InterSedes, *Revista electrónica de las sedes regionales de la Universidad de Costa Rica*,
ISSN 2215-2458, Volumen XXIV, Número 49, Enero-Junio, 2023.
10.15517/isucr.v24i49 | intersedes.ucr.ac.cr | intersedes@ucr.ac.cr

Ransomware, una amenaza latente en Latinoamérica

Ransomware, a latent threat in Latin America

Fredy Yesid Ávila Niño
Escuela de Policía Rafael Reyes
Santa Rosa de Viterbo, Boyacá,
Colombia
segundo.avila@correo.policia.gov.co

Resumen: En el presente artículo se evidencia que los ataques de ransomware en América Latina se han convertido en una de las ciber amenazas más importantes y a su vez más peligrosas para las organizaciones y usuarios en genera. Inicialmente se realizó una revisión bibliográfica y de casos relevantes ocurridos, lo que permitió recopilar información para determinar su evolución e impacto desde el año 2015. En esta fase se logró entender este concepto y sus características, posteriormente se identificaron los vectores de ataque y metodologías que utilizan los atacantes. Esto contribuyó a identificar los tipos de ransomware que han aparecido en los últimos años para así describir los métodos de infección que se utilizan por parte de los ciber criminales. Al reconocer el comportamiento de este malware y las tendencias asociadas a esta amenaza, se generan recomendaciones que permiten orientar a las organizaciones y a las personas para que eviten ser víctimas de ataques de este tipo, lo que constituye una contribución para mitigar este tipo de riesgo.

Palabras clave: Información, cibercrimen, delito informático, seguridad de los datos, protección de los datos, cibernética

Abstract: This article shows that Ransomware attacks in Latin America have become one of the most important and dangerous cyber threats for organizations and users in general; This according to the security report latinoamerica 2021 by antivirus company ESET, for this reason initially a literature review was conducted and relevant cases occurred, which allowed gathering information to determine its evolution and impact since 2015, likewise in this phase it was possible to understand this concept and its characteristics, then the attack vectors and methodologies used by the attackers were identified, this contributed to identify the types of Ransomware that have appeared in recent years to describe the methods of infection that are used by cyber criminals. By recognizing the behavior of this malware and the trends associated with this threat, recommendations are generated to guide organizations and individuals to avoid becoming victims of attacks of this type, which constitutes a contribution to mitigate this type of risk. This document is obtained from the research carried out in the development of the degree work: "EVOLUTION AND IMPACT OF RANSOMWARE IN LATIN AMERICA SINCE 2015".

Keywords: information, cybercrime, computer crime, data security, data protection, cybernetics

Recibido: 12-04-22 | Aceptado: 28-06-22

Cómo citar (APA): Ávila Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. InterSedes, 24(49), 92-119.

Publicado por la Editorial Sede del Pacífico, Universidad de Costa Rica

1. Introducción

Como su nombre lo indica, *ransomware* es un: "malware bastante interesante que, después de infectar el sistema, bloquea algunos recursos populares e importantes del sistema informático y luego exige dinero de rescate para devolver el acceso" (Chauhan & Kumar, 2015). Por lo general, los *ransomwares* utilizan tecnologías de cifrado para mantener los datos cautivos, como muestra de esto, el 12 de mayo de 2017 el ámbito empresarial en el mundo vivió un día muy complicado, ya que se vio impactado por un ciberataque que se produjo a nivel global. En principio se señaló que los atacantes produjeron alrededor de 80.000 incidentes, que afectaron a personas físicas y jurídicas de más de setenta países (Sobrino, 2018). Posteriormente, los medios determinaron que en realidad se habían producido 130.000 ataques y que los mismos habían ocurrido en cien países. El *ransomware*, en sus inicios fue pensado para atacar a las organizaciones, pero ahora los ciber criminales han diseñado diferentes variantes que pueden afectar a personas comunes, en diferentes plataformas y dispositivos.

Con la masificación de las tecnologías y el acceso a la red por parte de los usuarios, este ataque encuentra nuevas oportunidades para causar daño a las organizaciones y usuarios, ya que a la par de los avances tecnológicos y avances en cuanto a seguridad, el *Ransomware* también se adapta al entorno. Esto dio pie a la aparición de tres categorías: *ransomware* que cifra archivos, *ransomware* de pantalla de bloqueo y *ransomware* para dispositivos móviles.

En el primer caso, una vez es infectado el equipo, los archivos son cifrados para dejarlos inaccesibles al usuario, al mismo tiempo que se establece comunicación con el atacante a través de la red TOR y se exige transferencia de dinero o criptomonedas por descifrar los archivos. En el segundo caso, el objetivo de este tipo de *ransomware* es dejar inutilizable el sistema operativo de la víctima, para que sea posible tener control nuevamente de su máquina se debe realizar un pago al atacante. Por último, esta variante tiene la capacidad de llevar esta amenaza a otro tipo de dispositivos.

Es necesario reconocer los métodos de infección que son utilizados por los atacantes. En este punto la creatividad del atacante cumple un papel muy importante, dado que siempre se buscan nuevas formas de infectar para no levantar sospechas en el usuario

final. No obstante, existen cuatro métodos comúnmente usados, los cuales son: Troyanos, *Spear Phishing*, Escritorio Remoto y Móviles Android.

América Latina en los últimos años se ha visto afectada por los ciber criminales que lideran campañas de difusión de *ransomware*, puesto que organizaciones y personas ante las autoridades de cada país con mayor frecuencia reportan incidentes relacionados y cada vez el impacto es mayor. Por estas razones, se propone un compilado de buenas prácticas que les permitan a empresas y personas evitar ser víctimas de esta modalidad de ciber delito. El objetivo de este artículo es identificar cómo ha sido la evolución y el impacto del *ransomware* en América Latina, para generar recomendaciones que orienten a las organizaciones para evitar ser víctimas de este tipo de ataque. Con lo que se busca responder la pregunta problema: ¿Cuál ha sido la evolución e impacto del *ransomware* en América Latina desde el año 2015?

El *ransomware* se mantiene como uno de los ataques preferidos por los ciber-criminales. Esta modalidad criminal, con la que "se secuestra información de una compañía, Gobierno o usuario para cobrar un rescate, tiene en alerta al continente americano, ante una ola de ataques que ha puesto a prueba sus relativamente inmaduros sistemas de ciberseguridad" (Forbes, 2022).

Se ha logrado evidenciar que es posible obtener gran beneficio si el ataque consigue afectar a empresas o entidades de gobierno que aún no cuentan con planes de contingencia o contramedidas ante ataques cibernéticos de este tipo, ante los cual queda como única opción pagar el rescate de la información. Frecuentemente, se habla de *ransomware* y de todas las precauciones a tener en cuenta para evitar ser víctima de este tipo de ataque, sin embargo, se siguen presentando casos y siguen en producción nuevas variantes de este tipo de *malware*.

Un aspecto que ha dejado en evidencia el *ransomware* es que las organizaciones aún no comprenden la importancia de la implementación de políticas de seguridad, la gestión de copias de seguridad y mejores prácticas en cuanto a la administración de información. Esta situación a nivel latinoamericano ha llamado la atención de los atacantes.

