El proceso de infección y ejecución de un Ransomware en el sector empresarial

The process of infection and execution of a Ransomware in the business sector

Angel Antonio Orellano Huayanay

Universidad Nacional Mayor de San Marcos, Lima, Perú

Resumen

Debido al gran avance de la tecnología, actualmente la mayoría de las organizaciones cuenta con información digitalizada ya que permite un mejor y más rápido proceso de información, esto hace de estas organizaciones objetivos de cibercriminales que buscan sacar provecho secuestrando dicha información para paralizar las funciones de la organización obligándolas a pagar el rescate para devolver esa información. A los malwares encargados de esta actividad se les conoce como ransomware y son altamente peligrosos. Por ello mismo en el presente trabajo de investigación se piensa recolectar información de distintas fuentes bibliográficas con el fin de poder dar a conocer el completo circulo de vida de este tipo de malware, así como también se busca comprender el cómo funcionan, por esto la metodología usada fue la de revisión bibliográfica. La principal conclusión que se desarrollo fue el poder identificar los distintos tipos de ransomware, el cómo funcionan y que tipos de acciones se pueden tomar para prevenir la infección o en el peor de los caso minimizar los daños ocasionados por el ransomware.
Palabras Claves: ransomware, ciberseguridad, cibercrimen, Empresas.

Abstract

Due to the great advance of technology, nowadays most of the organizations have digitalized information since it allows a better and faster processing of information, this makes these organizations targets of cybercriminals who seek to take advantage by kidnapping such information to paralyze the functions of the organization, forcing them to pay the ransom to return the information. The malware responsible for this activity is known as ransomware and is highly dangerous. For this reason, in this research work we intend to collect information from different bibliographic sources in order to be able to know the full circle of life of this type of malware, as well as to understand how they work, so the methodology used was the literature review. The main conclusion that was developed was to identify the different types of ransomwares, how they work and what kind of actions can be taken to prevent infection or in the worst case minimize the damage caused by ransomware.
Keywords: ransomware, cybersecurity, cybercrime, companies.

1. Introducción

En la actualidad, casi toda empresa por más pequeña que sea tiene un espacio en la nube y/o maneja información en forma digital, lo que hace que entre en esta nueva era un tema bastante importante que es la ciberseguridad.

La ciberseguridad en empresas tiene un objetivo bastante claro, el cual es la protección de todos los activos informáticos de las empresas ante ataques de ciberdelincuentes, que buscan acceder a estos activos informáticos con el fin de modificarlos, eliminarlos o secuestrarlos para extorsionar a estas empresas(Infante-Moro et al., 2022).

Este último tipo de ataque posee un nombre característico, que es RANSOMWARE, el cual es la unión de dos palabras inglesas, "RANSOM" que viene de un término que se le da a los secuestros que exigen un rescate y "MALWARE" que es el término que se la da a los programas con un fin malicioso (Vielma Montañez, 2022). Los objetivos principales de este tipo de ataque son la información crítica de una empresa y su infraestructura, lo que ocasiona que las operaciones y actividades de la empresa victima paren inmediatamente, pues ya no tienen acceso a dicha información, esta situación hace que el gerente o el encargado de dicha empresa tome una decisión, o bien pagar el rescate que piden y confiar en la palabra del ciberdelincuente o tratar de resolver la situación por su cuenta, ambos casos generan una gran pérdida de tiempo y dinero a la empresa(Barker et al., 2022).

Un ejemplo de este tipo de ciberataque se menciona en (Riega Virú et al., 2021) , donde se dice que en mayo del año 2019, una ciudad en Estados Unidos, recibió un ataque de ransomware que impidió el acceso a miles de empleados y residentes a su computadora, lo que género que no se pudiese pagar facturas o acceder a sus correos electrónicos, el rescate que se pidió en este caso fue de 100 mil euros en bitcoins. Otro caso que también llama la atención es lo sucedido en mayo del 2021, donde el gran Oleoducto Colonial ubicado en Estados Unidos fue cerrado por un ciberataque, y esto puso en peligro cerca del 45% de suministros de combustible de la costa este del país lo que genero un pánico en la población incrementando la demanda por combustible e intensificando el problema de suministro, en este caso se llegó a pagar cerca de 5 millones de dólares en criptomonedas el mismo día, sin embargo esto no impidió que el problema creciese por el pánico que se generó.

Con lo mencionado se puede ver el gran papel que juega la ciberseguridad en las empresas hoy en día, además de también el conocer los distintos tipos de ataques que se pueden dar, es por lo que en la presente investigación bibliográfica se buscara dejar en claro gran parte de los aspectos básicos del ransomware y su funcionamiento.

