente virtual para poder individualizar el equipo comprometido estudiando el comportamiento del ransomware y poder prevenir a tiempo la masificación de este.

Otra forma de detectar y lograr un análisis predictivo más efectivo es la implementación de un correlacionador de eventos – SIEM, el cual nos dará en tiempo real alertas, notificaciones y peticiones que se realizan a cada dispositivo de la infraestructura TI que se enfocan en un escaneo activo y pasivo. Pero para lograr un mayor alcance de efectividad en la mitigación del cryptoransomware se necesita buscar concientizar a los usuarios de los peligros de las diferentes campañas de ciberamenazas promovidas por algunos actores como los cibercriminales.

Teniendo en cuenta el análisis de la Tabla 10. Esquema metodológico para detectar y prevenir Cryptoransomware podemos obtener una gran cantidad de métodos de controles preventivos que permitirían notificar o anunciar una posible intrusión mitigando el impacto critico dañino causado por las muestras de Cryptoransomware, se dieron a conocer 24 controles distribuido en 4 áreas (Infraestructura, Arquitectura y Red) , (Estaciones de trabajo, Servidores y medios de almacenamiento) , (Servicios y aplicaciones) y (Herramientas transversales) y la aplicabilidad de los controles de prevención fue de 20 controles lo cual podría mitigar un 83.3% de los comportamientos causador por las variantes de cryptoransomware observados en la Tabla 8 Variantes de Cryptoransomware vs Posibles comportamientos y porcentaje final. Por consiguiente, estos controles ayudan a optimizar el proceso de prevención en las áreas propuestas de manera anticipada evitando que se ejecute o se materialice alguna de las variantes de Cryptoransomware escogidas.

Durante el análisis metodológico para los controles de detección se define que esta sería la responsable de proteger y contener con algunos controles y políticas la infección de una ciberamenazas, se dieron a conocer 24 controles distribuidos en 4 áreas (Infraestructura, Arquitectura y Red) , (Estaciones de trabajo, Servidores y medios de almacenamiento) , (Servicios y aplicaciones) y (Herramientas transversales) y la aplicabilidad de los controles de prevención fue de 12 controles lo cual podría mitigar un 50% de los comportamientos causados por las variantes de cryptoransomware observados en la Tabla 8 Variantes de Cryptoransomware vs Posibles comportamientos y porcentaje final.

Validación esquema de métodos para la detección y prevención del cryptoransomware

Con el objetivo de elaborar un instrumento que nos permitirá validar la efectividad de los controles propuestos aplicados a los 24 controles preventivos y de detección con respecto a las 5 variantes de Cryptoransomware como lo son: CTB-Locker, Cryptowall, VaultCrypt, WannaCry y Petya se toman como referencia los siguientes ítems de calificación:

- Esta sería la fórmula para la sumatoria del método para detectar:

∑MD= Sumatoria de los controles aplicados para detectar
TD = Estimación general de los controles para detectar

$$CTD=\frac{\text{Sumatoria de los controles aplicados para detectar } (\sum MD)}{\text{Total controles de detección (TD)}}$$

Reemplazando las fórmulas obtenemos los siguientes resultados

∑MD= 12
TD = 24

$$CTD=\frac{12}{24}=0.5$$

Por lo que obtendríamos que la efectividad de los controles de detección para cubrir los comportamientos de las variantes de cryptoransomware sería de 0.5

Porcentaje para detectar:

$$CTD=\frac{12}{24} * 100 = 50\ \%\ de\ efectividad$$

Validando la sumatoria de cada método denominado por los controles de detección a cada una de las variantes del Cryptoransomware fueron de 12, que cumplieron de forma parcial a cada estrategia planteada, ya que estas metodologías de detección no cubren los bloqueos o inhabilitación de ejecutar Cryptoransomware representando una efectividad del 50%.

Esta sería la fórmula para la sumatoria del método para prevenir:

∑MP= Sumatoria de los controles aplicados para prevenir
TP = Estimación general de los controles para prevenir

$$CTP=\frac{\text{Sumatoria de los controles aplicados para prevenir}(\sum MP)}{\text{Total controles de prevencion (TP)}}$$

Reemplazando las fórmulas obtenemos los siguientes resultados

∑MP= 12
TP = 24

$$CTP=\frac{20}{24} = 0.83$$

Por lo que obtendríamos que la efectividad de los controles de prevención para cubrir los comportamientos de las variantes de cryptoransomware sería de 0.83

Porcentaje para prevenir:

$$\text{CTD}=\frac{20}{24} * 100 = 83\ \%\ de\ efectividad$$

Validando la sumatoria de cada control denominado por los controles de prevención a cada una de las variantes del Cryptoransomware fueron de 20, que cumplieron de forma parcial a cada estrategia planteada, ya que estos controles preventivos logran mitigar la ejecución Cryptoransomware representando una efectividad del 83.0%.