La tendencia con respecto al *ransomware* es evolucionar y hacerse más sofisticado. Este programa maligno aprovecha las vulne-

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

rabilidades activas en los sistemas operativos, implementa funciones que deshabilitan servicios, incluso logra reiniciar la máquina en modo seguro con el fin de evadir la protección, lo que exige un mayor grado de protección y una mejor implementación de la gestión de la seguridad.

Según información publicada por DarkTracer, compañía considerada como líder mundial en tecnología de seguridad cibernética y que se dedica, entre otras cosas, a monitorear la actividad de los grupos de *ransomware* en la Dark web, en la ventana de observación fijada desde el 1 de enero de 2019 al 9 de noviembre de 2021, un total de 53 bandas de *ransomware* afectaron a 3.767 organizaciones. Para comprender y contextualizar de mejor manera estas cifras, entre 2019 y 2020, un total de 22 grupos de *ransomware* afectaron a 1.315 organizaciones. En 2021 se registraron más de 2.452 organizaciones afectadas por ataques de este tipo; una cifra superior a los 1.315 que se registraron sumando los dos años previos y que refleja el crecimiento en la cantidad de víctimas (Ramírez Duque, 2022).

En el año 2020 se registraron 1.498 familias y variantes de *ransomware*, que equivale a un 5,5% de aumento con respecto al año 2019. Los países con mayor cantidad de detecciones de *ransomware* a nivel de empresas en Latinoamérica durante 2020 fueron Perú (30%), seguido por México (14,9%), Venezuela (13,2%), Brasil (11,3%) y Colombia (7,9%) (Eset, 2021).

Muchas empresas no realizan de forma adecuada la gestión de actualizaciones o una verificación periódica de vulnerabilidades en todos sus sistemas, ya que, como se ha mencionado anteriormente, una máquina infectada puede propagar el programa maligno en otras máquinas bajo la misma red. Para evidenciar aún más esta problemática, basta con realizar la búsqueda en *shodan* (motor de búsqueda de dispositivos en la red) de sistemas que aún tienen activa la vulnerabilidad *eternalblue* (vector de ataque de *wannacry*). Lo que se obtiene, es que, a pesar de conocer la vulnerabilidad y la medida para mitigarla, todavía son bastantes los sistemas vulnerables, casi tres años después de que la campaña de *Ransomware wannacry* fuera lanzada.

Aunque muchas personas aún piensan que el *ransomware* es problema exclusivo de sistemas operativos *Windows*, los ciber-criminales han producido versiones que apuntan a diferentes siste-

mas, como el caso de LILU, el cual tiene como principal objetivo infectar servidores basados en Linux. Otras variantes conocidas son: Erebus y JungleSec, que también apuntan a servidores Linux. Para el caso de los sistemas MAC, se encuentran FileCoder, KeRanger y Patcher.

Por otra parte, los dispositivos móviles también cuentan con cepas que los afectan, para Android se conocen entre otros, Android/Filecoder.C, DoubleLocker y Lockerpin; para IOS FileCoder, y Mabouia. La actividad del *ransomware* no da muestras de parar, por el contrario, evoluciona y afecta múltiples plataformas, cada vez causando afectaciones más graves. El *ransomware* es un problema creciente, puesto que es dinero fácil para el crimen organizado que busca apuntar a grandes organizaciones y siempre hay personas dispuestas a pagar. Sobre este asunto, "algunos autores o grupos de ransomware aceptan pagos a través de PayPal, pero tienden a exigir más dinero, para compensar los gastos adicionales que deben tomarse para asegurar las identidades de los ladrones" (Allsopp, 2017).

Con lo anteriormente mencionado, se hace necesario conocer cómo ha sido la evolución e impacto de los ataques de *ransomware* en América Latina, con el fin de identificar las causas o factores que hacen de este ataque una amenaza latente para las organizaciones y personas, e identificar las medidas que se han implementado para mitigar este riesgo. Esto contribuye a compilar buenas prácticas y recomendaciones para evitar que se presenten nuevas víctimas.

2. Referente teórico

Todo aquel programa que tenga como objetivo causar daño infiltrándose en un sistema de información, sin la autorización del propietario del sistema, es conocido como *malware*, una vez este software malicioso es ejecutado, toma control del sistema, de la información o los datos (secuestra) y a cambio el atacante exige un pago (rescate) para poder tomar control nuevamente de su máquina. A esto se le conoce como *ransomware*. Lo anterior permite establecer un concepto simple para definir esta amenaza, cuyo crecimiento se mantiene constante. Normalmente se cifran los archivos con una clave única, la cual solamente el creador del

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

ransomware conoce y si la victima realiza el respectivo pago también la puede conocer. El Instituto Nacional de Ciberseguridad de España, lo define como

> un tipo de malware que hoy en día se está propagando de forma muy activa por internet. Este programa maligno impide el acceso y amenaza con destruir los documentos y otros activos de las víctimas si estas no acceden a pagar un rescate. (INCIBE, 2020. p. 4)

Generalmente ese rescate se paga en criptomoneda. La extorsión basada en datos ha existido aproximadamente desde el año 2005, pero el desarrollo del software de cifrado de rescate y criptomonedas ha tenido una gran influencia.

Kim Zetter, publicó el artículo: *4 Ways to Protect Against the Very Real Threat of ransomware*, en donde se hace referencia a que los ataques de *ransomware* en computadores son comunes, "pero este ataque ha evolucionado para atacar y afectar teléfonos móviles" (2016) mediante el cambio de PIN del dispositivo, con el fin de solicitar un rescate para obtener el nuevo PIN. También señala que pagar el rescate no es garantía de que se proporcionará la clave de descifrado.

Por otra parte, este ataque se divide en dos tipos básicos, tal y como se manifiesta en el informe técnico de Symantec, *The Evolution of Ransomware*. "El tipo más común es el Cripto-Ransomware, que cifra archivos y datos; el segundo tipo es el locker-Ransomware" (Savage, Coogan & Lau, 2015), versión que bloquea el computador u otro dispositivo, evitando que las víctimas lo puedan usar. Haciendo más extensa la explicación de cada tipo, en el informe se indica que el *Locker Ransomware* solamente bloquea el dispositivo, los datos que se encuentran almacenados en el dispositivo, normalmente no se han tocado. Como resultado, si el *malware* es eliminado, los datos permanecen intactos. Incluso si no es posible eliminar el programa maligno, los datos posiblemente se pueden recuperar moviendo el dispositivo de almacenamiento, generalmente un disco duro, a otro equipo en funcionamiento. Esto hace que este tipo de *ransomware* sea mucho menos efectivo para extorsionar a las víctimas.

Además, el *Crypto Ransomware* encripta los datos, por lo que incluso si el *malware* se elimina del dispositivo o el medio de almacenamiento se mueve a otro dispositivo, no será posible acce-

der a los datos. Normalmente, no se dirige a archivos críticos del sistema, lo que permite que el dispositivo continúe funcionando a pesar de ser infectado; después de todo, el dispositivo podría ser necesario para pagar el rescate.