2. Metodología

2.1. Antecedentes

Conocer acerca del ransomware es un trabajo que lleva bastante tiempo realizándose, y a medida que avanza el tiempo y los recursos tecnológicos mejoran, los métodos de propagación mejoran con ellos. Esto dio pie a que se llevara una investigación acerca de los distintos métodos de propagación del ransomware en el sistema operativo Windows, y dando como resultado que, si bien existen variados métodos, el más común o mejor dicho el más utilizado por los cibercriminales es la ingeniería social(Moreno et al., 2020).

El conocer cómo puede llegar a invadir el ransomware a nuestros equipos por sí solo no es suficiente para poder evitarlos, sino que también debemos contar con medidas de precaución para evitar ser víctimas de este malware, es por lo que se planteó la siguiente investigación, en donde se buscaba analizar los ataques de ransomware para conocer las características de este y poder dar una recomendación respecto a las acciones a seguir para atenuar el daño recibido(Danny et al., 2020).

2.2. Método

Este estudio se elaboró como una revisión bibliográfica, basándose en el siguiente trabajo de investigación (Kitchenham et al., 2009). En esta caso el objetivo principal del estudio

es dar a conocer los aspectos básicos y necesarios de un ransomware. A continuación, se documentos los pasos del método de revisión bibliográfica seguido.

2.2.1. Preguntas de investigación:

Las preguntas de investigación que se plantearon para este estudio son ¿Qué acciones se deberían seguir para evitar verse afectado por el ransomware? y ¿Por qué es importante conocer al ransomware?

2.2.2. Proceso de Búsqueda:

El proceso de búsqueda se dio de forma manual, buscando en distintas fuentes de bibliografía como, Google Scholar, Scielo, entre otras utilizando los siguientes términos claves:

- TIPOS DE RANSOMWARE
- METODOS DE PROPAGACION DE LOS RANSOMWARES
- MEDIDAS DE PREVENCION ANTE RANSOMWARES

2.2.3. Criterios de inclusión y exclusión:

De todos los documentos encontrados se procedió a hacer un filtrado para poder seleccionar aquellos documentos potenciales para la revisión. Como criterios de exclusión e inclusión se utilizaron los detallados en la siguiente tabla.

Table 01. Criterios de exclusión e inclusión

Criterios de Inclusión	Criterios de Exclusión
- Tiempo de publicación no mayor a 4 años previo a la realización de este estudio.	-Estudios que no cumplen los criterios de Inclusión.
- Contenido completo para para su correcta visualización.	-Estudios que no esten en formatos aceptados como libros, cartas, entre otros.

Nota: Fuente propia

2.3. Material

Cumpliendo con el método de búsqueda bibliográfica se logró encontrar alrededor de 40 potenciales recursos bibliográficos, de los cuales 20 fueron los utilizados en el presente estudio.

3. Resultados Encontrados

3.1. Métodos de Propagación o Infección

Como primer paso en el estudio acerca del ransomware debemos conocer cómo es que este entra a nuestros sistemas de información, y para ello existen diversos métodos, que según

nos mencionan en (Moreno et al., 2020) estos métodos son: Redirección de Trafico, Adjuntos de correos, Botnets, Ingeniería Social, RAS (*ransomware as a service*) y Malvertisement.

3.1.1. Redirección de Trafico:

En (Moreno et al., 2020) mencionan que este tipo de propagación del ransomware consta de engañar a los usuarios por medio de publicidad falsas que tienen como fin redirigirlos hacia otras páginas que contengan el malware, también se menciona que generalmente este tipo de propagación se puede encontrar en sitios porno, que publicitan juegos o aplicaciones gratuitas, y que cuando el usuario descarga estos freeware y los instala, está instalando con ello el ransomware.

3.1.2. Adjuntos de correos*:*

Este método de propagación según nos comentan en (Moreno et al., 2020) consta de incitar al usuario a abrir documentos o links adjuntos a correos de fuentes confiables que fueron comprometidas, o de fuentes similares a las confiables, como facturas de servicios básicos, pago de impuestos o notificaciones legales. Una vez que el usuario ingresa al link o abre el documento adjunto, el ransomware entra al sistema del usuario.

3.1.3. Botnes:

Este tipo de propagación se da cuando un sistema ya comprometido distribuye el ransomware, esto se logra ya que los sistemas comprometidos llegar a descargar los ransomware en segundo plano (Moreno et al., 2020), adicionalmente este método de propagación permite que el atacante tenga acceso al sistema haciendo que todas las maquinas con el mismo botnet reciban las mismas instrucciones con un único servidor de comando y control(Lituma Briones, 2020).

