EVOLUCIÓN E IMPACTO DEL RANSOMWARE EN AMÉRICA LATINA DESDE EL AÑO 2015

FREDY YESID AVILA NIÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DUITAMA
2021

EVOLUCIÓN E IMPACTO DEL RANSOMWARE EN AMÉRICA LATINA DESDE EL AÑO 2015

FREDY YESID AVILA NIÑO

Proyecto de Grado – Monografía presentada para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Director Proyecto
Esp. Ing. DANIEL FELIPE PALOMO LUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DUITAMA
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Duitama. 10 de abril 2021

DEDICATORIA

Con amor dedico este trabajo a mis hijos, que gracias a su apoyo me impulsan en esta nueva etapa de mi vida, motivándome y siendo la razón para continuar creciendo personal y profesionalmente, también lo dedico a mi esposa que, con su apoyo incondicional, hace que todo obstáculo sea más fácil de superar.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACIÓN: toda aquella información que tenga valor o sistema que se relacione con su tratamiento, estos activos pueden ser procesos, datos, equipos, aplicaciones, personal, redes, instalaciones, soportes de información.

ADWARE: programa que, durante su instalación y uso, muestra automáticamente publicidad. Frecuentemente relacionado con programa maligno, no en todas las ocasiones lo es, pasa a ser *malware* cuando empieza a recopilar y extraer información del equipo en el que está instalado.

AMENAZA: es aquella situación o circunstancia que no es favorable y cuando ocurre puede tener efectos negativos, como indisponibilidad, perdida completa o de una parte de la información y mal funcionamiento.

ANTIVIRUS: programa diseñado para detectar, bloquear y eliminar programas, archivos y código malicioso.

BACKUP: es la copia de seguridad realizada sobre archivos, información o aplicaciones que se encuentran contenidas en un equipo de cómputo, con el fin de recuperar datos en caso de daño o perdida.

BITCOIN: es una criptomoneda, una moneda virtual o una moneda digital, “es un tipo de dinero que es completamente virtual en otras palabras, es como una versión en línea de efectivo”[1].

[1] BBC. Guide: What is Bitcoin and how does it work? [Sitio web]. [Consulta: 15 de enero 2021]. Disponible en: https://www.bbc.co.uk/newsround/25622442

BOTNET: hace referencia a un conjunto de computadores o dispositivos que son controlados de manera remota por un atacante, con el fin de realizar actividades maliciosas.

CIFRADO: es una operación o función matemática que se utiliza en conjunto con una clave para aplicar sobre un texto claro y permite obtener texto cifrado, lo que garantiza confidencialidad e integridad.

CRIPTOGRAFÍA: técnica mediante la cual se cifra un mensaje, o texto claro, de la cual se obtiene un mensaje cifrado o criptograma, el cual es ilegible para personas externas a la comunicación; es decir, es necesario conocer el sistema de cifrado y la clave.

CRIPTOMONEDA: es una moneda digital o virtual que está protegida por criptografía, lo que hace que sea casi imposible falsificar o gastar dos veces. Muchas criptomonedas son redes descentralizadas basadas en la tecnología *blockchain*.

DIRECCIÓN IP: número único e irrepetible que permite identificar a todo sistema o dispositivo conectado en la red.

DISPONIBILIDAD: es la capacidad que tiene un servicio, sistema o información, a ser accesible y utilizable por los usuarios autorizados a accederla, cada vez que sea requerido.

EXPLOIT: “es una pieza de *software*, un fragmento de datos o una secuencia de comandos que se aprovecha de un error o vulnerabilidad en una aplicación o un sistema para causar que ocurra un comportamiento no deseado o no anticipado”[2].

[2] BITDEFENDER. What is an exploit? [Sitio web]. [Consulta: 15 de enero 2021]. Disponible en: https://www.bitdefender.com/consumer/support/answer/10556/

MALWARE: abreviatura de software malicioso, es un término general para virus, gusanos, troyanos y otros programas informáticos dañinos.

MSP (proveedor de servicios gestionados): Un MSP es una persona o agencia que brinda servicios administrados a sus clientes, lo que incluye grandes organizaciones, industrias, hospitales o cualquier persona que tenga enormes infraestructuras de TI pero no tenga administración de TI interna.

PHISHING: "técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de buena reputación"[3].

RMM (gestión de supervisión remota): s el trabajo real que cualquier MSP hace para sus clientes, es decir, un MSP brinda servicios de "Monitoreo y administración remotos" a sus clientes.

SCAREWARE: es una táctica de *malware* que manipula a los usuarios haciéndoles creer que necesitan descargar o comprar software malicioso, a veces inútil. "El *scareware*, que suele iniciarse con un anuncio emergente, utiliza la ingeniería social para aprovechar el miedo de un usuario y lo induce a instalar un *software* antivirus falso"[4].

SPEAR PHISHING: es un intento dirigido de robar información confidencial, como: credenciales de cuenta o información financiera de una víctima específica, a menudo por motivos maliciosos. "Esto se logra adquiriendo los datos personales de

[3] NIST. Phishing definition. [Sitio web]. [Consulta: 17 de enero 2021]. Disponible en: https://csrc.nist.gov/glossary/term/phishing
[4] FORCEPOINT. What is Scareware? Scareware Defined, Explained, and Explored. [Sitio web]. [Consulta: 17 de enero 2021]. Disponible en: https://www.forcepoint.com/es/cyber-edu/scareware

la víctima, como sus amigos, su ciudad natal, su empleador, los lugares que frecuenta y lo que han comprado recientemente en línea”[5].

TROYANO: “un caballo de Troya, o troyano, es un tipo de código o *software* malicioso que parece legítimo pero que puede tomar el control de su computadora. Un troyano está diseñado para dañar, interrumpir, robar o, en general, infligir alguna otra acción dañina en sus datos o red”[6].

[5] DIGITAL GUARDIAN. What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing. [Sitio web]. [Consulta: 20 de enero 2021]. Disponible en: https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

[6] NORTON. What is a Trojan? Is it a virus or is it malware? [Sitio web]. [Consulta: 20 de enero 2021]. Disponible en: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

RESUMEN

Ransomware no es más que un programa malicioso (*malware*) diseñado para bloquear el acceso a los archivos o en algunos casos al sistema operativo, con esto el atacante consigue afectar uno de los tres pilares de la seguridad informática, la disponibilidad. Normalmente este tipo de ataque bloquea el acceso a través del cifrado de los archivos, cuya clave de cifrado solamente conoce el atacante, este a su vez, le solicita a la víctima cierta cantidad de dinero (en Criptomoneda) para conceder nuevamente el acceso a los archivos (clave de cifrado). Aunque esta técnica no es novedosa, la firma *Kaspersky* advierte que: "El *Ransomware* creció un 43% en el año 2018, mientras que los *backdoors* lo hicieron en un 44%"[7], y han logrado identificar diferentes cepas únicas de *Ransomware*.

En América Latina los ataques de *Ransomware* se posicionan como una de las amenazas más importantes, por esta razón es fundamental conocer su evolución e impacto desde el año 2015, entender el concepto y características, identificar los tipos de *Ransomware* que han aparecido en los últimos 5 años y describir los métodos de infección que se utilizan. Con esta información es posible generar recomendaciones para evitar ser víctima de este ataque.

PALABRAS CLAVE: *Ransomware*, *malware*, ataque, vulnerabilidad, amenaza.

[7] INFO CHANNEL. Ataques de ransomware se disparan: Kaspersky Lab. [Sitio web]. México: Staff High Tech Editores. [Consulta: 1 de mayo 2020]. Disponible en: https://www.infochannel.info/ataques-de-ransomware-se-disparan-kaspersky-lab

ABSTRACT

Ransomware is nothing more than a malicious program (malware) designed to block access to files or in some cases to the operating system, with this the attacker manages to affect one of the three pillars of computer security, availability. Normally this type of attack blocks access through encryption of files, whose encryption key is only known to the attacker, who in turn asks the victim for a certain amount of money (in Crypto-currency) to grant access again. to files (encryption key). Although this technique is not new, the firm Kaspersky warns that: "Ransomware grew 43% in 2018, while backdoors did 44%", and have managed to identify different unique strains of Ransomware.

In Latin America, Ransomware attacks are positioned as one of the most important threats, for this reason it is essential to know their evolution and impact since 2015, understand the concept and characteristics, identify the types of Ransomware that have appeared in the last 5 years and describe the infection methods used. With this information it is possible to generate recommendations to avoid becoming a victim of this attack.

KEY WORDS: Ransomware, Malware, Attack, Vulnerability, Threat.

INTRODUCCIÓN

El presente documento está orientado a la identificación de la evolución e impacto del *Ransomware* en América Latina en los últimos 5 años, lo que permite reconocer su comportamiento y tendencias. Posteriormente, se generan recomendaciones que permitan orientar a las organizaciones para que logren evitar ser víctimas de ataques de este tipo.

Como su nombre lo indica, 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" [8]. Por lo general, los *ransomwares* utilizan tecnologías de cifrado para mantener los datos cautivos.

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 (70) países" [9]. Posteriormente, los medios determinaron que en realidad se habían producido 130.000 ataques y que los mismos habían ocurrido en cien (100) países.

El *Ransomware*, en sus inicios fue pensado para atacar a las organizaciones, ahora los ciber criminales han diseñado diferentes variantes que pueden afectar a personas comunes, en diferentes plataformas y dispositivos. Es importante identificar en América Latina las medidas que se han implementado para mitigar

[8] CHAUHAN, Sudhanshu y KUMAR, Nutan. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. Amtersdam: Elsevier Science & Technology Books. 2015. p.206. ISBN 9780128018675

[9] Revista Ibero-Latinoamericana de seguros. Los seguros de 'cyber risk'. (A propósito del ciberataque mundial de fecha 12 de mayo de 2017). Bogotá: Universidad Javeriana, 2017, nro. 47 ISSN 0123-1154

este riesgo, esto contribuye a compilar buenas prácticas y recomendaciones para evitar que se presenten nuevas víctimas.