En cuanto a los medios de pago, Zetter comenta que, entre finales de los 90 hasta el 2005, los métodos de pago en línea no eran comunes, ni estaban disponibles, de modo que las víctimas para pagar rescates utilizaban mensajes de texto SMS o enviando tarjetas prepagas por correo (2016). Otro pago común consistía en hacer que la víctima llamara a un número de teléfono de tarifa premium que generaba ganancias para el atacante.

No obstante, los métodos de pago mencionados anteriormente se consideran de alto riesgo, ya que un investigador determinado podía rastrearlos hasta el atacante. Rosenberg, en su artículo *About the malicious software known as Ransomware*, en donde se considera que el auge del *ransomware* realmente se dio cuando, en el año 2008, *Bitcoin* entró en vigor (2020). Las criptomonedas son divisas electrónicas, lo que hace mucho más difícil rastrearlas y, por lo tanto, ayudan a que las transacciones sean anónimas.

Mientras que las criptomonedas tienen la ventaja de ser difíciles o imposibles de rastrear, también tienen riesgos: dos de los riesgos principales son la volatilidad del mercado y que no están reguladas por gobiernos o por entidades bancarias. Sin embargo, Mcafee, en el documento *Understanding Ransomware and Strategies to Defeat it*, resalta la invención de *Bitcoin*, que es esencialmente un activo digital y sistema de pago inventado por Satoshi Nakamoto y lanzado como software de código abierto en 2009 (2016). *Bitcoin* es la primera moneda digital descentralizada, por lo anterior, los ciber criminales han optado en su mayoría por exigir el rescate en este tipo de criptomoneda.

El *ransomware* comenzó a dirigirse exclusivamente a organizaciones, pero ahora los usuarios comunes pueden ser un objetivo similar. Este *malware* toma el control de la información en el sistema, la cifra para que no se pueda leer y luego cobra un rescate antes de desencriptar la información y hacerla legible nuevamente. Según Day, el *ransomware* evoluciona rápidamente, y los últimos tipos ahora toman el control total del sistema y evitan cualquier tipo de acceso a menos que se pague el rescate (2017).

El *ransomware* es esencialmente un servicio de alquiler y está disponible en la web oscura, que es un área de Internet utilizada

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

para actividades ilícitas. Dos ataques de este tipo fueron muy publicitados en 2017: WannaCry golpeó el NHS en el Reino Unido, interrumpiendo los servicios médicos, y NotPetya golpeó a Ucrania, afectando a sus industrias, así como a algunas compañías globales, como Maersk.

Los ataques de este tipo, para Allen, son amenazas criminales simples y directas con un cierre rápido, no hay intermediarios para validar los datos (2017). La simplicidad de la amenaza hace que el *ransomware* sea extremadamente popular con los criminales A esta fórmula se agrega el *Bitcoin*, una moneda anónima y difícil de rastrear. Por estas razones es fácil ver por qué a los ciberdelincuentes les gusta tanto este modelo de negocio.

Clases de ransomware

A medida que surgen nuevas variantes, puede resultar difícil realizar un seguimiento de las diferentes cepas. Si bien cada una de estas variedades de *malware* es diferente, a menudo se basan en tácticas similares para aprovecharse de los usuarios y mantener como rehenes los datos cifrados. Estos son algunos de los tipos de *ransomware* más comunes.

I. *Ransomware* de cifrado. Este tipo cifra todos los archivos del equipo, documentos, hojas de cálculo, pdf, imágenes, videos, etcétera. Un ejemplo de este tipo es CryptoLocker. En la siguiente imagen se muestra una captura de pantalla de un equipo afectado con este tipo de *malware*. El *ransomware* de cifrado se divide en tres tipos:

- **Symmetrical Cryptosystem Ransomware**: emplea un algoritmo de cifrado simétrico, por ejemplo DES o AES, para cifrar los archivos de la víctima, utilizando la misma clave para cifrado y descifrado. Esto hace plausible para la víctima para recuperar la clave secreta aplicando técnicas de ingeniería inversa o escaneo de memoria.
- **Asymmetrical Cryptosystem Ransomware**: en este tipo una clave pública incrustada en el *ransomware* o descargado durante la comunicación con el servidor de comando y control (C&C) se utiliza para cifrar la información de la víctima. Como la clave privada la mantiene solamente el atacante, es imposible que la víctima la obtenga sin pagar

el rescate. Sin embargo, esta técnica consume más recursos mientras cifra los archivos.

- **Hybrid Cryptosystem Ransomware**: utiliza una clave simétrica generada dinámicamente para cifrar los archivos y una clave pública precargada para cifrar la clave simétrica en sí, después de borrarla de la memoria.

II. Lock Screen Ransomware: bloquea la pantalla de la máquina de la víctima y solicita pago. En otras palabras, restringe el inicio de sesión o el acceso a archivos mientras exige el pago para levantar la restricción. Generalmente, se implementa a nivel del sistema operativo, lo que significa que no podrá usar el computador o el dispositivo infectado.

III. Master Boot Record (MBR) Ransomware-realware. Afecta al sector de arranque del disco duro del equipo impidiendo iniciar el sistema operativo. El MBR es el código almacenado en los primeros sectores de una unidad de disco duro. Contiene información sobre las particiones del disco e inicia el cargador de arranque del sistema operativo. Sin un MBR adecuado, el computador no sabe qué particiones contienen un sistema operativo y cómo iniciarlo.

IV. *Ransomware* de cifrado de servidores web. Está orientado a servidores web, con el propósito de cifrar sus archivos. Esta amenaza cifra los archivos con extensiones conocidas o comunes que se emplean para desarrollar un sitio web, funciona de manera correcta solo si se ejecuta con permisos de *root*. Una vez que el servicio está corriendo, cifra y borra los archivos originales, utilizando el algoritmo de RSA AES de 2048 bits y cambiando las extensiones a ".encrypt". De tal modo que la víctima visualiza el mensaje que solicita el pago en *bitcoin* por el rescate y recuperación de la información.

V. *Ransomware* de dispositivos móviles. Está dirigida a los dispositivos Android, principalmente, que pueden infectarse a través de aplicaciones no oficiales. El *ransomware* generalmente termina en un teléfono móvil gracias a un ataque de ingeniería social.

VI. *Ransomware* dispositivos IOT. La verdadera amenaza para los dispositivos de Internet de las cosas (IoT) no es solo acceder a ellos a través de un *router* inseguro o la exposición del dispositivo a Internet, sino que este tipo de dispositivos de IoT en sí mismos son vulnerables y se pueden ver afectados con facilidad.