3.1.4. Ingeniería Social:

Este método suele servir como complemento de otros tipo de métodos de propagación, ya que como menciona (Zamora Baidal et al., 2021) la práctica de este método consiste en poder conocer los intereses personales y los comportamientos de la víctima para poder asegurar el éxito de un ataque. Esta investigación que realiza el atacante se puede dar mediante herramientas tecnológicas o puede el atacante interactuar físicamente con la víctima, esto nos lo menciona (Campoverde Cabañarez, 2022), además menciona que la ingeniera social tiene como objetivo hacer uso del eslabón más débil de una organización.

3.1.5. RAS (*Ransomware as a Service*):

Este método de propagación es especial pues no es en sí una manera en la que los sistemas de la víctima son infectados si no es la manera en que los atacantes acceden a los Ramsomwares para infectar. En (Plaza González, 2021) se menciona que el ransomware como un servicio consta de la venta o alquiler de diversos tipos de ransomware a través de la dark web, lo peligroso de este tipo de propagación es que pone a disposición al ransomware no solo a expertos sino también a personas con poco conocimiento informático lo que genera una alta tasa de atacantes. Algo adicional que menciona (Plaza González, 2021) es que existen generalmente 3 entidades involucradas en este método, en primer lugar está el desarrollador del ransomware, en segundo lugar se encuentra el proveedor de servicios, y por ultimo está el atacante, quien recibe capacitación del desarrollador para poder maximizar las ganancias del ataque.

3.1.6. *MALVERTISEMENT:*

Este método según relata (Paredes Vargas, 2021) consiste en utilizar anuncios digitales para poder hacer ingresar los malwares al sistema víctima, en este caso estaríamos hablando de que mediante anuncios falsos el ransomware estaría ingresando al sistema informático de la víctima.

3.2. Tipos generales de Ransomware

De la gran cantidad de diferentes versiones de ransomware existentes, (Plaza González, 2021) menciona que se pueden agrupar en dos categorías según su fin, estas categorías son, los ransomware de bloque y los ransomware de cifrado.

3.2.1. Ransomware de Bloqueo

En (Plaza González, 2021) nos menciona que este tipo de ransomware tiene como objetivo inhabilitar todas las funciones del sistema infectado, dejando únicamente una ventana que informe del secuestro y del rescate que deberían pagar para poder acceder a sus sistemas. (Osorio Sierra, 2019) también incluye que este tipo de ransomware es considerado relativamente débil, pues no utiliza en ningún momento algún algoritmo de cifrado con los archivos del sistema por lo que la información de la víctima generalmente no corre riesgo de ser eliminada y se puede tratar de deshacer el bloqueo sin necesidad de pagar el rescate. Adicionalmente (Osorio Sierra, 2019) menciona que este tipo de ransomware logra su objetivo mediante la modificación del registro de arranque maestro o la modificación de la tabla de particiones del sistema víctima.

3.2.2. Ransomware de Cifrado

Este ransomware es mencionado por (Plaza González, 2021), quien dice que generalmente esta categoría de ransomware se ven presente en los ransomware actuales y su fin es el de poder cifrar los archivos de la víctima, usualmente estos archivos son buscados mediante sus extensiones alrededor de todo el sistema de archivos del equipo infectado. A diferencia del ransomware de bloqueo, con este ransomware los sistemas infectados aún son utilizables, sin embargo, toda la información que fue encriptado no será posible de visualizar y en su lugar se vera la nota de rescate por dicha información.

(Osorio Sierra, 2019) menciona que este tipo de ransomware utiliza algoritmos criptográficos simétricos y asimétricos con el fin de encriptar la información de la víctima, también añade que anteriormente la clave de la encriptación era guardada en el mismo sistema infectado por lo que realizando ingeniería inversa, era posible solucionar el problema y desencriptar la información, no obstante, actualmente ya no se guarda en el mismo sistema, sino que utilizan servidores web para recepcionar las claves. Otro de los avances más peligrosos de este tipo de ransomware es que actualmente algunos optan por dar un tiempo límite para pagar el rescate de lo contrario eliminarían la información encriptada.

3.3. Funcionamiento General del Ransomware (modus operandi)

El funcionamiento del ransomware puede ser divido en varios bloques dependiendo del enfoque que le dé el autor, en consideración de ello se utilizara la división del ciclo de vida del ataque de ransomware dada en (Osorio Sierra, 2019).

3.3.1. Despliegue

En (Bazante Veloz et al., 2019) mencionan que esta etapa consiste en poder introducir el ransomware dentro del sistema víctima, para esto pueden usar distintos métodos de propagación o infección. Estos métodos fueron explicados en el punto anterior. En (Osorio Sierra, 2019) menciona que además esta etapa tiene un elemento muy importante que se conoce como ENTREGA, que se puede definir como el mecanismo usado por el atacante para introducir al ransomware.