Teniendo en cuenta los niveles de efectividad con una detección del 50 % y prevención de un 83% con los controles planteados se podría cubrir combinando ambos grupos dentro de un esquema metodológico con un buen porcentaje de efectividad para la mitigación de los comportamientos comunes dentro de las variantes de Cryptoransomware: CTB-Locker, Cryptowall, VaultCrypt, WannaCry y Petya.

Consolidación de resultados

Al finalizar este trabajo de grado como monografía, compuesto por 4 fases para el desarrollo metodológico propuesto, las cuales representan un análisis y estudio profundizando en 5 variantes de Cryptoransomware CTB-Locker, Cryptowall, VaultCrypt, WannaCry y Petya, observando cada una de las características y afectaciones que pueden causar a diferentes áreas dentro de una empresa. Luego de obtener una caracterización de las diferentes variantes de cryptoransomware explicados en esta monografía se logra comprender la articulación y arquitectura de cada malware reconociendo un patrón diferente por cada intrusión y masificación dentro de las estaciones de trabajo permitiendo elaborar una caracterización a las variantes seleccionadas dentro de un modelo esquemático con controles y metodologías para detectar y prevenir ransomware.

Teniendo en cuenta las definiciones socializadas y estudios con respecto a los trabajos de grado de Estudio sobre el malware Ransomware de Carlos Estrada y elaboración de recomendaciones de buenas prácticas a partir del estudio de los principales tipos de malware ransomware que han atacado en ecuador a las estaciones de trabajo con sistema operativo Windows mediante análisis dinámico y estático de Andrade Valdez, Jennyfer Alexandra , se logra reconocer varias brechas de seguridad, vulnerabilidades, riesgos y amenazas de las variantes seleccionadas de Cryptoransomware. Por consiguiente, se plantean 24 controles basados en un esquema metodológico para detectar y prevenir como alternativas de ciberseguridad que se hacen prioritarias para aplicar en cualquiera de las áreas tecnológicas de una organización. Es imprescindible aplicar los debidos controles apoyado del esquema que se elaboró con una metodología para detectar y prevenir cryptoransomware mitigando ciberamenazas producto de los cibercriminales hacia cualquier tipo de organización con una efectividad del 83% en los controles para prevenir y 50% para detectar Cryptoransomware a unas variantes específicas.

Por último, se puede estimar que los controles propuestos para las áreas de aplicaciones, estaciones de trabajo, servidores y herramientas transversales poseen una aplicación para

gran totalidad de los ransomwares aun así se recomienda un plan o cronograma de actividades que se plasmen o estipulen en un documento oficial estándar como línea base para las estaciones de trabajo con sistema operativo Windows 10. De igual forma tener un sistema de implementación para verificar la aplicabilidad logrando una mayor reducción en los casos de infección. Se deberá tener en cuenta las políticas de seguridad de la información para tener una visualización de los controles mitigando los riesgos expuestos.

#	Familia Cryptoransomware	Controles por área			
		1	2	3	4
1	CTB-Locker	X	X	X	X
2	Cryptowall	X	X	X	X
3	VaultCrypt	X	X	X	X
4	WannaCry	X	X	X	X
5	Petya	X	X	X	X

Tabla 10. *Resultado de controles frente a familias de Cryptoransomware.*

CONCLUSIONES

Con el desarrollo de esta monografía como trabajo de grado se logra dar a conocer el nivel comportamental y características de 5 variantes de Cryptoransomware como son: CTB-Locker, Cryptowall, VaultCrypt, WannaCry y Petya, también se evidencian los inconvenientes que se tienen por individualizar los controles para detectar y prevenir el malware para este caso los incidentes por Cryptoransomware en estaciones de trabajo con sistema operativo Windows 10, esto pasa por no tener una arquitectura bien definida teniendo una estructura organizada y de fácil implementación con respecto a los controles de ciberseguridad. Por lo que se elaboró cada una de las fases del ciclo de vida de las variantes en el apartado de resultados junto con los comportamientos de ataque de un Cryptoransomware en la Tabla 8 Variantes de Cryptoransomware vs Posibles comportamientos y porcentaje final. Al mismo tiempo se construye el esquema de la metodología para detectar y prevenir Cryptoransomware por medio de los controles que estaban propuestos de manera teórica en la Tabla 10. Esquema metodológico para detectar y prevenir Cryptoransomware dentro del área de ciberseguridad.