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

3. Metodología

3.1 Enfoque

El enfoque de la investigación es cuantitativo, debido a que se realizó una valoración de los casos relevantes de ataques de *ransomware* en Latinoamérica. El alcance del estudio es descriptivo ya que identificó indicadores y características propias de cada caso que permitieron definir un conjunto de recomendaciones para que los usuarios no sean víctimas de este tipo de ataque. Entre los años 2014 y 2017, la cantidad de ataques presentaba un aumento en promedio de 30% cada año, pero después del famoso caso de WannaCry en 2017, el interés de los ciberdelincuentes disminuyó, lo que produjo un periodo de relativa calma. Posteriormente, en 2018 esta modalidad de ataque retomó fuerzas y, desde entonces, ha mantenido un ritmo de crecimiento constante de casi 7% por año (Datta Business Innovation, 2020). Para el estudio que se realizó en 2020 se definió como ventana de observación de un lustro. Se requería recopilar información que no superara ese tiempo ya que en el campo de las tecnologías se presentan avances significativos de manera constante, como las versiones de los sistemas operativos. Por ejemplo, en el año 2017, cuando se produjo el incidente a escala global, la mayor parte de los sistemas infectados fue Windows XP y en el año 2020 este sistema operativo ya se consideraba totalmente obsoleto, de tal forma que el enfoque y las recomendaciones van orientadas a prevenir este tipo de incidentes en sistemas más actualizados.

3.2 Población de estudio

Se realizó levantamiento de información sobre casos relevantes de ataques de *ransomware* a nivel latinoamericano. Inicialmente se estudiaron casos que tuvieron gran impacto en entornos empresariales o institucionales para, a partir de esto, identificar los vectores de ataque y la metodología que utilizaron los atacantes para lograr afectar a las víctimas. Para determinar qué casos son relevantes, se tomó como parámetro el nivel de afectación que sufrió la empresa o institución en relación con las pérdidas económicas y el tiempo de recuperación ante el incidente.

Los países más atacados de la región son: Brasil con casi la mitad de las detecciones (46,69%), le siguen México (22,57%), Colombia (8,07%), Perú (5,56%), Ecuador (3,86%), Chile (2,29%), Venezuela (2,17%) y Argentina (1,93%) (Datta Business Innovation, 2020).

3.3 Técnicas de recolección

Se realizó una revisión documental sobre el *ransomware* con el propósito de conocer las diferentes cepas y variantes de este *malware*, también los principales vectores de ataque y las modalidades que utilizan los ciber delincuentes. Por otra parte, se profundizó sobre los casos sucedidos en América Latina para identificar los casos más relevantes y de mayor impacto en la región. Con esto se procuró obtener la información suficiente para proponer un conjunto de acciones que le permitan a los usuarios y a las organizaciones prevenir un ataque de esta naturaleza.

En 2019, los países de América con el mayor porcentaje de usuarios que encontraron *ransomware* fueron los siguientes:

Cuadro 1

Proporción de usuarios atacados por *ransomware*, del total de usuarios que detectaron *malware* en el país

País	Proporción de usuarios (%)
Estados Unidos	5,49
Paraguay	4.87
Venezuela	3,34
Canadá	3.25
Guatemala	2,81

Fuente: Kaspersky (2021).

En 2020, los países de América con la mayor participación eran en su mayoría los mismos, aunque con un porcentaje menor de usuarios que encontraron *ransomware*.

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

Cuadro 2

Proporción de usuarios atacados por *ransomware*, del total de usuarios que detectaron *malware* en el país

País	Proporción de usuarios atacados (%)
Estados Unidos	5,49%
Venezuela	4.87%
Canadá	3,34%
Paraguay	3.25%
Uruguay	2,81%

Fuente: Kaspersky (2021).

3.4 Procesamiento de análisis

De acuerdo con la información recopilada en el estudio a través de revisión documental fue posible identificar los vectores de ataque preferidos por los ciber delincuentes, así:

3.4.1 Mensajes de correo electrónico con enlaces maliciosos. El método más común de infección consiste en que los atacantes hacen uso de mensajes engañosos difundidos a través del correo electrónico. Normalmente se hace pasar el remitente por una empresa o entidad conocida, un banco o una agencia del gobierno. El propósito es persuadir al usuario para que pueda descargar o acceder a un documento importante mediante un *link* o enlace. Las direcciones url que se incluyen en el cuerpo del mensaje buscan dirigir a la víctima a un sitio comprometido, en donde se descargan los archivos maliciosos que infectan el sistema y los archivos.

3.4.2 Archivos maliciosos adjuntos en correo electrónico. Se trata de la misma modalidad que se menciona en el punto anterior, la gran diferencia es que el mensaje además de parecer legítimo, proveniente de fuente confiable, adjunta un archivo en formato .doc o .pdf. En otros casos, el adjunto es un archivo de imagen, el destinatario al ser engañado descarga y ejecuta el archivo, con lo cual lanza la carga útil del *ransomware* e infecta el sistema de manera automática.

Los ciberdelincuentes normalmente utilizan los siguientes tipos de archivos:

- **Documentos de Microsoft Office.** Este tipo de archivos son los que con mayor frecuencia se utilizan; en un mayor porcentaje, los documentos de Word y las hojas de cálculo de Excel. También en algunos casos se utilizan las presentaciones de Power Point. En este tipo de documentos se encuentran macros integradas, las cuales contienen una serie de instrucciones almacenadas que se ejecutan en forma de secuencias a través de una orden y con esto se inicia la descarga el *malware*.
- **Archivos PDF.** Este tipo de archivos pueden ocultar código malicioso que puede poner en peligro la seguridad de los equipos o dispositivos de los usuarios a través de la creación y ejecución de archivos Java Script.
- **Archivos ZIP y RAR.** Este tipo de archivos son los más utilizados por los ciber delincuentes para difundir las campañas de *ransomware*. Esto se debe a una función de WinRaR que permite que se establezcan unas órdenes para descomprimir el contenido del archivo en el computador y que sea ejecutado en el próximo reinicio. Para evitar que esto suceda es necesario actualizar el programa a la versión más reciente.
- **Kits de *exploits*.** Son un conjunto de herramientas que están diseñadas con el fin de aprovechar vulnerabilidades. Estos kits normalmente se ejecutan cuando el usuario ingresa a una web que ha sido comprometida. Dentro de la página se encuentra un código malicioso oculto. Frecuentemente, los atacantes utilizan anuncios, mejor conocidos como publicidad maliciosa, la cual lleva a la víctima al sitio en donde se ejecutará la descarga con la carga maliciosa, de tal forma que el sistema se infecta y cifra los archivos. Para esto los atacantes utilizan ventanas emergentes o anuncios que resulten llamativos o de interés para la víctima con el propósito de conseguir que hagan clic en el enlace al sitio comprometido. El anuncio puede ser una imagen provocativa, un mensaje de notificación o una oferta de software gratuito.

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

Este tipo de publicidad se está convirtiendo en un método cada vez más popular para la distribución de *ransomware*. La publicidad maliciosa aprovecha las mismas herramientas e infraestructuras que se usan para mostrar los anuncios legítimos en la web. Por lo general, los atacantes compran espacio publicitario, que se vincula a un kit de explotación.