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 reportan incidentes relacionados con mayor frecuencia 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.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los incidentes de ciber seguridad en el mundo aumentan exponencialmente en los últimos años, pero llama la atención particularmente el *Ransomware*, puesto que es un método ampliamente conocido, y a pesar de los esfuerzos, estrategias y medidas que se han tomado para mitigar este tipo de ataque, continúan presentándose casos, incluso los ciber delincuentes han logrado paralizar ciudades enteras ya que consiguen infectar los sistemas de administración pública.

Cuando una organización sufre un ataque de *Ransomware* el impacto es alto, toda vez que se ve afectada la disponibilidad de la información, los archivos son cifrados o simplemente dejan inutilizable el sistema operativo de la víctima, una característica adicional de este tipo de ataque es que logra infectar a otros equipos conectados en la misma red, tal y como sucedió en mayo de 2017. *WANNACRY*, escanea tanto la red interna de la empresa como la externa, realizando conexiones hacia el puerto 445 (SMB), en busca de equipos que no estén actualizados, para propagarse a través de ellos e infectarlos [10], esto fue determinado en el informe #*Wannacry* de Panda *Security*.

Ese mismo ataque infectó máquinas con sistema operativo *Windows* vulnerable en países como Rusia, Reino Unido, Estados Unidos y España, en donde fue mediático el caso de Telefónica. Las versiones vulnerables a este *Ransomware* son: *Windows XP*, *Windows* Vista, *Windows* 7, *Windows Server* 2012, *Windows* 10 y *Windows Server* 2016. Cabe mencionar que XP y *Windows* 7 ya no cuentan con soporte por parte de *Microsoft*, este último finalizó el 14 de enero del 2020.

[10] PANDA SECURITY. Informe #*Wannacry*. [Sitio web]. Madrid: Panda. [Consulta: 2 de mayo 2020]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/05/1705-Informe_WannaCry-v160-es.pdf

En los últimos años se han documentado casos en Latinoamérica, en los cuales, a causa de ataques de este tipo, hospitales, universidades, empresas, entidades de gobierno y miles de usuarios han visto comprometidos sus activos de información. Son recurrentes los casos de *Ransomware*, así como las múltiples variantes que han aparecido; cada una de ellas con características y funcionalidades diferentes, incluso, se encuentran cepas de *ransom* para diferentes sistemas operativos y dispositivos móviles.

Sin embargo, a pesar de los esfuerzos y medidas que se toman para protegerse de los ataques, aparecen nuevas variantes y nuevos vectores de ataque, lo que indica que aún existen brechas de seguridad que los atacantes han identificado para seguir ejecutando campañas de *Ransomware* dirigido a organizaciones, entidades de gobierno y usuarios comunes. Durante el año 2019, en América Latina se observó un aumento de casos relacionados a campañas de *ransomware*, entre Perú, México, Brasil, Colombia y Argentina, representan el 68,23 por ciento de los ciberataques de este tipo.

Figura 1. Detecciones de *ransomware* en América Latina 2019.

País	Porcentaje de detecciones
Perú	20.93%
México	14.05%
Brasil	12.26%
Colombia	10.85%
Argentina	10.14%
Ecuador	8.18%
Venezuela	6.96%
República Dominicana	3.90%
Guatemala	2.51%
Chile	2.16%
Bolivia	1.75%
Costa Rica	1.72%
Honduras	1.08%
Nicaragua	0.72%
Panamá	0.65%
El Salvador	0.53%
Cuba	0.36%
Paraguay	0.31%
Uruguay	0.29%
Martinica	0.18%

Fuente: WELIVESECURITY. Detección de ransomware en América latina 2019. [En línea]. ESET (Recuperado en 5 mayo 2020) Disponible en: https://www.welivesecurity.com/la-es/2020/01/09/ransomware-amenaza-vigente-utilizada-ataques-dirigidos/paises-mayor-deteccion-ransomware-america-latina-2019/

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál ha sido la evolución e impacto del *Ransomware* en América Latina desde el año 2015?

2. JUSTIFICACIÓN

El secuestro de información se mantiene, durante los últimos años, como uno de los ataques preferidos por los ciber-criminales, esto debido a que 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, quedando como única opción, pagar el rescate de la información. Frecuentemente, se habla de *Ransomware* y de todas las precauciones para tener en cuenta para evitar ser víctima de este ataque, sin embargo, se siguen presentando casos y siguen en producción nuevas variantes de este tipo de *malware*.

Un aspecto importante 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 vulnerabilidades activas en los sistemas operativos, implementa funciones que deshabilitan servicios, incluso logra reiniciar la maquina 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.

Es evidente que 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 maquina 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 sistemas, 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. “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”[11].

Con lo anteriormente mencionado, se hace necesario conocer cómo ha sido la evolución e impacto del *ransomware* ataque 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.

[11] ALLSOPP, Wil. Advanced Penetration Testing: Hacking the World's Most Secure Networks. San Francisco: John Wiley & Sons, Incorporated. 2017. p.147. ISBN 9781119367680

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Identificar cómo ha sido la evolución y el impacto del *Ransomware* en América Latina desde el año 2015, generando recomendaciones que orienten a las organizaciones para que eviten ser víctimas de este ataque.

3.2 OBJETIVOS ESPECÍFICOS

- Comparar las características de los diferentes tipos de *Ransomware* que han surgido desde el año 2015 hasta la actualidad.

- Describir las metodologías más utilizadas por los atacantes para la ejecución del ataque.

- Identificar las medidas que han tomado las organizaciones y las personas para protegerse de este tipo de amenaza.

- Proponer un compilado de buenas prácticas en cuanto a la prevención del *Ransomware*, para las organizaciones y para las personas.

4. MARCO REFERENCIAL

4.1 MARCO 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*.

El crecimiento de este tipo de amenaza se mantiene constante, normalmente cifrar los archivos con una clave única, la cual solamente el creador del Ransomware conoce y si la victima realiza el respectivo pago también puede conocer. El Instituto Nacional de Ciberseguridad de España, lo define como: "El *Ransomware* es un tipo de *malware* que hoy en día se está propagando de forma muy activa por internet. Este *malware* impide el acceso y amenaza con destruir los documentos y otros activos de las víctimas si estas no acceden a pagar un rescate"[12].

El *Ransomware*, es un *malware* que bloquea el computador o simplemente impide acceder a sus datos haciendo uso de cifrado de clave hasta que se pague un rescate. 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.

[12] INCIBE. *Ransomware*: una guía de aproximación para el empresario. [Sitio web]. Madrid: Instituto Nacional de Ciberseguridad. [Consulta: 15 de marzo de 2020] Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

Kim Zetter, en el año 2016 publica 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”[13], realizando 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”*[14], 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.

Por otra parte, 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

[13] WIRED. 4 Ways to Protect Against the Very Real Threat of Ransomware [Sitio web]. Washington: ZETTER, Kim. 2016. [Consulta: 15 de marzo de 2020]. Disponible en: https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/

[14] SYMANTEC. The Evolution of Ransomware [Sitio web]. California. SAVAGE. Kevin, COOGAN. Peter y LAU. Hon. [Consulta: 15 de marzo de 2020]. Disponible en: https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf

dispositivo, no será posible acceder 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, Kim Zetter, en su artículo: "4 *Ways to Protect Against the Very Real Threat of Ransomware*", comenta que "entre finales de los 90 hasta el 2005, los métodos de pago en línea no eran comunes, ni estaban disponibles"[15], las víctimas para pagar rescates utilizaban mensajes de texto SMS o enviando tarjetas prepagas por correo. 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, M. Joyce. 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"[16]. Las Criptomonedas son divisas electrónicas, lo que hace mucho más difícil rastrear y, por lo tanto, ayuda a que las transacciones sean anónimas.

Mientras que las criptomonedas tienen la ventaja de ser difícil o imposible 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 *whitepaper* "*Understanding Ransomware and Strategies to*

[15] WIRED. 4 Ways to Protect Against the Very Real Threat of Ransomware [Sitio web]. Washington: ZETTER, Kim. 2016. [Consulta: 15 de marzo de 2020]. Disponible en: https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/

[16] PHYS.ORG. About the malicious software known as ransomware [Sitio web] Rosenberg, M. Joyce. [Consulta: 18 de marzo de 2020]. Disponible en internet: https://phys.org/news/2015-04-qa-malicious-software-ransomware.html

Defeat it", resalta la invención de Bitcoin[17], que es esencialmente un activo digital y sistema de pago inventado por Satoshi Nakamoto y lanzado como código abierto *software* en 2009. *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 Graham 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"[18].

El *ransomware* como servicio es esencialmente un *ransomware* de alquiler y está disponible en la web oscura, que es un área de Internet utilizada para actividades nefastas. 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 son: "amenazas criminales simples y directas con un cierre rápido, no hay intermediarios para validar los datos, 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" [19], por estas

[17] MCAFFE. Understanding Ransomware and Strategies to Defeat it" [Sitio web]. Santa Clara. McAffe.[Consulta: 20 de marzo de 2020]. Disponible en: http://www.mcafee.com/it/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf
[18] DAY, Graham. Security in the Digital World: For the home user, parent, consumer and home office. Londres: IT Governance Ltd, 2017. p.64. ISBN 9781849289610
[19] ALLEN, Jeffrey. Surviving ransomware. American Journal of Family Law. 2017, vol. 31, no. 2, s. 65. ISSN 0891-6330.

razones es fácil ver por qué a los ciberdelincuentes les gusta tanto este modelo de negocio.

4.2 MARCO CONCEPTUAL

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. De esta manera aparecen 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 se establece a través de la red TOR comunicación con el atacante 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 importante reconocer los métodos de infección que son utilizados por los atacantes, en este punto es donde 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*.