3.3.2. Instalación – Propagación

En (Bazante Veloz et al., 2019) se menciona que cuando el ransomware ya está dentro del sistema de la víctima, este puede entrar en espera hasta cierto evento que desencadene su ejecución, este evento puede ser por el apagado, reinicio o encendido del sistema, también la apertura de algún programa puede desencadenar en la ejecución del ransomware. En (Osorio

Sierra, 2019) se menciona que después de ejecutarse el ransomware comienza a realizar los preparativos para poder instalarse correctamente, ya sea instalando las librerías que necesite o agregando tareas para que su funcionamiento sea automático.

3.3.3. Centro de comando y control

Como se menciona en (Bazante Veloz et al., 2019), en este segmento se busca poder establecer una comunicación con los servidores del atacante, para que estos puedan obtener las claves de cifrado o bloqueo del sistema, estas sirven para poder posteriormente desencriptar o desbloquear el sistema de la víctima. En (Osorio Sierra, 2019) se menciona que este punto se logra efectuar gracias a que se utilizan mecanismos de explotación o infección para poder utilizar las vulnerabilidades del sistema de la víctima, se mencionan dos ejemplos de estos mecanismo, el RAT y los Exploit Kit que cumplen con estos propósitos.

3.3.4. Destrucción

A esta etapa se le llama destrucción porque aquí se llega a cumplir el objetivo del ransomware, es decir se logra encriptar la información crítica de la víctima o bien bloquear el sistema por completo de la víctima. Para el caso del bloqueo (Bazante Veloz et al., 2019) menciona que el ransomware logra inhabilitar el acceso a la pantalla de la víctima, privándola de poder realizar cualquier función, un ejemplo del cómo puede lograr esto es modificando el Master Boot Record, según menciona el autor. Además, con la etapa anterior logra comunicarse con los servidores del atacante para poder enviarle la clave de desbloqueo del sistema. En (Osorio Sierra, 2019) mencionan que para el caso de un ransomware de encriptación, lo primero que se realiza es la búsqueda de los archivos que se quieren encriptar, la búsqueda se realiza sobre todos los documentos locales que tenga el sistema, así como también sobre los documentos compartidos en red, dándole prioridad a estos últimos. Una vez completado la búsqueda de los archivos, el ransomware se pone en contacto con el servidor del atacante para poder enviar la clave de cifrado, confirmándoles que el ataque fue exitoso. Adicionalmente ciertos ransomware tienen la capacidad de poder eliminar las copias de seguridad que se tengan en el sistema de la víctima para evitar que se restaure a un estado previo al ransomware.

3.3.5. Extorsión

Esta etapa según nos menciona (Bazante Veloz et al., 2019), consiste en hacerle presente a la víctima sobre el estado de sus archivos o bien del sistema en sí, para el caso de los ransomware de bloqueo. Para esto dejan una nota en el sistema, en el caso del ransomware de encriptación, la nota generalmente está en el mismo lugar que los archivos encriptados, y para el caso de los ransomware de bloque es lo único que puede visualizar la víctima, pues su sistema está inhabilitado. El autor también menciona que en esta nota se solicita el pago del rescate que generalmente es en bitcoins ya que las transacciones de esta criptomoneda son anónimas, por lo que no se podrá conocer al atacante. Finalmente, algo que el autor deja en claro es que pagar el rescate no garantiza que los atacantes desencripten o desbloqueen el sistema que fue víctima.

3.4. Ramsomwares Específicos

En este apartado se mencionará algunos de los ransomware más conocidos o usados.

3.4.1. WannaCry

En (Ezequiel Sena, 2018) nos menciona que este ransomware vio la luz en el año 2017, donde llego a afectar más de 200 mil ordenadores, repartidos en 150 países, esta gran propagación causo gran revuelo en esa época, puesto que como objetivos tenía a empresas, colegio y hospitales. Esta gran propagación se debió a que este ransomware a diferencia de

anteriores ransomware, no solo buscaba encriptar, sino que también tenía un módulo especializado en infectar y propagarse, llamándose modulo worm. Su funcionamiento iniciaba una vez que el módulo worm haya sido incrustado en un sistema por cualquier método, después de esto el módulo worm trataba de instalar en el sistema donde se encontraba su segundo modulo que tiene como nombre modulo ransomware, que era el especializado en encriptar. Con el segundo modulo instala este ransomware empezaba sus ciclo, buscando todos los archivos que debía encriptar, para mandar a los atacantes la clave del encriptado y mostrar a la víctima la ventana de rescate. El peligro más grande de este ransomware se da cuando termina de encriptar se vuelva a activar su modulo worm para buscar las direcciones IP que puedan ayudarlo a replicarse y conseguir nuevas víctimas.