Una vez que la victima hace clic en el anuncio, el kit de *exploits* escanea su sistema en busca de información sobre su software, sistema operativo, detalles del navegador y más. Si el kit de explotación detecta una vulnerabilidad, intenta instalar *ransomware* en la máquina del usuario. Muchos de los principales ataques de este tipo se propagan a través de publicidad maliciosa, incluidos CryptoWall y Sodinokibi.

3.4.3 *Ransomware* en redes sociales. Una tendencia que empieza a tomar fuerza es la difusión de *ransomware* a través de redes sociales. Esto debido a que también permiten él envió de documentos adjuntos maliciosos y de enlaces que dirigen a la víctima a un sitio web comprometido. Funciona de la misma forma que las campañas que se envían a través de correo electrónico, pero la particularidad es que por medio de redes sociales el atacante se adapta a los gustos de la víctima con el fin de hacer que el usuario acepte el intercambio de mensajes.

3.4.4 Protocolo de escritorio remoto (RDP). Este protocolo de comunicaciones permite conectarse a otro computador a través de una conexión de red, es otro vector de ataque popular para la difusión de campañas de *ransomware*. Algunos ejemplos que se propagan a través de RDP incluyen SamSam, Dharma y GandCrab, entre muchos otros. De forma predeterminada, el protocolo RDP recibe solicitudes de conexión a través del puerto 3389. Los ciberdelincuentes aprovechan esto mediante el uso de escáneres de puertos para buscar en Internet computadores con los puertos expuestos. Una vez han identificado máquinas vulnerables buscan obtener acceso explotando las vulnerabilidades de seguridad o utilizando ataques de fuerza bruta para descifrar las credenciales de inicio de sesión. Una vez que el atacante logra obtener acceso a la máquina, puede hacer en cierta medida lo que desee. Generalmente, esto implica deshabilitar el software antivirus y otras soluciones de seguridad que se encuentren instaladas, eliminar copias de seguridad accesibles y finalmente desplegar el *ransomware*. También

es posible que se habilite una puerta trasera que sea posible utilizar en el futuro.

3.4.5 MSP y RMM. Los ciberdelincuentes frecuentemente se dirigen a los proveedores de servicios administrados (MSP) con ataques de *phishing* e intentando explotar 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 presión sobre la víctima para pagar 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.

3.5.6 Publicidad maliciosa. Este método se está convirtiendo en uno de los preferidos por los ciberdelincuentes para la distribución de ransomware. La publicidad maliciosa aprovecha las mismas herramientas e infraestructuras que se utilizan para mostrar anuncios legítimos en la web. Normalmente, los atacantes compran espacio publicitario, que está vinculado a un kit de explotación.

3.4.7 Propagación de la red. Las cepas más antiguas de *ransomware* tenían la capacidad de cifrar únicamente la máquina local que infectó inicialmente. A partir de esto, este tipo de programa maligno ha evolucionado y las variantes más avanzadas tienen mecanismos de autopropagación 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 presentaban mecanismos de auto propagación, incluidos WannaCry, Petya y SamSam.

3.4.8 Unidades USB y computadoras portátiles. Estos dispositivos portátiles son un medio común para realizar la entrega de ransomware. La conexión de un dispositivo infectado puede provocar que este cifre la máquina local y se propague potencialmente por la red. Por lo general, esto sucede sin que el usuario se percate del hecho: un empleado o funcionario conecta involuntariamente una unidad USB infectada, que encripta su punto final, pero también puede ser deliberado. Un caso que fue muy comentado sucedió en Pakenham, un suburbio de Melbourne, en donde ciudadanos descubrieron unidades USB sin marcar en sus buzones de

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

correo. Las unidades contenían *ransomware* disfrazado de oferta promocional de Netflix.

3.4.9 Descargas de archivos en redes p2p o sitios de software pirata. Muchos de los sitios que promueven la descarga de software licenciado gratuito o craqueado, al igual que parches o *cracks*, para disponer de la versión del software completa sin verificaciones de licenciamiento, finalmente tienen intenciones muy diferentes; existe una alta probabilidad de que esos programas estén modificados para descargar módulos adicionales que pueden infectar el equipo del usuario. Un claro indicador de esto es que siempre se solicita deshabilitar el antivirus para poder realizar la instalación. En cualquiera de los dos casos, el atacante debe engañar al usuario, requiere que exista una intervención directa para descargar y ejecutar el archivo malicioso.

3.4.10 *Ransom as a Service* (RaaS). En este tipo de servicio, un proveedor ofrece una herramienta que contiene *ransomware* con el propósito de realizar un ataque y mantener secuestrados los archivos informáticos, información o sistemas. Normalmente, el que usa el *malware* o que aloja el *ransomware* solicita un rescate financiero para devolver el acceso a los datos a la víctima. En otras palabras, pueden "ordenar" la capacidad de plagiar un sistema y mantener como rehenes los datos de otra persona. Al igual que con los rescates tradicionales, los usuarios de *ransomware* como servicio a menudo toman medidas deliberadas para hacer que sus comportamientos sean difíciles de rastrear, incluida la solicitud de pagos digitales. De acuerdo con lo expuesto anteriormente se logra identificar la forma en la que los atacantes realizan la distribución del *ransom*, y del mismo modo se logra identificar que algunas cepas utilizan métodos definidos que garantizan que el ataque genere el impacto esperado.

3.4.11 *Ransomware* 2.0. La manera en que el *ransomware* 2.0 infecta los sistemas y se propaga a través de las redes no ha cambiado. Los datos aún están encriptados con un algoritmo virtualmente imposible de descifrar y aún se exige un rescate a la víctima. No obstante, donde el *ransomware* 2.0 muestra un comportamiento diferente al tradicional es en el aspecto de cómo extorsionan a la víctima para que realice el pago. Si la víctima decide no pagar el rescate, el atacante amenaza con publicar los datos secuestrados en línea.

Esto podría ser un duro golpe para una organización, ya que una posible exposición masiva de datos personales y confidenciales podría causar daños irreparables a la reputación, pérdida de negocios y algunas multas considerables de organismos reguladores como la ICO. También hay que considerar el daño que esto podría representar para los interesados, por ejemplo, los clientes de la empresa y las partes directa o indirectamente relacionadas.

4. Resultados

Un estudio revelado el 28 de mayo de 2020 por la Policía Nacional de Colombia muestra que los ataques de *ransomware* son una tendencia al alza en todo el país. Este informe señala que: el 30% de todos los ataques de *ransomware* en América Latina se han dirigido específicamente a Colombia (Erazo, 2020).

El mencionado informe fue elaborado en alianza con Cisco, McAfee, Microsoft, Absolute, Fortinet y Claro. En él se afirma que la amenaza del *ransomware* en Colombia está subestimada. A la cantidad de ataques colombianos le siguen Perú (16%), México (14%), Brasil (11%) y Argentina (9%), siendo las pymes los objetivos preferidos de los ciberdelincuentes. El estudio muestra que el 83% de las empresas del país carecen de los protocolos de respuesta necesarios para manejar la violación de las políticas de seguridad de la información. Por otra parte, a septiembre de 2020, Brasil tenía la mayor proporción de usuarios únicos atacados con *ransomware* en América Latina, con casi el 46,7 por ciento de los usuarios infectados. México ocupó el segundo lugar, con aproximadamente el 22,6 por ciento de los usuarios atacados, seguido de Colombia, con más del ocho por ciento.