El principal método de propagación, son los troyanos, estos son alojados en sitios web malintencionados o sitios legítimos que previamente han sido comprometidos

por los cibercriminales. Las páginas con contenido pornográfico, descargas de *software* o de juegos, son las que con mayor frecuencia se utilizan para redirigir al usuario a otro sitio comprometido, que, a su vez, les infecta con el *Ransomware*.

Otro de los métodos utilizados, es el *Spear Phishing*, el cual es un *phishing* dirigido, ya que el atacante busca infectar a un blanco específico, hace el envío de correos masivos que contienen enlaces a los sitios comprometidos, también puede realizarse por mensajería instantánea o redes sociales. Por otra parte, también es utilizado el escritorio remoto, que se lleva a cabo explotando alguna vulnerabilidad activa en la máquina de la víctima o mediante el uso de ataques de fuerza bruta, que le permita al atacante usar el Protocolo de Escritorio Remoto (RDP).

En cuanto a los dispositivos móviles, se apunta mucho más a *Android*, esto por tener la mayor cuota del mercado para lograr infectar estos dispositivos, el atacante publica aplicaciones maliciosas, que al ser instaladas desencadenan el *malware*. Lo anterior no quiere decir que *Android* sea el único sistema operativo de móviles vulnerable, por el contrario, para IOS, también existen campañas de *Ransomware*.

Para que el ataque sea exitoso, el sistema de la víctima debe tener alguna vulnerabilidad en el sistema operativo activa, es decir, encontrar un defecto en la seguridad de un sistema, el cual le permite al atacante aprovechar esta brecha para su propio beneficio y generar en el sistema un comportamiento irregular. Los atacantes una vez identifican la vulnerabilidad, proceden a construir el respectivo *exploit*, que persigue el objetivo de concretar un determinado ataque, como lo puede ser: acceso de forma no autorizada, toma de control, escalar privilegios o directamente ataques de denegación de servicio.

El tipo de *Ransomware* que más afecta a las organizaciones es el *Criptomalware*, su impacto es muy alto en la infraestructura tecnológica. Incluso puede llegar a paralizar la operación de las empresas, ya que deja sin acceso a ninguno de los

archivos, esto mediante el cifrado de los archivos, que consiste en la codificación de información sensible para poder evitar que esta llegue a personas no autorizadas.

Wil Allsopp, en su libro: *Advanced Penetration Testing*: *Hacking the World's Most Secure Networks*, hace referencia a que: “desde la perspectiva del *ransomware*, la criptografía asimétrica es útil porque significa que los archivos se pueden bloquear y, a cambio de un rescate, se proporciona algo tangible para recuperarlos, algo que de ninguna manera la víctima podría adquirir”[20], y esa es la clave secreta.

Una amenaza, es un evento que cuenta con el potencial de causar daño o pérdida, este es el caso del *Scareware*, que es un software falso, que se hace pasar por una aplicación legitima como antivirus o una herramienta de limpieza, optimización, la cual asegura haber detectado amenazas activas en el computador, a su vez exige dinero para que el *software* le ayude a resolver el problema, o como el *Doxware* (o *leakware*), que amenaza a la víctima con publicar en internet, la información que le ha extraído si no se realiza el pago antes del tiempo que el atacante establezca.

Ha sido tan exitoso este tipo de ataque, que los delincuentes han optado por ofrecerlo como servicio, se denomina: RaaS (*Ransomware as a Service*), aquí el *malware* es manejado por un tercero que se encarga de distribuir la campaña de *Ransom*, cobrar los rescates y gestionar los descifradores, todo esto a cambio de un porcentaje del valor del rescate. Esto demuestra que no se requiere un alto nivel de conocimientos técnicos para hacer daño, es posible contratar a alguien que ejecute el ataque.

Por otra parte, en el año 2016, la Europol, *Politie* (Holanda), *Kaspersky* y *McAfee* lanzan el proyecto *NoMoreRansom*, el cual es un esfuerzo conjunto entre fuerzas y

[20] ALLSOPP, Wil. Advanced Penetration Testing : Hacking the World's Most Secure Networks. San Francisco: John Wiley & Sons, Incorporated. 2017. p.147. ISBN 9781119367680

cuerpos de seguridad y compañías tecnológicas, para disminuir el impacto de las operaciones de los cibercriminales que lanzan ataques de *ransomware*.

Para *NoMoreRansom* es claro que es más factible evitar la amenaza, que revertir los daños causados a causa de un ataque, por esta razón este proyecto también se dirige a la etapa de educación y formación de usuarios sobre cómo funciona el *ransomware* e informar oportunamente sobre las contramedidas se pueden tomar para prevenir eficazmente una infección. Desde su lanzamiento, se han incorporado nuevas entidades y organizaciones a esta lucha contra el *ransom*, como lo son: *Avast, Bitdefender, Eset, Emisoft, Check Point, Trend Micro, Kisa, ElevenPaths, Cisco, F-secure, Bleeping Computer, Tesorion*, Policía de Bélgica, Policía de Rumania, Policía de Francia; además de muchas fuerzas de seguridad, en donde se destaca a nivel Latinoamericano la presencia de la Policía de Colombia.

Un control clave hoy para recuperarse de los ataques de *ransomware* es la restauración de los archivos de datos utilizando las copias de seguridad obtenidas a través del proceso documentado de recuperación ante desastres. “Si estos controles no están establecidos e integrados con la continuidad del negocio, los datos pueden ser irrecuperables y si no se definen procesos efectivos, la demora en el procesamiento puede ser inaceptable”[21]. Lo anterior de acuerdo con Domenic Antonucci.

[21] ANTONUCCI. Domenic. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. San Francisco: John Wiley & Sons, Incorporated. 2017. p.137. ISBN 9781119308805

5. DESARROLLO DE LOS OBJETIVOS

Con el propósito de comprender el origen, características, tipos, metodologías y medidas de protección ante el *Ransomware*, se realiza una recopilación sobre los antecedentes documentales que se relacionan directamente con el tema.

5.1 DEFINICION DE *RANSOMWARE*

En la XVI Jornada internacional de seguridad informática, organizada por ACIS "Asociación Colombiana de Ingenieros de Sistemas", se hace referencia sobre el *Ransomware* como una "familia de *malware*, la cual tiene como particularidad que al activarse dentro del sistema hace la búsqueda de información, documentos, imágenes o archivos, entre otros, con el fin de cifrarlos"[22]. Una vez se completa la tarea de cifrado, genera un mensaje indicando los pasos a seguir para obtener la clave que le permita recuperar o tener nuevamente acceso a los archivos cifrados.

Para *Sophos*, en el documento "Cómo protegerse del *Ransomware*", resalta que "es una de las amenazas con mayor potencial para extenderse y perjudicar"[23]. Desde la detección de *CryptoLocker* en 2013, se ha observado una nueva generación de múltiples variantes de *ransomware*, que se difunde por medio de mensajes de correo electrónico y *spam*, con la finalidad de extorsionar tanto a usuarios particulares como a organizaciones.

[22] ACSIS. Entendiendo el Ransomware. [Sitio web]. Bogotá: BELLO VIEDA, Jaime Andrés. [Consulta: 5 de mayo 2020]. Disponible en: https://acis.org.co/archivos/JornadaSeguridad/Memorias/15.pdf

[23] SOPHOS. Cómo protegerse del Ransomware. [Sitio web]. Abingdon: Sophos. [Consulta: 5 de mayo 2020]. Disponible en: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophosransomwareprotectionwpna.pdf?la=es-ES

Por otra parte, *Trend Micro*, en el *whitepaper*: Proteja su organización del *ransomware* manifiesta que: “es un tema de crimen, no una simple amenaza”[24], e indica como en América Latina está afectando a la mayoría de las empresas, sin importar actividad económica o la cantidad de empleados, con el afán de extorsionarlas a cambio de devolver la información de sus usuarios críticos y servidores.

5.2 CARACTERISTICAS DEL RANSOMWARE

Para lograr entender la naturaleza de los ataques de *ransomware*, es fundamental realizar la caracterización e identificación de los principales atributos que componen a este *malware*. Esta problemática se presenta a nivel mundial, es por esto por lo que las diferentes compañías dedicadas a la seguridad informática y los entes de estado encargados de la ciberseguridad, han establecido estrategias para mitigar el riesgo asociado, pero la posibilidad de recuperar la información que ha sido secuestrada es muy baja.

En el documento “*The Smarter SMB’s Guide to Ransomware*”, de la compañía Milner expertos en ciber seguridad, resaltan que “cada variante de *ransomware* tiene sus propias características y particularidades, pero en principio existen algunos componentes clave que comparten”[25], como lo son:

- Propagación de las campañas de *ransomware* por correo electrónico, esto es en principio norma general, pero existen algunas variantes que se descargan a través de publicidad, sitios web maliciosos o un archivo. En las variantes que se transmiten vía email lo hacen falsificando los remitentes, con el fin de generar

[24] TREND MICRO. Proteja su organización del ransomware. [Sitio web]. Tokio: Trend Micro. [Consulta: 5 de mayo 2020]. Disponible en: https://resources.trendmicro.com/rs/945-CXD-062/images/Solution_Brief_Ransomware_Enterprise.pdf

[25] MILNER. The Smarter SMB’s Guide to Ransomware. [Sitio web]. [Consulta: 5 de mayo 2020]. Disponible en: https://www.milner.com/docs/default-source/ebooks/milner-ebook_smb_ransomware_guide.pdf?sfvrsn=49ede358_6

confianza en el destinatario del correo para que descargue el archivo adjunto .zip o .rar, los cuales contienen archivos .exe que agregan claves al registro de Windows, esto posteriormente le permite ejecutarse.

- Comunicación encubierta, en cuanto el *malware* es descargado y ejecutado en el equipo, establece comunicación con el servidor de comando y control (C&C).

- Cifrado avanzado, una vez establecida la conexión con el servidor, se generan las claves de cifrado: una pública, una privada. La mayoría de las variantes de *ransomware* usan una clave 256-AES (Advanced Encryption Standard) o una clave 2048-RSA, pero algunas incluso pueden ir tan lejos como 4096-RSA.