3.4.2. CryptoWall

En (RUIZ, 2020) se menciona que este ransomware generalmente llega a un sistema de información mediante correos electrónicos de dudosa procedencia o cuando se descarga algún archivo fraudulento, en este último lo que hace el ransomware es pedirle a la víctima que actualice algún programa, como puede ser un reproductor de video para poder infiltrarse completamente en el sistema de la víctima. Una vez dentro continua con su ciclo de ataque, encriptando todos los archivos que se encuentren en el sistema, y mandando la nota de rescate a la víctima para que pueda hacer el pago.

3.4.3. TeslaCrypt

En (Andrade Valdez & Galarza Zurita, 2019) se menciona que este ransomware fue visto por primera vez en el año 2015, además este ransomware es del tipo de encriptado, ya que su principal objetivo es encriptar archivos del sistema de su víctima, sin embargo, este ransomware tenía la peculiaridad de que afectaba principalmente a video jugadores ya que los archivos en los que enfocaba para encriptar eran videojuegos, perfiles del juego o partidas grabadas. Actualmente este ransomware fue actualizado y ya puede encriptar archivos con extensiones como son .doc, .jpg, .png entre algunas más. También menciona que este ransomware hace uso del algoritmo de encriptación AES-256 y que generalmente se distribuye por correos spam, que contienen archivos ejecutables maliciosos.

3.4.4. CTB-Locker

El autor (ORDUZ BARRERA, 2018) menciona que este ransomware ingresa a los sistemas de las victimas mediante correos electrónicos que contengan algún troyano que al momento de ingresar en el equipo de la víctima permita a un tercero ingresar a descargar directamente este ransomware sin ser detectado por la víctima. Este ransomware una vez instalado y ejecutado procede a encriptar todos los archivos que buscaba para poder mostrarle a la víctima la ventana de rescate. Además, se menciona que el país de Colombia era el sexto más afectado por este tipo ransomware hasta el año 2018. Una particularidad de este tipo de ransomware es que por cada víctima genera un código de transacción bitcoin diferente, es decir que cada víctima tenía su propio código de pago para el rescate, esto hacia más difícil de detectar con anticipación a este tipo de ransomware.

3.4.5. CryptoLocker

En (Danny et al., 2020) se menciona que este ransomware fue lanzado el año 2013 y que en ese mismo año se lanzó su versión mejorada. En primer instancia este ransomware entraba por correo electrónico a través de ejecutables, y que inmediatamente ingresaba escaneaba y encriptaba los archivos necesarios. En su versión mejorada este ransomware implemento el uso de C# y la red TOR que servía para mejorar el anonimato del ransomware haciéndolo en ese entonces indetectable ante antivirus o firewalls. El algoritmo que utilizaba para cifrar los archivos era el RSA de 2048 bits, y además en esta versión se empleó en el rescate que el pago sea mediante bitcoins.

3.4.6. Locky

Este ransomware es mencionado en (Ezequiel Sena, 2018) donde dicen que apareció por primera vez en el año 2016, trayendo consigo un gran revuelo, ya que a diferencia de otros tipos de ransomware este analizaba el valor de los archivos que encriptaba asignando un precio de rescate particular a cada víctima. En un inicio este ransomware era propagado mediante correos con archivos corrompidos, generalmente en formato Word o Excel, pero con el paso del tiempo fue actualizado y ahora generalmente utiliza archivos comprimidos. Este ransomware opera de una manera que lo hace imposible de desencriptar manualmente, pues en un inicio utiliza su conexión a un servidor C&C para contactar al atacante la correcta infiltración en el sistema de la víctima, con esto el atacante envía una clave publica RSA de 2048 bits y con eso, el ransomware utiliza el algoritmo desencriptación AES. Con la infección finalizada el ransomware avisa a la victima de su estado, pidiéndole un rescate por la información.

3.4.7. Cerber

En (Andrade Valdez & Galarza Zurita, 2019) se menciona que este ransomware a diferencia de otros, tiene una gran gama de versiones, esto debido a sus constantes actualizaciones y que es cualquier persona pueda crear su propia versión, sin embargo, parte del dinero entregado como rescate siempre se dirige a los creadores originales del ransomware. Este hecho hace que el método de propagación de ransomware sea muy variado. Una particularidad de este tipo de ransomware es que puede analizar los archivos y seleccionar aquellos más importantes para ser priorizados al momento de encriptar, además esta encriptación puede realizarla en cualquier maquina infectada sin necesidad de que este conectada a internet. Los archivos comprometidos por este ransomware tienen la extensión. cerber, adicionalmente este ransomware al igual que la mayoría pide el rescate mediante transacciones de bitcoin.