Por medio de las características y comportamientos de 5 variantes de Cryptoransomware se pudo analizar e identificar un patrón y factor común para cada área planteada como lo fueron: Infraestructura, arquitectura, red, estaciones de trabajo, servidores, medios de almacenamiento , servicios, aplicaciones y herramientas transversales teniendo en cuenta que los patrones más repetitivos presentes en los resultados son: Cifrado de información, Métodos de infección y masificación, extorsión por medio de pagos por criptomonedas y el valor exagerado por la recuperación de la información. Durante este estudio se ve reflejado la importancia de analizar y entender cómo operan los cibercriminales con la difusión de estos ataques para poder tomar medidas que nos permitan detectar, proteger, defender y mitigar en gran medida nuestras estaciones de trabajo sin que sufran algún incidente o evitar que se materialice un daño mayor.

Dentro del esquema propuesto analizado y orientado a las estaciones de trabajo se pudo tener una visión mayor en los controles que abarcan esta área durante el desarrollo de las fases de análisis de cada variante de Cryptoransomware, que pueden ayudar al personal de tecnología e informática y equipos de ciberseguridad y seguridad de la información a implementar controles realizando un seguimiento y poder configurar una línea base para mitigar los riesgos a los que se enfrentan estas estaciones de trabajo pudiendo ser uno de los objetivos principales por los cibercriminales.

Por último, se pudo validar el nivel de efectividad del esquema metodológico por medio de 24 controles para detectar y prevenir Cryptoransomware, observando que se puede implementar de forma exitosa en estaciones de trabajo únicamente en sistemas operativos Windows 10, con un porcentaje bastante alto de detección y prevención combinados logrando mitigar las ciberamenazas.

BIBLIOGRAFIA

ZHANG, Ellen. (2017). [Consultado el 15 de Enero del 2021] What is Event Correlation? Examples, Benefits, and More. Digital Guardian. Disponible en: https://digitalguardian.com/blog/what-event-correlation-examples-benefits-and-more/

TRENDLABS. (2017). [Consultado el 30 de noviembre del 2020]. Ransomware - Definition. Trendmicro.com. Disponible en: https://www.trendmicro.com/vinfo/us/security/definition/ransomware

TECNOLÓGICO, I., DOMINGO, S., DOMINICANA, R., PERDOMO, C., ARSENIO, N., Acosta, R., & Nilda, O. (2010). [Consultado el 20 de Enero del 2021] Ciencia y Sociedad. In https://www.redalyc.org/pdf/870/87020009002.pdf. Disponible en: https://www.redalyc.org/pdf/870/87020009002.pdf/

SIERRA, Andres. (2019). [Consultado el 15 de Enero del 2021] Esquema metodológico apoyado en una herramienta (software) para la detección y prevención de Crypto Ransomware en una estación de trabajo. Itm.edu.co, Revista CEA. Disponible en: https://doi.org/http://hdl.handle.net/20.500.12622/1391

OPEN SOURCE. (2021). [Consultado el 15 de Enero del 2021] What is virtualization? Opensource.com. Disponible en: https://opensource.com/resources/virtualization/

MITRE ATT&CK®. (2021). [Consultado el 20 de Enero del 2021] Matrix - Enterprise | MITRE ATT&CK®. Mitre.org. Disponible en: https://attack.mitre.org/matrices/enterprise/

METIVIER, Becky. (2019). [Consultado el 15 de Diciembre del 2020]. Anatomy of a Ransomware Attack and How to Detect the Threat. Tylercybersecurity.com. Disponible en: https://www.tylercybersecurity.com/blog/anatomy-of-a-ransomware-attack-and-how-to-detect-the-threat

LUTKEVICH, Ben. (2017). [Consultado el 15 de Enero del 2021] firewall. SearchSecurity; TechTarget. Disponible en: https://searchsecurity.techtarget.com/definition/firewall/