- Rescate en criptomonedas, terminado el proceso de cifrado, para recuperar la información o control del sistema, los ciber delincuentes normalmente exigen un pago en bitcoin o cualquier otra criptomoneda. Aunque bitcoin es la más utilizada.

- Plazo ajustado o limitado, con el fin de ejercer presión sobre la víctima, en el sistema infectado aparece una ventana que informa sobre lo sucedido, la encriptación de los archivos y establece un tiempo límite para realizar el pago, y de no ser efectuado dentro del plazo estipulado, los archivos ya no podrán ser recuperados, puesto que la clave de cifrado será destruida.

McAfee Labs predice: “algunas técnicas de *ransomware* que los desarrolladores pueden emplear pronto”[26], las cuales son:

- Cifrado de nombres: las últimas versiones de *ransomware* ahora cifran los nombres de los archivos junto con cada archivo de datos. Los archivos cifrados tienen nombres compuestos al azar números y letras.

[26] MCAFFE. Understanding Ransomware and Strategies to Defeat it” [Sitio web]. [Consulta: 5 de mayo 2020]. Disponible en: http://www.mcafee.com/it/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf

- Copia de seguridad y publicación: algunos *ransomware* han movido copias de los archivos a servidores de los atacantes y, si no paga el rescate, publicaran los archivos en Internet.

- Sitios web: El *ransomware* se inyectará en sitios web con vulnerabilidades conocidas y una vez se ejecute en la máquina de la víctima cifrará todos los archivos en los directorios de inicio.

5.3 FASES EN UN ATAQUE TÍPICO DE *RANSOMWARE*

Las fases típicas en un ataque de *ransomware* son:

Fase 1. Infección: una vez enviado al sistema a través de un archivo adjunto de correo electrónico, generalmente utilizando la técnica de *phishing*, una aplicación infectada u otro método, el *ransomware* se instala en el equipo de la víctima y en cualquier dispositivo de red al que pueda acceder.

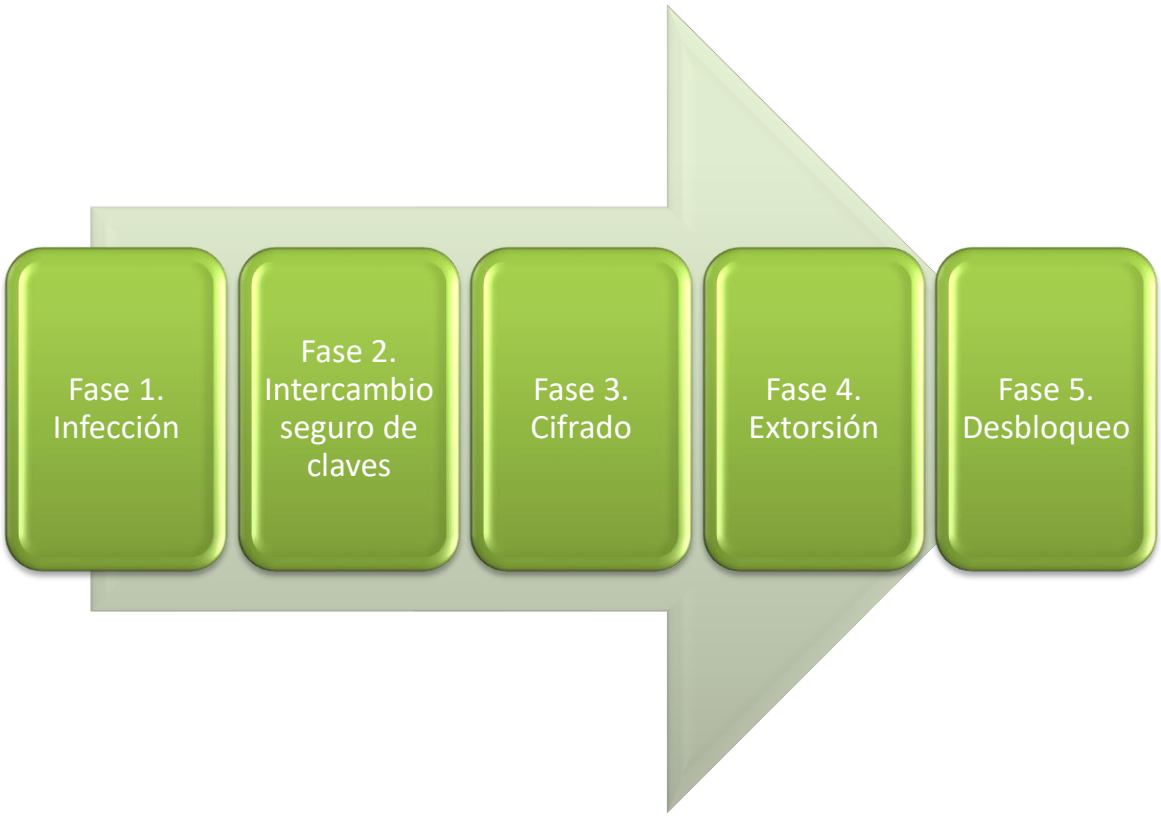
Fase 2. Intercambio seguro de claves: el *ransomware* se pone en contacto con el servidor de comando y control operado por los ciberdelincuentes detrás del ataque para generar las claves criptográficas que se utilizarán en el sistema local.

Fase 3. Cifrado: el *ransomware* empieza a cifrar cualquier archivo que pueda encontrar en la máquina local y en la red.

Fase 4. Extorsión: una vez se ha completado el cifrado, el *ransomware* muestra las instrucciones para realizar el pago de rescate de la información o el sistema afectado, del mismo modo se advierte al usuario que de no realizar el pago dentro del tiempo establecido los datos serán destruidos.

Fase 5. Desbloqueo: las organizaciones o los usuarios pueden pagar el rescate y esperar que los ciberdelincuentes descifren los archivos afectados, o pueden intentar la recuperación eliminando los archivos y sistemas infectados de la red y restaurando los datos desde copias de seguridad limpias.

Figura 2. Fases de un ataque



Fuente: Elaboración propia

Por otra parte, al negociar con ciberdelincuentes es a menudo una causa de pérdidas económicas, ya que un informe reciente encontró que: “el 42% de las organizaciones que pagaron un rescate no consiguieron descifrar sus archivos”[27].

[27] DATACENTER KNOWLEDGE. Ransomware has crippled your data center – now what? [Sitio web]. [Consulta: 5 de febrero 2021]. Disponible en: https://tmt.knect365.com/uploads/DCK-datacenter-ransomware-guide2019-9afd99804b7529633e4a7d8972eb86f2.pdf

5.4 TIPOS DE *RANSOMWARE* LANZADOS DESDE 2015

En esta sección de la monografía, se describen las clases de *ransomware* y las variantes más relevantes que se han lanzado desde el año 2015.

5.4.1 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 que existen.

5.4.1.1 *Ransomware* de cifrado: este tipo cifra todos los archivos del equipo, documentos, hojas de cálculo, pdf, imágenes, videos. un ejemplo de este tipo es *CryptoLocker*. En la siguiente imagen se muestra un pantallazo de un equipo afectado con este tipo de *malware*.

Figura 3. Variante de *CryptoLocker*

Fuente: WELIVESECURITY. El FBI advierte sobre el crecimiento del ransomware. [En línea]. Eset Latinoamérica. (Recuperado en 5 mayo 2020) Disponible en: https://www.welivesecurity.com/la-es/2015/01/26/fbi-crecimiento-ransomware/

El *ransomware* criptográfico 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 lo 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. “La mayoría de las familias modernas de *ransomware* criptográfico utilizan esta técnica para que aproveche ambos tipos de cifrado”[28].

5.4.1.2 *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. Cuando el usuario intenta iniciar sesión, el *ransomware* del

[28] ALMASHHADANI, Ahmad. A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware. IEEE Access. 2019, vol. 7, s. 47053-47067. ISSN 2169-3536.

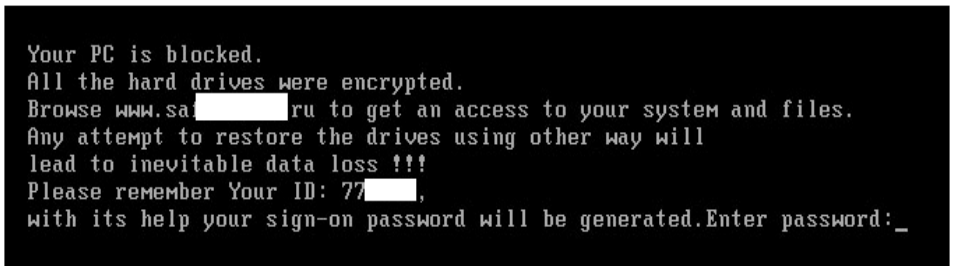
bloqueador de pantalla mostrará una ventana emergente exigiendo el pago. A continuación, la figura 4 muestra como este *malware* bloquea la pantalla.