3.4.8. Crysis

En (Andrade Valdez & Galarza Zurita, 2019) *se mencion*a que este ransomware está dentro de los 5 ransomware con mayor incidencia de ataque en Latinoamérica hasta el año 2019. Su método de propagación es por medio de archivos ejecutables maliciosos, una vez dentro del sistema de la víctima procede a encriptar todos los archivos que necesite y para ello usa una fusión entre los algoritmos RSA y AES que lo hace prácticamente imposible de desencriptar sin la clave de encriptación.

3.4.9. Jigsaw

En (MOLANO ARTUNDUAGA & VERNAZA ARBOLEDA, 2021) se menciona que este ransomware recibió este nombre en el año 2016, ya que utilizo imágenes de la franquicia de películas Saw, lo que hace particular además de ello a este ransomware es que por cierto tiempo que la víctima se rehusé a pagar el rescate elimina parte de los archivos encriptados. Otra cosa que menciona el autor es que el uso de estas imágenes sirvió para poder generar cierta angustia o preocupación extra en las victimas de este ransomware.

3.5. Consecuencias del Ransomware

Los ransomware tienen distintos grados de consecuencias dependiendo de a quién o a que sistema infecte, algunos ejemplos de grande eventos ocurridos debido a este tipo de malware son la batalla por Atlanta ocurrido debido al ransomware SamSam y Baltimore contra el ransomware RobinHood (Vielma Montañez, 2022) .

3.5.1. Batalla por Atlanta

En (Vielma Montañez, 2022) se menciona que este evento se desarrolló en el año 2018, donde la ciudad de Atlanta detuvo sus actividades de un momento a otro, esto se debió a que

fue víctima de un ataque de ransomware, llamado SamSam, el cual logro deshabilitar gran parte de los sistemas administrativos de las oficinas del ayuntamiento, además de también inhabilitar a distintos departamentos. Esto ocasionó que las actividades se realicen de forma manual, cosa que debido a la carga era completamente difícil, el rescate pedido por este ransomware fue de 51 mil dólares. La ciudad de Atlanta por recomendación del Buro federal no pago el rescate y realizo la reactivación de todos sistemas desde cero, llegando a demorar un mes en volver a poner los servicios en orden y costando todo esto cerca de 12 millones de dólares.

3.5.2. Baltimore contra el ransomware RobinHood

Según (Vielma Montañez, 2022) este ataque se dio en el año 2019, donde la principal víctima fue la ciudad de Baltimore y el atacante fue el ransomware conocido como RobinHood. Este ataque hizo que la ciudad tuviese que crear de cero las credenciales para cerca de 10 mil empleados, además de tener que restablecer manualmente cada uno de los sistemas. Esto afecto a la población ya que, al no contar con sus datos, las operación administrativas que normalmente se hacían por internet no funcionarán, haciendo que gran parte de estas operaciones se realicen manualmente. Al igual que en el caso anterior a esta ciudad se le recomendó no pagar el rescate que ascendía a 70 mil dólares, esto se debe a que nada garantiza que el pagar el rescate libere los datos. Todas las operaciones que realizo la ciudad por culpa de este ataque costo alrededor de los 18 millones de dólares ya que también debieron restablecer los servicios locales.

3.6. Técnicas de Prevención del Ransomware

No solo es importante conocer el cómo funcionan o que tipos de ransomware existen sino también es importante conocer el cómo podemos evitarlos, y para ello se describirán algunas técnicas que ayudan a prevenir ser víctimas de este tipo de malware.

3.6.1. Educar a los empleados sobre cómo evitar infecciones de ransomware

En este punto (PEREZ CASTRO, 2021) nos menciona que es importante darles conocimientos a los empleados sobre qué tipo de peligros puede haber en la red, esto ya que el eslabón más débil de toda organización siempre es el empleado o usuario, ya que sin importan que tan buena sean las herramientas que garanticen la seguridad de la organización, una mala ejecución por parte del empleado o usuario puede dejar a la organización vulnerable. (Barker et al., 2022) menciona 3 puntos que se debe tener en cuenta el empleado o usuario de la organización, primero, no abrir ni hacer clic sobre archivos o enlaces cuya procedencia es desconocida, ya que estos pueden redirigir a sitios altamente peligrosos, segundo, evitar en la medida de lo posible hacer uso de sitios web personales o aplicaciones ajenas al trabajo en equipos de la organización, ya que por estos medios pueden ingresar el ransomware, por último se menciona que no se deben conectar dispositivos propios o que no se conozca su procedencia, pues estos tienen una alta probabilidad de esta infectados.