Es importante mencionar los casos más relevantes que se han presentado en América latina desde el año 2015:

Ministerio de Desarrollo Social de Panamá: el 9 de enero de 2021 el Ministerio de Desarrollo Social de Panamá publicó un comunicado en el que explicó que el 6 de enero dicho organismo "fue víctima de un ataque de *ransomware* que afectó su infraestructura de red dejando fuera de servicio varios servidores e inhabilitando los sistemas de backup, dificultando la recuperación de los sistemas y la vuelta a la operatoria normal" (Harán, 2021).

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

La empresa Cencosud: las consecuencias de este ataque, ocurrido el 4 de diciembre de 2020, no sólo se evidenciaron en la Argentina, sino también en Chile, Perú y Colombia. Los cibercriminales amenazaron a la empresa con publicar los detalles personales de los clientes, como nombres, números de documentos y credenciales de las tarjetas de crédito.

Corte Superior de Justicia de Brasil: el 5 de noviembre de 2020 el Tribunal Superior de Justicia (STJ) anunció que la red de tecnología de la información del tribunal sufrió un ataque de piratas informáticos. Cuando se llevaron a cabo las sesiones de juicio, los sistemas del Tribunal Superior de Justicia se cerraron para detener la propagación en toda la red del tribunal, pero no antes de que todos los archivos del caso y las copias de seguridad estuvieran encriptados.

BancoEstado en Chile: el 6 de septiembre de 2020 el BancoEstado informó que durante ese fin de semana detectó en sus sistemas un software malicioso. Según el diario La Tercera, "la amenaza se trata de un ransomware, que consiste en un software malicioso que infecta computadores y no permite que se puedan utilizar. Generalmente, este tipo de programa maligno pide un rescate en dinero para poder liberar los equipos" (Marusic, 2020).

Compañía Telecom de Argentina: el 18 de julio de 2020, uno de los principales proveedores de servicios de telecomunicaciones en Argentina, *Telecom*, realizó un anuncio en donde manifestó que estaba sufriendo un ataque de *ransomware*. Los ciber atacantes exigían el pago en criptomoneda Monero de aproximadamente de 7,5 millones de dólares, e incluso amenazaron con incrementar el valor del rescate a 15 millones si no se realizaba el pago en tres días.

Pemex (México): la empresa de petróleos mexicana reportó el 10 de noviembre de 2019 que había sufrido varios intentos de ataques cibernéticos dirigidos, que finalmente afectaron al 5% de los computadores y por los cuales los ciberdelincuentes exigían un pago de 565 bitcoins.

A raíz del ataque del *ransomware* WannaCry en 2017, CSIRT Américas

> ha facilitado la identificación y el aislamiento temprano de los puntos críticos de infección en las Américas para frenar la propagación de WannaCry dentro de la región. Para mitigar brotes futuros, la plataforma ha creado un depósito

> central de herramientas para sus componentes regionales de modo de prevenir y combatir las infecciones de *ransomware*. (Banco Interamericano de Desarrollo, 2020, p. 23)

5. Conclusiones

Desde el año 2015 han surgido diferentes cepas de *ransomware*, lo que hace tan complicado para las empresas o los usuarios encontrar un mecanismo efectivo de prevención contra este tipo de amenaza, esto se debe a que cada cepa se comporta de manera diferente e incluso puede explotar vulnerabilidades activas en el sistema o simplemente engañar al usuario final para que ejecute el *malware* en su máquina.

Actualmente existen diferentes variantes de *ransomware*, y cada una de ellas cuenta con unas características especiales que se han incorporado por parte de los ciberdelincuentes con el fin de afectar a las víctimas de manera más eficiente y estas no tengan otra opción que pagar el rescate solicitado. Otro asunto es la variedad de vectores de ataque que han logrado abarcar, en este aspecto continúa siendo el correo electrónico el medio preferido para difundir estas campañas, pero los atacantes han buscado nuevas formas de propagar el *malware*.

De acuerdo con las metodologías que utilizan los atacantes para difundir las campañas de *ransomware*, se encontró que el correo electrónico es el medio más utilizado y tal vez el más vulnerable, debido a que resulta muy sencillo para los atacantes realizar envío masivo de correos y posteriormente esperar a que algún usuario haga clic en el archivo malicioso adjunto. Sin embargo, como se logró evidenciar, no es el único método utilizado por los atacantes, ya que cada vez utilizan técnicas más sofisticadas y efectivas.

Los ciberdelincuentes, para ejecutar este tipo de ataques, desarrollan estrategias elaboradas con el único propósito de alcanzar el mayor número de víctimas posible, puesto que cuanta más gente reciba el *malware* mayor será la probabilidad de infectar equipos. Incluso los atacantes ofrecen el *ransomware* como servicio, de modo que cualquier persona que desee hacer parte de una campaña dirigida proporciona los datos de la organización a atacar y cede a los atacantes un porcentaje de lo que se logre recaudar.

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

Las empresas y los usuarios deben tomar medidas preventivas para disminuir el impacto causado por este tipo de ataques, realizar copias de seguridad periódicas de los datos importantes, reforzar continuamente los sistemas con diferentes capas de protección. Estos son aspectos fundamentales a tener en cuenta por los usuarios sin importar el ámbito en el que se desenvuelvan, ya sea empresarial o personal.

En términos generales las empresas, para mitigar la amenaza de *ransomware*, deben contar con un plan de respuesta a incidentes, copias de seguridad, usar soluciones antivirus y anti-spam, habilitar análisis regulares del sistema y la red, deshabilitar los *scripts* de macros, mantener todos los sistemas parcheados, restringir el acceso a Internet, aplicar el principio de privilegio mínimo y, finalmente, participar en organizaciones y programas de intercambio de información sobre ciberseguridad.

Dentro de las recomendaciones propuestas para prevenir el *ransomware*, se realiza una distribución según la forma en la que el atacante apunta a la organización o a la persona, de tal forma que se tiene un compilado de buenas prácticas según el vector de ataque utilizado. Una de las claves para mitigar de forma proactiva los ataques de *ransomware* es mediante la concienciación, desde la direcciónyel área de TI hasta el usuario final.

La naturaleza de este tipo de ataque hace que se masifique esta modalidad criminal, toda vez que los ciberdelincuentes propagan el *malware* o realizan un ataque dirigido y es cuestión de tiempo para que un usuario desprevenido haga clic sobre el enlace o el archivo malicioso, lo cual basta para que empiece el proceso de cifrado de la información y que se mantiene hasta que la víctima realice el pago.