Figura 4. *Screenlocker ransomware*

Fuente: BEST SECURITY SEARCH. Your computer is locked! Screenlocker Ransomware Virus. [En línea]. [Consultado: 05 mayo2020]. Disponible en: https://bestsecuritysearch.com/computer-locked-screenlocker-ransomware-virus-removal-steps-protection-updates/

5.4.1.3 *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. El *ransomware* realmente cifra la tabla de archivos maestra (MFT). Este es un archivo especial en particiones NTFS que contiene información sobre todos los demás archivos: su nombre, tamaño y asignación a los sectores del disco duro. En el computador infectado aparece un mensaje similar al siguiente:

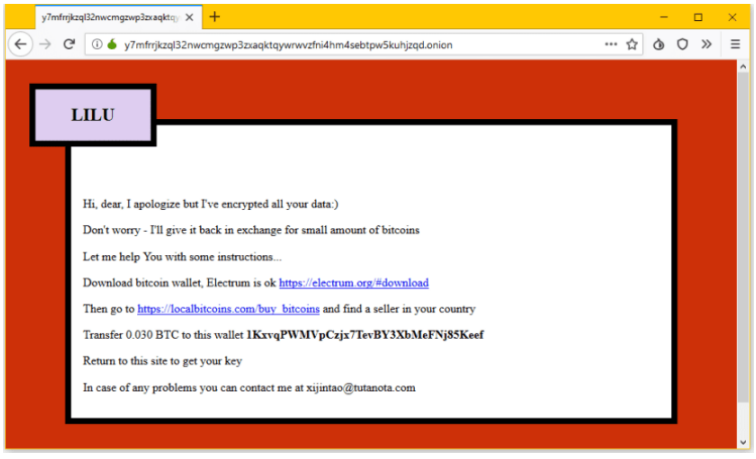
Figura 5. *MBR Ransomware*



Fuente: KASPERSKY. And Now, an MBR Ransomware. [En línea]. Security list. [Consultado: 05 mayo2020]. Disponible en: https://securelist.com/and-now-an-mbr-ransomware/30626/

5.4.1.4 *Ransomware* de cifrado de servidores *web*. Está orientada 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, como es el caso de *Lilu.* Los servidores afectados muestran un mensaje de este tipo:

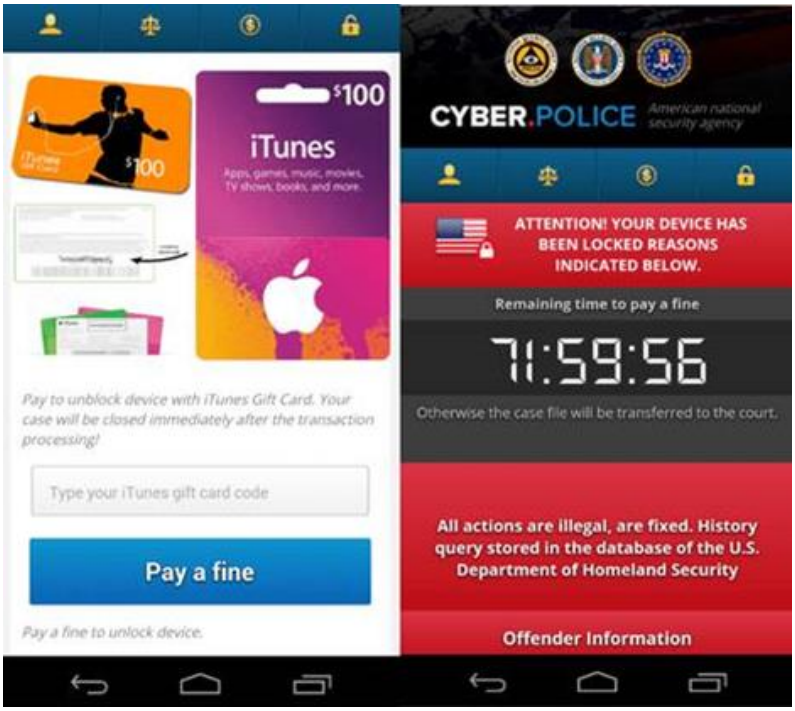
Figura 6. *Lilu Ransomware*



Fuente: DESDE LINUX. Lilu, nuevo ransomware infecta miles de servidores basados en Linux [En línea]. [Consultado: 05 mayo2020]. Disponible en: https://blog.desdelinux.net/lilu-nuevo-ransomware-infecta-miles-de-servidores-basados-en-linux/

5.4.1.5 *Ransomware* de dispositivos móviles. Está dirigida a los dispositivos *Android* principalmente, pueden infectarse a través de aplicaciones no oficiales. El *ransomware* generalmente termina en un teléfono móvil gracias a un ataque de ingeniería social. Por ejemplo, los atacantes engañarán al usuario para que descargue *malware* instalando una aplicación falsa de una tienda de aplicaciones de terceros, o haciendo clic en un enlace de spam en las redes sociales o enviado por SMS. Un ejemplo es *FLocker*, el cual muestra en las pantallas de los dispositivos lo siguiente:

Figura 7. *FLocker Ransomware*



Fuente: Centro de respuestas ante incidentes cibernéticos. FLocker, un ransomware para Android que afecta a Smart TVs. [En línea]. [Consultado: 05 mayo 2020]. Disponible en: https://www.cert.gov.py/index.php/noticias/flocker-un-ransomware-para-android-que-afecta-smart-tvs

5.4.1.6 *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 vulnerable y se pueden ver afectados con

facilidad. De tal forma que ha sido posible encontrar vulnerabilidades que le permiten a los ciberdelincuentes infectar con *ransomware* hasta cafeteras como se puede evidenciar en la siguiente imagen:

Figura 8. Máquina de café infectada con *Ransomware*

Fuente: Hackread. White hat hacker infects smart coffee machine with ransowmare. [En línea]. [Consultado: 05 diciembre 2020]. Disponible en: https://www.hackread.com/white-hat-hacker-smart-coffee-machine-ransowmare/

5.4.2 VARIANTES DE *RANSOMWARE*. A medida que surgen nuevas variantes de *ransomware,* ya que los atacantes buscan a través de nuevas variantes y funcionalidades, puede resultar complicado 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 que existen:

- ***Ransomware Ryuk***. Especialmente efectivo en el año 2019 y se han detectado ataques particularmente fuertes en América Latina. Un caso muy mencionado fue el de la empresa nacional de petróleo mexicana, PEMEX, la cual tuvo que cerrar completamente en noviembre de 2019 debido a un incidente de seguridad relacionado con el *ransomware Ryuk.*

Esta variante es muy peligrosa porque su propósito es infectar un sistema y posteriormente esconderse por un lapso, mientras este *malware* busca los sistemas más críticos en la red para maximizar su impacto. “Numerosas organizaciones latinoamericanas han sufrido por infecciones de *Ryuk* a finales de 2019”[29]. Se cree que el *ransomware Ryuk* es operado por el mismo grupo que gestiona el *malware Trickbot*, un grupo conocido como *Wizard Spider*, que proviene de Rusia.

- ***Ransomware Phobos***. Esta variante utiliza servicios vulnerables que las empresas subcontratan y aprovechando esto ganan acceso. Actualmente es la variedad más común en el momento, ya que está presente en el 70% de los incidentes por *ransomware*, esto lo han determinado *Intsights defend forward*. Una vez dentro, extraen credenciales válidas y se mueven lateralmente hasta que logran llegar al servidor del Directorio Activo.

Posteriormente, deshabilitan el *firewall* de *Windows* y a veces desinstalan soluciones EDR y antivirus, antes de distribuir el *malware* utilizando Directiva de Grupo. No cifran la red por completo, se concentran únicamente en los servidores más críticos de la empresa al mismo tiempo que causan traumatismos significativos en las operaciones cotidianas.

- ***Cosmic Banker***. Es un *malware* que ha impactado en bancos latinoamericanos desde el 2018. *Scitum* lo detectó en 2019 cuando hubo una distribución masiva. Una de las características más relevantes es que el archivo ejecutable contenía comentarios muy específicos en portugués, que también habían sido detectados en otros incidentes.

[29] INTSIGHTS. El Lado Oscuro de América Latina. [Sitio web]. [Consulta: 07 de mayo 2020]. Disponible en: https://wow.intsights.com/rs/071-ZWD-900/images/Span_El%20Lado%20Oscuro%20de%20Ame%CC%81rica%20Latina.pdf

La campaña se enfoca en las credenciales de entidades bancarias mexicanas. No obstante, el grupo detrás de *Cosmic Banker* también es autor de otra campaña que se enfoca en usuarios de entidades bancarias de Brasil. Algunos de los elementos del ataque coinciden con un artefacto malicioso, bautizado por *Trend Micro* como *Banload*, el cual afectó a varios bancos en Brasil.

- ***Catasia***. Este *ransomware* distribuía correos electrónicos suplantando diferentes organizaciones gubernamentales mexicanas. Los correos contenían un documento en Word con macros que descargaban el *malware* en segundo plano cuando se habilitaba dicha función. El programa maligno es capaz de acceder a la cámara web y micrófono de la víctima, permitiendo grabación de video y voz.

En versiones más recientes, se hace el envío de correos con archivos .zip en lugar de documentos en *Word*. La característica más resaltante de este *malware* es que el atacante actualiza su funcionalidad, para incluir ataques de hombre en el medio a navegadores. El *malware Catasia* ha tenido éxito al ser alojado en infraestructuras que no son maliciosas, donde también se alojan operaciones de negocios legítimas. La investigación arrojó que solo se está usando sobre objetivos mexicanos, a pesar de haber sido originado en Colombia.

- ***Trickbot***. Troyano bancario usado en ataques cibernéticos contra pequeñas y medianas empresas (PYMES). Creado para acceder a cuentas online – principalmente cuentas bancarias, para obtener información de identificación personal y luego usarla en fraude y robo de identidad. El *malware* ha evolucionado y los creadores han incluido nuevos módulos y expandido sus habilidades. El *Trickbot* se envía a través de spam malicioso que contiene documentos de Word, lo cual permite al programa maligno el robo de credenciales y la extracción de datos sensibles y valiosos.

Trickbot ha afectado a muchas organizaciones en América Latina, pero México fue atacada más fuertemente por variantes que enviaban *Emotet*. Entre finales de 2018 y finales de 2019, el número de robots infectados con *Emotet* se disparó en Sudamérica. Los huéspedes infectados incluyen organizaciones en los sectores automotriz, de finanzas, de energía, de construcción, de comercio minorista, de entretenimiento, de logística, y de tecnología.

- ***Netwalker****.* Creado por el grupo *Circus Spider* en el año 2019. *Netwalker* tiene un comportamiento similar a la mayoría de las otras variantes de *ransomware*, utilizando como vector de ataque principal los correos electrónicos de *phishing*, seguidos de la filtración y el cifrado de datos confidenciales para mantenerlos como rehenes a cambio de un gran rescate.