3.6.2. Analizar los correos electrónicos

(PEREZ CASTRO, 2021) menciona que es importante que una organización cuente con su propio servicio de correo electrónico ya que se puede tener un mejor control acerca de qué tipo de correos entran y salen de la organización. Además, menciona que siempre se debe tener en cuenta 3 aspectos antes de abrir cualquier correo, primero, si se conoce al remitente, segundo, preguntarse acerca de la necesidad de ingresar a un archivo o enlace enviado por correo, por último, acerca si se tuvo alguna comunicación con el remitente para que justifique su correo.

3.6.3. Implementar estrategia de privilegios mínimos

En (PEREZ CASTRO, 2021) se menciona que se debe tener en consideración la cantidad de usuarios y que tipo de privilegios tienen, pues lo ideal sería tener la cantidad justa

de usuarios y que cada uno de ellos cuente con los permisos estrictamente necesarios. De esta manera se busca que en caso ingrese algún tipo de ransomware, este solo infecte lo mínimo posible debido a que el usuario infectado solo contara con permisos mínimos.

3.6.4. Actualizaciones de seguridad

(PEREZ CASTRO, 2021) menciona que para evitar infecciones de ransomware es recomendable siempre tener los programas o sistemas actualizados a su última versión, esto debido a que las actualizaciones generalmente se dan para parchear ciertas vulnerabilidades que se descubrieron, y si no se tiene las actualizaciones necesarias los cibercriminales pueden aprovechar estas vulnerabilidades para infectar de ransomware a la organización.

3.6.5. Respaldar la información

(PEREZ CASTRO, 2021) menciona que para poder minimizar las consecuencias después de un ataque de ransomware siempre es bueno tener copias de seguridad de la información, es decir que se recomienda hacer respaldos de la información periódicamente, y entre más cerca el tiempo entre respaldos, menos serán los datos que se pierdan después de un ataque. Además, estos respaldos deben estar separados de las maquinas en dispositivos externos para evitar infectarse en caso de un ataque de ransomware.

4. Análisis de las preguntas de investigación

4.1. Análisis sobre las acciones para prevenir ser víctimas de ransomware

Una vez que el ransomware ingresó al sistema de información, hay muy poco que hacer pues actualmente los procesos de encriptación son prácticamente imposibles de desencriptar sin conocer la clave de encriptación, por lo que la mejor manera de hacerle frente a este malware es preparando medidas que hagan disminuir la posibilidad de poder infectarse de ransomware, por ello se habló de ciertas medidas preventivas, siendo las más importantes realizar respaldos de información que logran disminuir el efecto que puedan traer ser víctimas de ransomware, otra medida con gran importancia es capacitar a los empleados sobre un correcto uso de los sistemas para evitar entrar en contacto con potenciales fuentes de infección, esto se considera de suma importancia pues generalmente el ransomware ingresa por algún fallo en el uso de los sistemas por parte de los empleados.

4.2. Análisis de la importancia de conocer al ransomware

Con toda la información obtenida se puede validar la gran importancia que representa el conocer cómo se puede uno infectar con ransomware, ya que con esta información es mucho más sencillo poder tomar medidas preventivas que ayuden a no padecer de este problema. También se pudo observar que tan grave puede llegar a ser el ransomware si es que infecta organizaciones cruciales para el correcto desarrollo de la vida cotidiana de la población.

5. Conclusiones

Con respecto a la siguiente investigación realizada se desarrolló las siguientes conclusiones:

Con toda la información encontrada y revisada se puede conocer cómo es que funciona el ransomware desde el cómo existen varios métodos de infección, hasta que tipo de acciones se pueden realizar para minimizar o prevenir daños ocasionados por un ataque de ransomware.

En esta investigación se pudo conocer la importancia de tener presente la existencia del ransomware, así como que tan grave puede llegar a ser un ataque, por lo que se podría dar paso

a una investigación acerca de posibles soluciones o medidas para contrarrestar el ransomware en ejecución.

6. Referencias

Andrade Valdez, J. A., & 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*. 215. https://bibdigital.epn.edu.ec/handle/15000/19922

Barker, W. C., Fisher, W., Scarfone, K., & Souppaya, M. (2022). Gestión de riesgo de ransomware: un perfil de marco de ciberseguridad. *National Institute Of Standards and Technology. U.S. Department of Commerce, NISTIR 837*.