6. Recomendaciones

Como se mencionó anteriormente, el objetivo de este artículo es identificar cómo ha sido la evolución y el impacto del *ransomware* en América Latina para generar recomendaciones que orienten a las organizaciones para que eviten ser víctimas de este tipo de ataque. Por lo tanto, en este apartado se muestra un compilado de buenas prácticas para contribuir a la prevención de ataques de *ransomware* que puede ser útil tanto para las organizaciones como para las personas. Las recomendaciones se plantean proponiendo

una serie de consejos de acuerdo con los medios más comunes de propagación de esta amenaza y de las recomendaciones realizadas por firmas de antivirus como Kaspersky y McAffe, el Instituto Nacional de Ciberseguridad (INCIBE) y No More Ransom.

6.1 Archivos adjuntos de correo electrónico. El correo electrónico continúa siendo el medio más utilizado por los atacantes para propagar el *ransomware*. Con el fin de disminuir la probabilidad de ser víctima de este tipo de ataques se deben considerar los siguientes consejos de prevención:

- Abrir únicamente los archivos adjuntos de remitentes de confianza.
- Verificar la dirección de correo electrónico del remitente para corroborar que esta sea correcta.
- Se debe tener presente que los nombres de dominio y los nombres para mostrar pueden falsificarse de manera sencilla.
- No abrir archivos adjuntos que requieran habilitar las macros. Si considera que el archivo adjunto es legítimo, busque orientación o asesoría por parte del Departamento de TI, en el caso de las empresas.

6.2 URL maliciosas. Haciendo uso del correo electrónico, los atacantes envían este tipo de enlaces maliciosos, este método, al igual que el anterior, es muy utilizado para distribuir *ransomware*.

Consejos de prevención:

- Tener cuidado con todos los enlaces incrustados en correos electrónicos y mensajes directos.
- Verificar la URL ubicando el cursor sobre el enlace antes de hacer clic.
- Usar CheckShortURL para expandir URL abreviadas.
- Tratar de ingresar manualmente los enlaces en su navegador para evitar hacer clic en enlaces de *phishing*.

6.3 Protocolo de escritorio remoto. Las vulnerabilidades representan un riesgo potencial para los usuarios debido a que muchas veces no se realiza este tipo de verificaciones en los equipos de cómputo, por lo tanto, se utiliza con frecuencia este método de infección.

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

Consejos de prevención:

- Aunque suene repetitivo, utilizar contraseñas seguras y robustas.
- Cambiar el puerto RDP del puerto predeterminado 3389.
- Habilitar RDP si realmente se considera necesario.
- Utilizar una VPN.
- Habilitar un factor de doble autenticación (2FA) para sesiones remotas.

6.4 MSP Y RMM. Algunos servicios resultan vulnerables y esto es aprovechado por los ciberdelincuentes. Por lo tanto, es recomendable tomar medidas adicionales de protección.

Consejos de prevención:

- Habilitar factor de doble autenticación (2FA) en el software RMM.
- Los MSP deben estar muy atentos a las estafas de phishing.

6.5 Publicidad maliciosa. Haciendo uso de publicidad engañosa, la cual normalmente aprovecha la curiosidad e ingenuidad de algunos usuarios, es bastante sencillo que muchas personas hagan clic sobre este tipo de publicidad, por lo que vale la pena atender ciertas recomendaciones.

Consejos de prevención:

- Mantener el sistema operativo, aplicaciones y navegadores webs actualizados.
- Deshabilitar los complementos que no usa habitualmente.
- Utilizar un bloqueador de anuncios.
- Habilitar los complementos de reproducción por clic en el navegador web, lo que evita que complementos como Flash y Java se ejecuten automáticamente. Una gran cantidad de publicidad maliciosa se basa en la explotación de estos complementos.

6.6 Descargas automáticas. Este tipo de descargas son potencialmente peligrosas ya que se ejecutan sin que el usuario intervenga, por lo tanto, frecuentemente pasan inadvertidas.

Consejos de prevención:

- Instalar siempre los últimos parches o actualizaciones de seguridad de software.
- Eliminar los complementos innecesarios del navegador.
- Instalar un bloqueador de anuncios.

6.7 Propagación de la red. En este aspecto el nivel de riesgo se incrementa toda vez que existen cepas que tienen módulos dedicados a difundir el *ransomware* en otros equipos conectados a la misma red.

Consejos de prevención:

- Segmentar la red y aplicar el principio de privilegio mínimo.
- Implementar y mantener una estrategia de respaldo de *ransomware* confiable.
- Si por algún motivo algún equipo en la red resulta infectado, se debe desconectar de inmediato. Con el fin de evitar que la infección se propague a otros equipos conectados a la red.

6.8 Software ilegal. En internet se encuentran diversas páginas que permiten la descarga de software que requiere el pago de una licencia de manera gratuita, en donde normalmente se ofrece el activador o crack, estos archivos al ejecutarlos en la máquina son los que instalan el *ransomware*, o dejan abierta una puerta trasera por donde posteriormente será implantada la infección.

Consejos de prevención:

- Evitar el uso de software ilegal.
- No visitar sitios web que alojan software pirateado, cracks, activadores o generadores de claves.
- Tener cuidado con las ofertas de software que son demasiado buenas para ser verdad.

6.9 Unidades USB y computadoras portátiles. Las unidades USB históricamente han sido un vector de ataque que se ha utilizado para infectar computadores con troyanos, *malware*, y otro tipo de virus informáticos, de tal forma que el *ransomware* no es la

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

excepción y también se utiliza este medio. Por otra parte, si se permite la conexión a la red de un equipo portátil que ya esté infectado, este puede empezar a infectar a los demás equipos en la red.

Consejos de prevención:

- Nunca conectar dispositivos desconocidos a su computadora.
- No conectar dispositivos a sistemas públicos compartidos, como quioscos de impresión de fotografías y computadores en cibercafés.
- Las empresas deben implementar y mantener sólidas políticas de seguridad BYOD.
- Utilizar un software antivirus de buena reputación que pueda escanear y proteger unidades extraíbles.
- Dentro de las políticas de la organización se debe regular la conexión de equipos portátiles a la red corporativa.

6.10 Ransomware para dispositivos móviles. El ciberdelincuente puede utilizar *malware* móvil para robar los datos confidenciales de un teléfono inteligente o bloquear un dispositivo, por lo que, a continuación, se mencionan algunos consejos que ayudan a proteger los dispositivos móviles:

- Mantenerse informado sobre las últimas amenazas y tendencias de cibercrimen. El *ransomware* está en constante evolución y apunta a diferentes dispositivos. Cuanto más conocimiento se tenga sobre cómo se llevan a cabo estos ataques, más fácil y rápido será encontrar una solución.
- Instalar parches de seguridad. El *ransomware* puede infectar un dispositivo a través de descargas no autorizadas. Esto puede ocurrir al visitar accidentalmente sitios web comprometidos. Esto también suele darse por ser redirigido a estos sitios web sospechosos a causa de un *malware* que se esconde en un sitio legítimo. Una contramedida es asegurarse de que todas las aplicaciones y sistemas operativos estén actualizados.
- Tener precaución con la instalación de aplicaciones falsas. Estas aplicaciones son una fuente de *malware*. Antes de instalar cualquier aplicación, debe asegurarse de descargarla

de App Store, Google Play o App Gallery (Huawei), que son las tiendas de aplicaciones oficiales, por lo que aplicaciones de terceros pueden ser peligrosas.