GRACE, Jennifer van. (2021), [Consultado el 30 de noviembre del 2020]. Ransomware is malicious software that can take over your computer or mobile device, holding your precious data hostage and demanding cash. Norton.com. Disponible en: https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

GOUD, Naveen. (2019).). [Consultado el 13 de Diciembre del 2020]. Types of Ransomware Attacks - Cybersecurity Insiders. Cybersecurity Insiders. Disponible en: https://www.cybersecurity-insiders.com/types-of-ransomware-attacks/

GONZALEZ, Daniel y HAYAJNEH, Thaier. (2017). [Consultado el 15 de Diciembre del 2020]. Detection and prevention of crypto ransomware. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017, 2018-January, 472–478. Disponible en: https://doi.org/10.1109/UEMCON.2017.8249052

FRUHLINGER, Josh. (2020). [Consultado el 13 de Diciembre del 2020]. Ransomware explained: How it works and how to remove it. CSO Online. Disponible en: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

ESTRADA COLA, Carlos. (2018), [Consultado el 30 de noviembre del 2020]. Estudio sobre el malware Ransomware. Universitat Oberta de Catalunya (UOC). Disponible en: http://hdl.handle.net/10609/89025

EMSISOFT. (2019). [Consultado el 15 de Diciembre del 2020]. Cómo se propaga el Ransomware: 9 métodos de infección más comunes y cómo detenerlos. Sertecomsa.com; Sertecomsa.com. Disponible en: https://www.sertecomsa.com/post/2019/12/20/c%C3%B3mo-se-propaga-el-ransomware-9-m%C3%A9todos-de-infecci%C3%B3n-m%C3%A1s-comunes-y-c%C3%B3mo-detenerlos

EMSISOFT MALWARE LAB. (2021). [Consultado el 15 de Diciembre del 2020]. Ransomware statistics for 2020: Q4 report. Emsisoft | Security Blog. Disponible en: https://blog.emsisoft.com/en/35083/how-ransomware-spreads-9-most-common-infection-methods-and-how-to-stop-them/

DE GROOT, Juliana. (2020). [Consultado el 15 de Diciembre del 2020]. What is Cyber Security? Definition, Best Practices & More. Digital Guardian. Disponible en: https://digitalguardian.com/blog/what-cyber-security

CHALLITA, Antonio. (2018). [Consultado el 13 de Diciembre del 2020]. The four most popular methods hackers use to spread ransomware. ITProPortal; ITProPortal Disponible en: https://www.itproportal.com/features/the-four-most-popular-methods-hackers-use-to-spread-ransomware/

CELIKTAS, Baris. y KARACUHA, Ertugrul. (2018). [Consultado el 15 de Diciembre del 2020]. Ransomware, Detection and Prevention Techniques, Cyber Security, Malware Analysis ISTANBUL TECHNICAL UNIVERSITY ↔ INFORMATICS INSTITUTE USING SIGNATURE AND ANOMALY BASED DETECTION METHODS Barış ÇELİKTAŞ Department of Applied Informatics Applied Informa. July. Disponible en: https://www.researchgate.net/publication/326191046_Ransomware_Detection_and_Prevention_Techniques_Cyber_Security_Malware_Analysis

CAMELO, Leonardo. (2019). [Consultado el 13 de Diciembre del 2020]. Seguridad de la Información en Colombia. Blogspot.com. Disponible en: https://seguridadinformacioncolombia.blogspot.com/search?q=doxware

BRIGHTLINE TECHNOLOGIES. (2017). [Consultado el 15 de Enero del 2021]. How to Detect and Prevent Ransomware Attacks. Brightline Technologies; Brightline Technologies. Disponible en: https://brightlineit.com/detect-prevent-ransomware-attacks/

ASALE, Rae. (2020). [Consultado el 15 de Enero del 2021] Diccionario de la lengua española RAE - ASALE. “Diccionario de La Lengua Española” - Edición Del Tricentenario. Disponible en: https://dle.rae.es/efectividad

ANEXO

Se anexa evidencia de contacto con los autores del trabajo de grado Andrade Valdez, J. A. y Galarza Zurita, G. P. (2019) Elaboración de recomendaciones de buenas prácticas a partir del estudio de los principales tipos de malware Ransomware que han atacado en Ecuador a las estaciones de trabajo con sistema operativo Windows mediante análisis dinámico y estático por medio de correo electrónico.