Netwalker a diferencia de otras cepas de este *malware* además de cifrar los datos, sino se realiza el pago *Circus Spider* amenaza con exponer una parte de estos en línea, y si la víctima no cumple con sus demandas dentro del tiempo establecido, liberará el resto de la información en la web oscura.

- ***Emotet****.* Originalmente conocido como un troyano bancario, se conoció por primera vez en el año 2014. Su objetivo principal era interceptar las credenciales bancarias a través de ataques *man-in-the-browser*. *Emotet* ha evolucionado hasta convertirse en un conjunto de *malware* de propósito general que se actualiza automáticamente y que también actúa como cargador de *payloads* como *Qbot* y *Trickbot,* que a su vez carga *Ryuk* y *Mimikatz*.

- ***Tycoon****.* Es un *ransomware Java* multiplataforma dirigido a *Windows* y *Linux* que se ha observado desde diciembre de 2019. Se implementa en forma de un entorno de ejecución de *Java* (JRE) troyanizado y aprovecha un formato de imagen de *Java* oscuro para pasar desapercibido.

Se observó que los ciberdelincuentes detrás de *Tycoon* utilizaban mecanismos de entrega altamente específicos para infiltrarse en pequeñas y medianas empresas e instituciones en las industrias de educación y *software*, donde procedían a cifrar servidores de archivos y exigir un rescate. Sin embargo, debido a la reutilización de una clave privada *RSA* común, puede ser posible recuperar datos sin necesidad de pago en variantes anteriores.

- ***MAZE***. Es un *malware* dirigido a organizaciones de todo el mundo. Se cree que *Maze* opera a través de una red afiliada donde los desarrolladores comparten sus ganancias con varios grupos que lo implementan en redes organizacionales. Lo que genera más preocupación no es solo la penetración en la organización, los operadores de este *ransomware* tienen la reputación de aprovechar los activos en la red infectada para moverse lateralmente a otras redes. En el caso que la empresa afectada sea un proveedor de servicios de TI, probablemente esta infección puede aprovecharse para atacar a los clientes que dependen de sus servicios de TI.

5.5 ATAQUES RELEVANTES DE *RANSOMWARE* EN AMERICA LATINA

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”[30].

El mencionado informe, fue elaborado en alianza con Cisco, McAfee, Microsoft, Absolute, Fortinet y Claro, donde se afirma que la amenaza del *ransomware* en Colombia está "subestimada". A la cantidad de ataques colombianos le siguen Perú

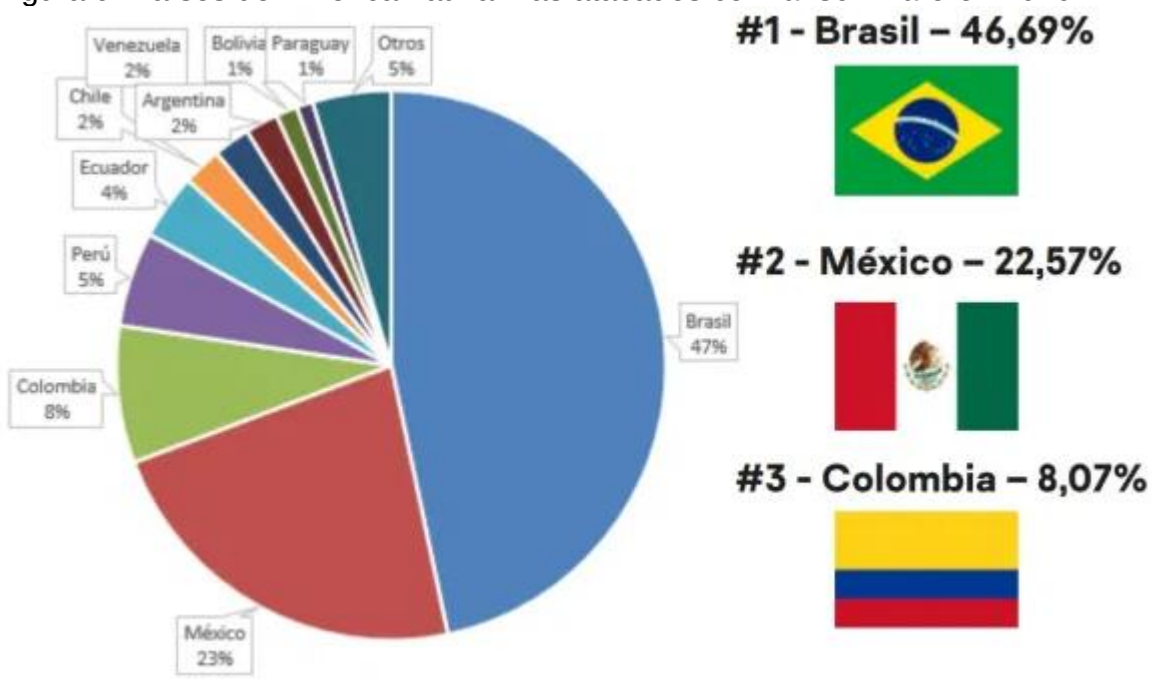
[30] COINTELEGRAPH. Colombia Is the Ransomware Capital of Latin America. [Sitio web]. [Consulta: 07 de enero 2021]. Disponible en: https://cointelegraph.com/news/colombia-is-the-ransomware-capital-of-latin-america

(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. En la siguiente figura se muestra la estadística completa.

Figura 9. Países de América Latina más atacados con *ransomware* en 2020.



Fuente: América Latina registra 5 mil ataques de ransomware por día [En línea]. [Consultado: 05 enero 2021]. Disponible en: https://www.enfasys.net/2020/10/16/america-latina-registra-5-mil-ataques-de-ransomware-por-dia/

Es importante para el presente estudio 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"[31].

- **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 operativos 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

[31] WELIVESECURITY. Ataque de ransomware afectó al Ministerio de Desarrollo Social de Panamá. [Sitio web]. [Consulta: 06 de enero 2021]. Disponible en: https://www.welivesecurity.com/la-es/2021/01/12/ataque-ransomware-afecta-ministerio-desarrollo-social-panama/

puedan utilizar. Generalmente, este tipo de *malware* pide un rescate en dinero para poder liberar los equipos”[32].

- **Compañía Telecom de Argentina:** el 18 de julio de 2020 uno de los principales proveedores de servicios de telecomunicaciones en Argentina “Telecom Argentina” 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, 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 el cual 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*”[33].

[32] LA TERCERA. CMF inició supervisión in situ en BancoEstado por ataque de ransomware y la estatal instruyó a sus ejecutivos a no conectarse a la red. [Sitio web]. [Consulta: 06 de enero 2021]. Disponible en: https://www.latercera.com/pulso/noticia/cmf-inicio-supervision-in-situ-en-bancoestado-por-ataque-de-ransomware-y-la-estatal-instruyo-a-sus-ejecutivos-a-no-conectarse-a-la-red/2QEL4J43HZF6BJ5ENWKRJAJXVQ/

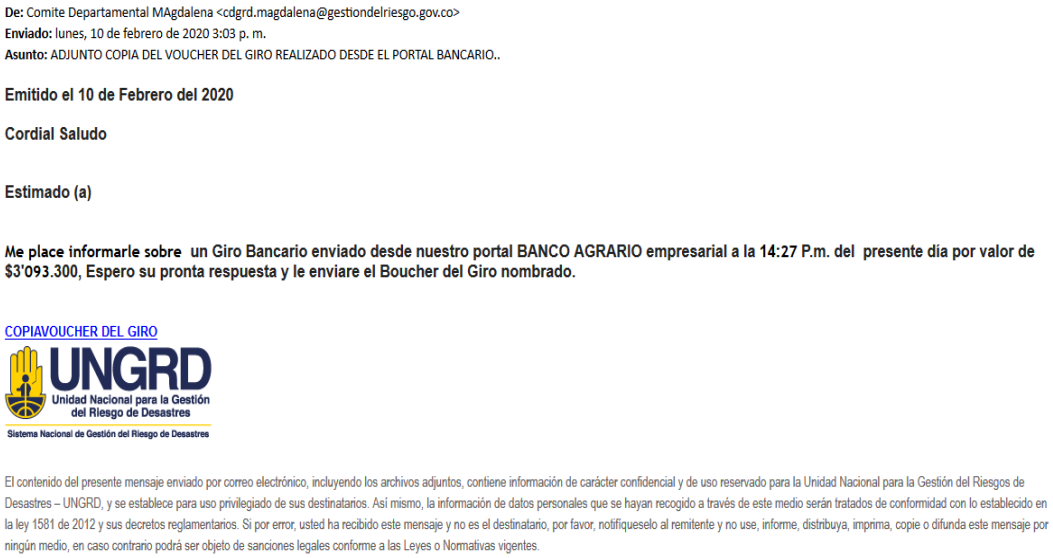
[33] Observatorio de ciberseguridad. Riesgos, avances y el camino a seguir en américa latina y el caribe. [En línea]. [Consulta: 07 de enero 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

5.6 METODOLOGIAS UTILIZADAS POR LOS ATACANTES

En la "Guía de *ransomware*" de *ESET*, "se consideran algunas de las formas en las cuales se realiza la propagación del *ransomware*"[34], son similares a las que se usan para distribuir otro tipo de *malware*. Por tanto, los vectores de infección más comunes según la guía y los medios más utilizados son:

5.6.1 Mensajes de correo electrónico con enlaces maliciosos. El método más común de infección, 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. A continuación, se muestra un ejemplo de lo anteriormente mencionado.

Figura 10. Correo con enlace malicioso.



De: Comite Departamental MAgdalena <cdgrd.magdalena@gestiondelriesgo.gov.co>
Enviado: lunes, 10 de febrero de 2020 3:03 p. m.
Asunto: ADJUNTO COPIA DEL VOUCHER DEL GIRO REALIZADO DESDE EL PORTAL BANCARIO..