Bazante Veloz, F. D., Barona López, L. I., Valdivieso Caraguay, Á. L., & Hernández Álvarez, M. B. (2019). Indicadores para la detección de ataques ransomware. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E19*, 493–506. https://search.proquest.com/openview/841aa93ba3c3df451268e843ef187b70/1?pq-origsite=gscholar&cbl=1006393

Campoverde Cabañarez, L. M. (2022). *Implementación de técnicas en ingeniería social en un gobierno autónomo descentralizado de la provincia de Santa Elena*. https://repositorio.upse.edu.ec/handle/46000/7726

Danny, V., Francisco, B., & Navira, A. (2020). EXPLORATORY STUDY OF STRATEGIES FOR PROTECTING CORPORATE NETWORKS OF RANSOMWARE INFECTIONS. *Revista Científica Multidisciplinaria Arbitrada YACHASUN*, *4*(7), 71–87. https://doi.org/https://doi.org/10.46296/yc.v4i7.0035

Ezequiel Sena, M. (2018). *Criptografía maliciosa: Ransomware*. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1304_SenaME.pdf

Infante-Moro, A., Infante-Moro, J. C., & Gallardo-Perez, J. (2022). Factores claves para concienciar la ciberseguridad en los empleados. *Revista de Pensamiento Estratégico y Seguridad CISDE*, *7*(1), 69–79.

Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering - A systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Lituma Briones, L. C. (2020). *Laboratorio virtual de análisis y comportamiento de malware basado en técnicas y métodos de seguridad informática para los laboratorios en la facultad de Sistemas Y Telecomunicaciones*.

MOLANO ARTUNDUAGA, E. D., & VERNAZA ARBOLEDA, E. (2021). *MONTAJE DE UN AMBIENTE CONTROLADO UTILIZANDO RANSOMWARE Y APLICANDO HERRAMIENTAS DE SEGURIDAD QUE PERMITAN DETECTAR LAS VULNERABILIDADES DE LA INFORMACIÓN IMPLICADA*. https://repository.unad.edu.co/handle/10596/42038

Moreno, J., Rodriguez, C., & Leguias, I. (2020). Revisión sobre propagación de ransomware en sistemas operativos Windows. *I+D Tecnológico*, *16*(1), 39–45. https://doi.org/https://doi.org/10.33412/idt.v16.1.2438

ORDUZ BARRERA, D. M. (2018). *ANÁLISIS DE EMERGENCIAS CIBERNÉTICAS QUE SE PRESENTAN EN LAS CIUDADES DE TUNJA, DUITAMA Y SOGAMOSO CON RESPECTO AL RESTO DEL PAÍS EN LOS ÚLTIMOS 2 AÑOS*. https://repository.unad.edu.co/handle/10596/31410

Osorio Sierra, A. F. (2019). *Esquema metodológico apoyado en una herramienta (software)*

para la detección y prevención de Crypto Ransomware en una estación de trabajo Esquema metodológico apoyado en una herramienta (software) para la detección y prevención de Crypto Ransomware en. http://hdl.handle.net/20.500.12622/1391

Paredes Vargas, C. L. (2021). *Oportunidades de mejora detrás de la principal preocupación del sistema financiero: fraudes informáticos*. http://hdl.handle.net/10654/39412

PEREZ CASTRO, J. C. (2021). *ESTUDIO MONOGRÁFICO SOBRE LA AMENAZA RANSOMWARE, SU IMPACTO EN LAS ORGANIZACIONES Y BUENAS PRÁCTICAS PARA SU PREVENCIÓN Y MANEJO*. https://repository.unad.edu.co/bitstream/handle/10596/42143/jcperezca.pdf?sequence=1&isAllowed=y

Plaza González, M. (2021). *Análisis de un ataque Ransomware. Desarrollo del ransomware Gengar*. 80. http://diposit.ub.edu/dspace/bitstream/2445/182628/3/tfg_marcos_plaza_gonzalez.pdf

Riega Virú, Y., Huamani Chirinos, H. L., & Machuca Vílchez, J. A. (2021). Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú. *Lex - Revista De La Facultad De Derecho Y Ciencias Políticas*, *19*(28), 197–236. https://doi.org/10.21503/lex.v19i28.2318

RUIZ, J. C. (2020). *ANALISIS MONOGRAFICO DE LA PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA*. https://repository.unad.edu.co/handle/10596/36760

Vielma Montañez, A. (2022). *EL RANSOMWARE Y LA CULTURA DE SEGURIDAD*. UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN.

Zamora Baidal, D., Triviño, A., Puris Cáceres, A. Y., Zhuma Mera, R. E., & Oviedo Bayas, B. (2021). Análisis y técnicas de prevención ante ataques ransomware. *Revista Tecnológica Ciencia y Educación Edwards Deming*, *5*(1), 98–108. https://doi.org/10.37957/ed.v5i1.72