23/7/2021 Gmail - Solicitud de permisos para hacer uso de trabajo de grado como referencia

Gmail johnatan mazo <[redacted]>

Solicitud de permisos para hacer uso de trabajo de grado como referencia

2 mensajes

johnatan mazo <[redacted]> 28 de abril de 2021, 22:19
Para: jenn[redacted]mail.com, gio[redacted]outlook.com

Cordial saludo Jennyfer y Giovanny,

Este correo lo envió con el fin solicitar un permiso para hacer uso del trabajo de grado:

• Elaboración de recomendaciones de buenas prácticas a partir del estudio de los principales tipos de malware ransomware que han atacado en ecuador a las estaciones de trabajo con sistema operativo windows mediante análisis dinámico y estático.

De su auditoria para tomarlo como referencia en mi trabajo de grado como opción de grado para la ingeniería de telecomunicaciones de la Universidad Nacional Abierta y a Distancia de colombia

Este trabajo lo tomaré como referencia para realizar una actualización como monografía para estaciones de trabajo de Windows 10.

Requerimiento:

- Requiero una carta de autorización.

Mis datos:
Johnatan Mazo Ramírez
[redacted]
Universidad Nacional Abierta y a Distancia

Quedo atento,
Muchas gracias.

--

Johnatan Mazo Ramirez
Security Information

JOHNATAN MAZO
SEGURIDAD INFORMÁTICA

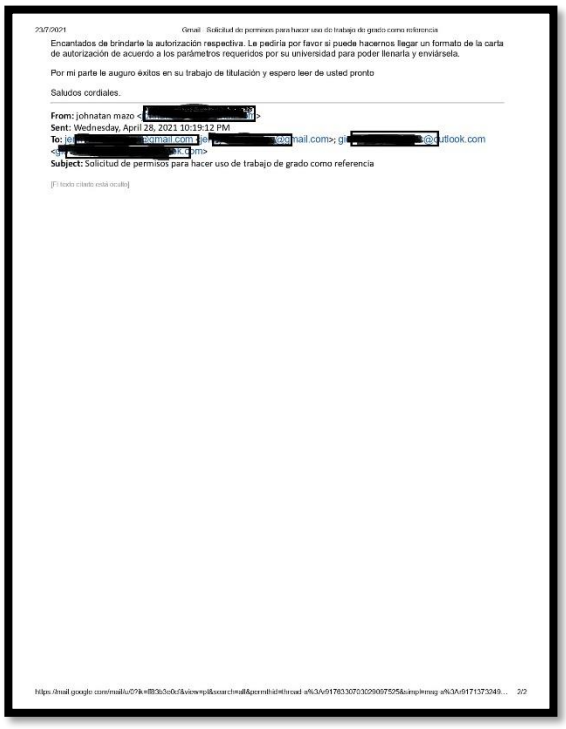
Saferoot | Seguridad Informatica
Medellín Tlf: [redacted]
[redacted]@johnatanmazo.com - www.johnatanmazo.com

No me imprimas si no es necesario. Protejamos el medio ambiente

Giovanny Galarza Zurita <[redacted]@outlook.com> 28 de abril de 2021, 12:15
Para: johnatan mazo <[redacted]mail.com>, "[redacted]mail.com" <[redacted]mail.com>

Estimado Jonathan:

https://mail.google.com/mail/u/0?ik=ff83b3e0cf&view=pt&search=all&permthid=thread-a%3Ar9178330703029097595&simpl=msg-a%3Ar9171373249... 1/3



23/7/2021 Gmail - Solicitud de permisos para hacer uso de trabajo de grado como referencia

Encantados de brindarle la autorización respectiva. Le pediría por favor si puede hacernos llegar un formato de la carta de autorización de acuerdo a los parámetros requeridos por su universidad para poder llenarla y enviársela.

Por mi parte le auguro éxitos en su trabajo de titulación y espero leer de usted pronto

Saludos cordiales.

From: johnatan mazo <[redacted]>
Sent: Wednesday, April 28, 2021 10:19:12 PM
To: [redacted]mail.com>; [redacted]mail.com>; [redacted]@outlook.com
<[redacted]om>
Subject: Solicitud de permisos para hacer uso de trabajo de grado como referencia

[El texto citado está oculto]

https://mail.google.com/mail/u/0?ik=ff83b3e0cf&view=pt&search=all&permthid=thread-a%3Ar9178330703029097595&simpl=msg-a%3Ar9171373249... 2/2