Emitido el 10 de Febrero del 2020

Cordial Saludo

Estimado (a)

Me place informarle sobre un Giro Bancario enviado desde nuestro portal BANCO AGRARIO empresarial a la 14:27 P.m. del presente día por valor de $3'093.300, Espero su pronta respuesta y le enviare el Boucher del Giro nombrado.

COPIAVOUCHER DEL GIRO

UNGRD
Unidad Nacional para la Gestión del Riesgo de Desastres
Sistema Nacional de Gestión del Riesgo de Desastres

El contenido del presente mensaje enviado por correo electrónico, incluyendo los archivos adjuntos, contiene información de carácter confidencial y de uso reservado para la Unidad Nacional para la Gestión del Riesgos de Desastres – UNGRD, y se establece para uso privilegiado de sus destinatarios. Así mismo, la información de datos personales que se hayan recogido a través de este medio serán tratados de conformidad con lo establecido en la ley 1581 de 2012 y sus decretos reglamentarios. Si por error, usted ha recibido este mensaje y no es el destinatario, por favor, notifíqueselo al remitente y no use, informe, distribuya, imprima, copie o difunda este mensaje por ningún medio, en caso contrario podrá ser objeto de sanciones legales conforme a las Leyes o Normativas vigentes.

Fuente: Elaboración propia

[34] ESET. Guía de Ransomware. [Sitio web]. [Consulta: 07 de mayo 2020]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/10/guia-ransomware-eset.pdf

5.6.2 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 legitimo 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, lanzando la carga útil del *ransomware* e infectando 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 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.

Figura 11. Correo con adjunto malicioso.

Responder | Reenviar

De: E-LOTTERY ADMIN [mailto:1002njar@mol.go.th]
Enviado el: martes, 10 de marzo de 2020 12:44 a. m.
Asunto: SpamCONFIRME_SU_NOTIFICACIÓN_GANADORA_DE_MASTERCARD_DE_MARO_2020!_NÚMERO_DE_SERIE:_5388/20

MasterCard® Office 2000 Purchase Street New York USA
☎: +1-315-326-7060

REF: HWS / 200128330/19
LOTE NO: 18/203 / 225
NÚMERO DE SERIE: 5388/20
GANADOR NO: 2977172
BOLETO NO: 564-75600545- 188
CANTIDAD GANADA: $ 500,000.00 USD

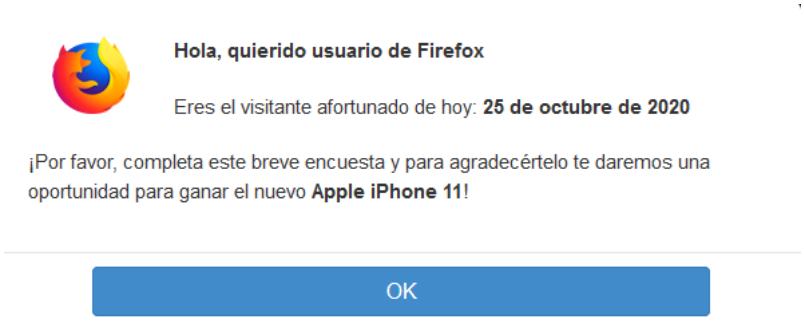
Estimado Ganador

Me complace informarle el resultado del sorteo de lotería por correo electrónico por computadora del programa MasterCard® / Bitcoin International (E-LOTTERY) que tuvo lugar el 28 de Febrero de 2020. en Nueva York, USA. Esta es una lotería generada por computadora para Usuarios de Internet que usan direcciones de correo electrónico activas y no requieren que juegues o compres ningún boleto de lotería. Este sorteo de lotería se basa completamente en la selección electrónica de ganadores que usan sus direcciones de correo electrónico de diferentes (www) sitios de la World Wide Web. Su dirección de correo electrónico se adjuntó al número ganador: 2977172 con la suma ganadora de $ 500,000 (QUINIENTOS MIL DÓLARES DE ESTADOS UNIDOS) en el archivo de crédito en efectivo con REF: HWS / 200128330/19.

Fuente: Elaboración propia

5.6.3 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 tal y como se evidencia en la figura 9.

Figura 12. Publicidad maliciosa.



Fuente: Elaboración propia

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 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*.

5.6.4 *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 el 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, 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.

5.6.5 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.

5.6.6 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.

5.6.7 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.

5.6.8 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*.

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

5.6.10 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.

5.6.11 ***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.

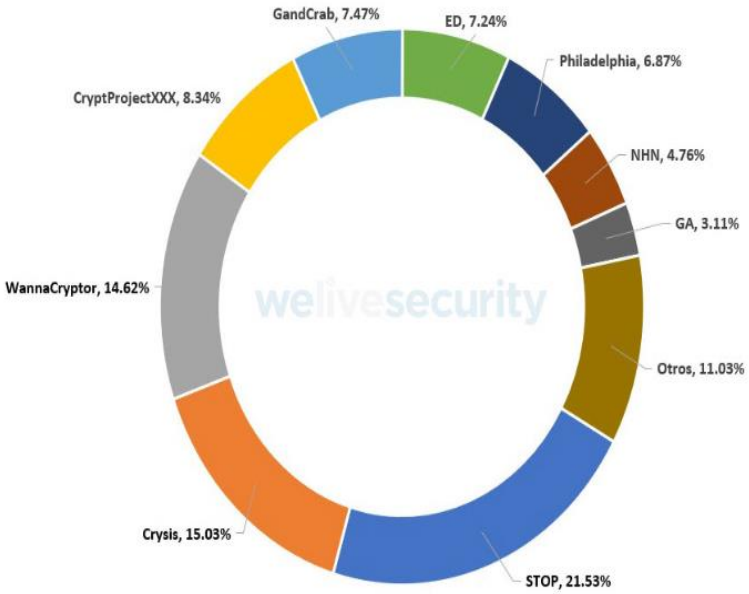
En otras palabras, pueden "ordenar" la capacidad de plagiar un sistema y mantener como rehenes los datos de otra persona. Al igual que con los rescates tradicionales, los usuarios de *ransomware* como servicio a menudo toman medidas deliberadas para hacer que sus comportamientos sean difíciles de rastrear, 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 logran identificar que algunas cepas utilizan métodos definidos que garantizan que el ataque genere el impacto esperado.

5.6.12 ***Ransomware 2.0.*** La manera en que el *ransomware* 2.0 infecta a los sistemas y se propaga a través de las redes no ha cambiado, esto se ha mantenido. 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 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 podrían 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. La siguiente imagen evidencia el tipo de *ransomware* y su cuota de participación en los ataques de este tipo.

Figura 13. Familias de *ransomware* 2019.



Fuente: WELIVESECURITY. *Ransomware*: una amenaza vigente utilizada en ataques cada vez más dirigidos. [En línea]. [Consultado: 05 mayo 2020]. Disponible en: https://www.welivesecurity.com/la-es/2020/01/09/ransomware-amenaza-vigente-utilizada-ataques-dirigidos/

Colombia, se encuentra entre los países que recibió el mayor número de ataques por *ransomware* en Latinoamérica con un total de 252”[35], lo que corresponde al 30% después de Brasil y Argentina.

[35] Cámara Colombiana de Informática y Telecomunicaciones. Ransomware, una ciberamenaza subestimada en Colombia [Sitio web]. [Consultado: 05 mayo 2020]. Disponible en internet: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Figura 14. Vectores de ataque comunes

Fuente: Cámara Colombiana de Informática y Telecomunicaciones. Ransomware, una ciberamenaza subestimada en Colombia. [En línea]. [Consultado: 05 mayo2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Como es posible evidenciar en la imagen anterior, en Colombia el principal método de difusión del *ransomware*, es a través del correo electrónico, en donde los atacantes suplantan entidades estatales y entidades bancarias, con el fin de generar en la victima una falsa sensación de seguridad y el ataque tenga un mayor porcentaje de éxito.

5.7 FORMAS DE IDENTIFICAR UN ARCHIVO ADJUNTO MALICIOSO

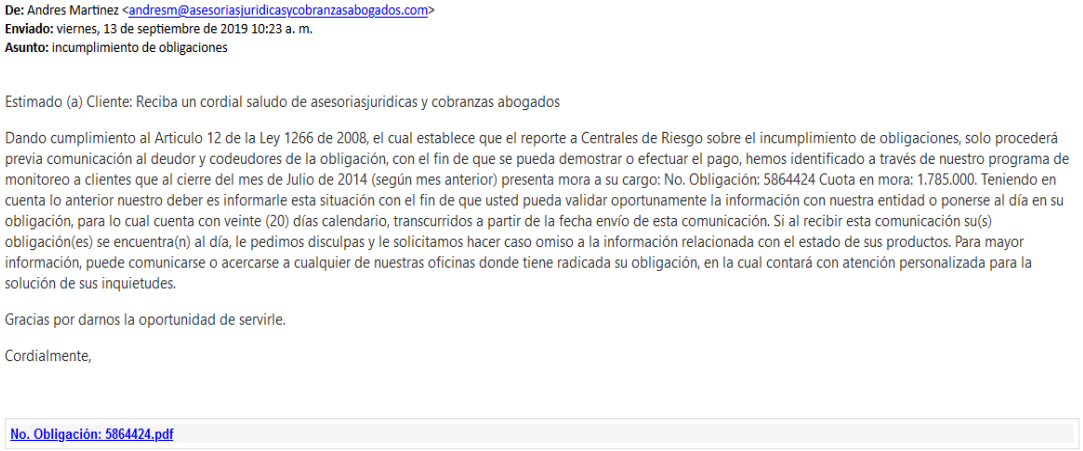
Evidentemente el *ransomware* es muy peligroso y ha logrado afectar a muchas organizaciones y a usuarios en América Latina. Para evitar problemas relacionados con este *malware*, se propone un listado de las cuatro formas para reconocer un archivo adjunto malicioso en los correos electrónicos.