- Realizar una copia de seguridad de todos los archivos siempre es una muy buena idea. La copia de seguridad de los archivos permite que el usuario pueda recuperar la información sin tener la necesidad de pagar el rescate. Esto no solamente aplica para *ransomware*, también si se pierde o daña el teléfono.
- Utilizar una solución de seguridad móvil sólida. Siempre es recomendable mantener todos los dispositivos protegidos con una solución de seguridad integral.

6.11 Acciones por realizar en caso de infección de *ransomware*. La intención principal de la elaboración del presente proyecto es definir un conjunto de buenas prácticas para evitar ser víctima de este tipo de ataque, No obstante, en el caso de producirse un incidente relacionado con *ransomware*, se deben considerar los siguientes pasos:

- Tomar una instantánea del sistema. Antes de apagar el sistema, en el caso de que el *malware* lo permita, se debe intentar capturar una instantánea de la memoria del sistema. Esto permite que más adelante sea posible localizar el vector de ataque del *ransomware*, así como cualquier material o recurso criptográfico que pueda ayudar a descifrar los datos.
- Apague el sistema. Con el fin de evitar que se produzca una mayor propagación del *ransomware* y que el daño sobre los datos sea mayor, se debe apagar el sistema que esté infectado.
- Identificar el vector de ataque. Es importante que el usuario logre identificar el momento exacto en el que perdió acceso a los datos, así como los correos electrónicos que pueden ser sospechosos de contener el *ransomware* o los enlaces que dirigen al archivo o página que entrega el ejecutable, esto es útil para evitar una mayor propagación del ataque.
- Bloquear el acceso a la red. Ya que muchas cepas de *ransomware* tienen la capacidad de moverse dentro de la red en

InterSedes, ISSN 2215-2458, Volumen 24, Número 49, Enero-Junio, 2023, pp. 92-119 (Artículo).

la que se encuentra el equipo infectado. Es importante que se bloquee cualquier servidor de comando y control identificado utilizado por *ransomware*. A menudo el malware no puede cifrar datos si no tiene acceso a estos servidores.

- Notificar a las autoridades competentes. Es fundamental informar a las autoridades para que puedan ayudar con la investigación. La Policía Nacional puede contribuir mediante el CSIRT a entender qué ha sucedido realmente y qué tipo de *ransomware* fue el que impactó a la organización o usuario. Los pagos que se solicitan como rescate tienden a aumentar a medida que pasa el tiempo hasta que se realiza el pago.

7. Referencias Bibliográficas

Allen, J. (2017). Surviving ransomware. *American Journal of Family Law*. https://www.proquest.com/docview/1915305812

Allsopp, W. (2017). *Advanced Penetration Testing: Hacking the World's Most Secure Networks*. San Francisco: John Wiley & Sons, Incorporated.

Alvarado, N. (29 de noviembre de 2017). *5 elementos esenciales para reducir la inseguridad desde lo local*. Discurso de apertura de la encargada de seguridad ciudadana del BID, Nathalie Alvarado, en la Clínica de Seguridad Ciudadana, Medellín, Colombia. https://blogs.iadb.org/seguridad-ciudadana/es/elementos-para-reducir-la-inseguridad/

Avila, F. (2021). *Evolución e impacto del Ransomware en América Latina desde el año 2015*. [Proyecto de Grado Universidad Nacional Abierta y a Distancia] https://repository.unad.edu.co/bitstream/handle/10596/42667/fyavilan.pdf?sequence=3&isAllowed=y

Avila, F. (2021). *Impacto del Ransomware en América Latina desde el año 2015*. Editorial Académica Española.

Banco Interamericano de Desarrollo (2020). Observatorio de ciberseguridad. Riesgos, avances y el camino a seguir en américa latina y el Caribe. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Chauhan, S. y Kumar, N. (2015). *Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques*. Amtersdam: Elsevier Science & Technology Books.

Datta Business Innovation. (2020). América Latina registra 5 mil ataques de ransomware por día. https://datta.com.ec/articulo/america-latina-registra-5-mil-ataques-de-ransomware-por-dia

Day, G. (2017). *Security in the Digital World: For the home user, parent, consumer and home office*. Londres: IT Governance Ltd.

Erazo, F. (2020). *Colombia Is the Ransomware Capital of Latin America*. Cointelegraph. Recuperado de https://cointelegraph.com/news/colombia-is-the-ransomwarecapital-of-latin-america

ESET. (2021). Security Report Latinoamerica 2021. https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Forbes. (2022). Ransomware, el ciberataque que prendió las alarmas en Latinoamérica. https://forbes.co/2022/06/11/tecnologia/%EF%BF%BC%EF%BF%BCransomware-el-ciberataque-que-prendio-las-alarmas-en-latinamerica/

Harán, J. (2021) *Ataque de ransomware afectó al Ministerio de Desarrollo Social de Panamá*. We live security. https://www.welivesecurity.com/laes/2021/01/12/ataque-ransomware-afecta-ministerio-desarrollo-social-panama/

Kaspersky. (2021). *Ransomware en cifras: Reevaluación del impacto global de esta amenaza.* Secure list. https://securelist.lat/ransomware-by-the-numbers-reassessing-the-threats-global-impact/93569/

Kaspersky: América Latina registra 5 mil ataques de ransomware por día. (2021, mayo 26). latam.kaspersky.com. https://latam.kaspersky.com/about/press-releases/2020_kaspersky-america-latina-registra-5-mil-ataques-de-ransomware-por-dia

INCIBE. (2020). *Ransomware: una guía de aproximación para el empresario.* https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

Marusic. M. (2020). *CMF inició supervisión in situ en BancoEstado por ataque de ransomware y la estatal instruyó a sus ejecutivos a no conectarse a la red*. La Tercera. https://www.latercera.

com/pulso/noticia/cmf-inicio-supervision-in-situ-enbancoestado-por-ataque-de-ransomware-y-la-estatal-instruyo-a-sus-ejecutivos-a-no-conectarse-ala-red/2QEL4J43HZF6BJ5ENWKRJAJXVQ/

Ramírez Duque, A. (2022, julio 6). Tendencias en Ciberseguridad en Latinoamérica. *Revista Empresarial & Laboral*. https://revistaempresarial.com/tecnologia/seguridad-informatica/tendencias-en-ciberseguridad-en-latinoamerica/

Rosenberg, M. (2015). *About the malicious software known as ransomware*. PHYS https://phys.org/news/2015-04-qa-malicious-software-ransomware.html

Savage. K, Coogan. P y Lau. H. (2015). *The Evolution of Ransomware.* https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/theevolution-of-ransomware.pdf

Sobrino, W. (2018). Los seguros de 'cyber risk'. (A propósito del ciberataque mundial de fecha 12 de mayo de 2017). *Revista Ibero-Latinoamericana de seguros.* https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/21179

Zetter, K. (2016). *4 Ways to Protect Against the Very Real Threat of Ransomware*. Wired. https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/