- Tipos de archivos. Existe una extensa lista de archivos considerados como peligrosos o de alto riesgo, como lo son: .exe, .vbs, .wsf, .cpl, .cmd, .scr y .js lo que

muchos usuarios ignoran es que un gran porcentaje de los correos electrónicos con archivos adjuntos utilizados en campañas de difusión contienen archivos adjuntos del tipo: .pdf, .doc, .xls y .zip. Por lo que es altamente recomendable prestar atención especial a los archivos de Word, Excel y Adobe. Adicionalmente, se debe tener mucho cuidado con los nombres de los archivos. Un claro ejemplo de esto es un archivo llamado "example.exe.jpg" que efectivamente no es una imagen, pero para un usuario desprevenido este es un truco simple que resulta muy efectivo.

- Asunto urgente. Se debe tener mucho cuidado con los correos electrónicos que denotan urgencia en el asunto y en el contenido del mensaje, del mismo modo con los archivos adjuntos. Por ejemplo, si se ha recibido un mensaje del banco con un archivo adjunto que contiene la factura o extracto de la tarjeta de crédito. El signo de alarma es que en el mensaje se solicita visualizar el archivo y contactar lo antes posible o de lo contrario se tendrá que pagar unas tarifas exorbitantes o se produce algún tipo de afectación al usuario. Cuando se combina un archivo adjunto con un mensaje que tiene un sentido de urgencia puede ser un factor que juegue en contra del destinatario, ya que esto lo impulsa a abrir de manera rápida el archivo adjunto. Un ejemplo de lo anterior se puede observar en la figura 15, donde se presenta una situación que incita al usuario a tomar acciones a partir de la descarga del archivo.

Figura 15. Mensaje de correo con asunto urgente



De: Andres Martinez <andresm@asesoriasjuridicasycobranzasabogados.com>
Enviado: viernes, 13 de septiembre de 2019 10:23 a. m.
Asunto: incumplimiento de obligaciones

Estimado (a) Cliente: Reciba un cordial saludo de asesoriasjuridicas y cobranzas abogados

Dando cumplimiento al Articulo 12 de la Ley 1266 de 2008, el cual establece que el reporte a Centrales de Riesgo sobre el incumplimiento de obligaciones, solo procederá previa comunicación al deudor y codeudores de la obligación, con el fin de que se pueda demostrar o efectuar el pago, hemos identificado a través de nuestro programa de monitoreo a clientes que al cierre del mes de Julio de 2014 (según mes anterior) presenta mora a su cargo: No. Obligación: 5864424 Cuota en mora: 1.785.000. Teniendo en cuenta lo anterior nuestro deber es informarle esta situación con el fin de que usted pueda validar oportunamente la información con nuestra entidad o ponerse al día en su obligación, para lo cual cuenta con veinte (20) días calendario, transcurridos a partir de la fecha envío de esta comunicación. Si al recibir esta comunicación su(s) obligación(es) se encuentra(n) al día, le pedimos disculpas y le solicitamos hacer caso omiso a la información relacionada con el estado de sus productos. Para mayor información, puede comunicarse o acercarse a cualquier de nuestras oficinas donde tiene radicada su obligación, en la cual contará con atención personalizada para la solución de sus inquietudes.

Gracias por darnos la oportunidad de servirle.

Cordialmente,

No. Obligación: 5864424.pdf

Fuente: Elaboración propia

- Mensaje descontextualizado. Puede recibir un archivo adjunto malicioso de un compañero de trabajo o amigo. Es posible que el atacante suplante la cuenta de correo o si su cuenta se ha visto comprometida, es posible que reciba un correo electrónico malicioso, como "fotos de la última reunión". En este caso, debe evaluar el contexto del correo electrónico y, antes de hacer clic en el archivo adjunto, se debe verificar la legitimidad del mensaje de otra manera, como la comunicación vía teléfono con el remitente.

- Remitente desconocido. A menudo se reciben correos electrónicos. Por tanto, es habitual recibir mensajes inesperados e incluso no deseados (spam) que aparentemente traen propuestas interesantes. En ninguna circunstancia se debe hacer clic en los archivos adjuntos de correos electrónicos que provienen de personas que no conoce. Si no conoce al remitente del correo electrónico, ignore el mensaje y elimínelo.

5.8 MEDIDAS QUE HAN TOMADO LAS ORGANIZACIONES Y LAS PERSONAS PARA PROTEGERSE DEL RANSOMWARE

En los Estados Unidos la Oficina de Derechos Civiles (OCR), la Oficina Federal de Investigaciones (FBI) y la Comisión Federal de Comercio sugieren tomar en cuenta los siguientes concejos para prevenir los ataques de este tipo de *malware*:

- Los usuarios deben comprender que los ataques de *ransomware* ocurren todo el tiempo, constantemente los ciberdelincuentes están difundiendo este tipo de campañas, puesto que este vector de ataque ha sido muy explotado y la gran variedad de cepas existentes de este *malware*. El Departamento de Justicia de Estados Unidos ahora estima que un promedio de 4.000 ataques de *ransomware*

ocurren diariamente. Esta cifra representa un aumento del 300 por ciento de esta actividad delictiva[36]. Informes recientes indican que el sector de la salud es objetivo de este tipo de ataques con mayor frecuencia con respecto a otros sectores. El proveedor de seguridad cibernética *Solutionary* descubrió que la industria de la salud representó el 88 por ciento de todo el *ransomware* detectado el último trimestre del 2015[37]. Factores como el valor de los registros de atención médica, puesto que estos registros pueden venderse hasta 50 veces el valor de la información de una tarjeta de crédito en el mercado negro, según el FBI.

- Es importante asegurarse, en el caso de las empresas que todos los empleados reciban formación e información sobre *ransomware*. Es muy importante que los empleados estén al tanto de la amenaza que representa este *malware* y que reciban capacitación actualizada sobre lo siguiente:

Detectar el malware:

- El personal debe estar en capacidad de poder reconocer cuando se hace clic en un enlace, se abre un archivo adjunto o se visita un sitio web que pueda ser malicioso.

- El personal debe tener la capacidad de poder reconocer que cuando se produce la imposibilidad de acceder a ciertos archivos, es debido a la encriptación, eliminación y / o cambio de nombre o reubicación de datos de *ransomware*.

Prevenir el *ransomware:*

Es importante recordar al personal:

---

[36] The United States Department of Justice. How to protect your networks from ransomware. [Sitio web]. [Consulta: 06 de noviembre 2020]. Disponible en: https://www.justice.gov/criminal-ccips/file/872771/download

[37] NTT Security. Solutionary SERT Q2 report: eighty-eight percent of all ransomware is detected in healthcare industry. July 26, 2016. [Sitio web]. [Consulta: 06 de noviembre 2020]. Disponible en: https://www.solutionary.com/threat-intelligence/threat-reports/quarterly-threat-reports/sert-threat-report-q2-2016/

- Nunca se debe abrir un archivo adjunto de correo electrónico a menos que sepa qué es y confíe en el remitente.

- Nunca hacer clic en un enlace en un mensaje de correo electrónico a menos que sepan cuál es y confíen en el remitente.

- Nunca instalar o descargar software en las computadoras de la empresa, especialmente software gratuito, sin antes consultar al área de TI.

- Es fundamental hacer una copia de seguridad de los datos importantes y almacenarlos en lo posible sin conexión. Una de las formas más efectivas de protegerse en caso de un ataque de *ransomware* es mantener una copia de seguridad de la información más importante y sensible. Al implementar esta buena práctica le permitirá restaurar los datos y recuperarse rápidamente de un ataque de este tipo. Las nuevas variantes de *ransomware* eliminan o cifran las copias de seguridad en línea, por lo que se recomienda mantener las copias de seguridad fuera de línea y no disponibles en las redes.

- Cifrar los datos confidenciales, se debe considerar la posibilidad de encriptar y proteger con contraseña toda la información y los dispositivos del usuario o de los empleados.

- Asegurarse que se implementen las medidas de protección técnicas básicas. Se debe garantizar la implementación de las siguientes salvaguardas técnicas:
    - *Software* antivirus actualizado en computadoras.
    - Actualizaciones automáticas habilitadas para sistemas operativos y navegadores web.
    - Contraseñas complejas (Robustas)
    - Instalar bloqueadores de ventanas emergentes.

- Evitar la postura que adoptan muchos usuarios al pensar que sus datos o los de su empresa no son de interés para ningún delincuente. Si bien algunos ataques de *ransomware* se distribuyen a gran escala y aleatoriamente, no se debe olvidar que para los ciberdelincuentes cualquier víctima representa beneficio económico, aún más si puede afectar a empresas.

- A medida que aumenta la popularidad del *ransomware*, las empresas y los usuarios deben adoptar una mejor postura con respecto a la seguridad de la información. El creciente número de ataques es resultado directo de la facilidad con la que en la actualidad se pueden adquirir los programas de *ransomware*, incluso servicios *RaaS* (*Ransom as a Service*).

- En la red se encuentran disponibles programas de *ransomware* simples que, pagan un porcentaje de cualquier rescate cobrado a los creadores del programa. Lo cual es otra manera en la cual desde el interior de la empresa se puede producir el ataque.

- Se debe mantener informado y actualizado, en Colombia se cuenta con el Grupo de Respuesta a Emergencias Cibernéticas de Colombia COLCERT y el Equipo de Respuesta a Incidentes de Seguridad Informática CSIRT de la Policía Nacional en donde se generan alertas, notificaciones y boletines alertando a la comunidad en general de campañas de *ransomware* y de otro tipo de amenazas que utilizan técnicas similares para afectar a los usuarios.

5.8.1 Herramientas de descifrado. Existen disponibles múltiples herramientas que permiten recuperar la información cifrada por un ataque de *ransomware*, lo primero que se debe identificar es el tipo de *malware* que ha infectado el equipo para esto es importante revisar la nota de rescate, puesto que normalmente proporciona detalles sobre el tipo de *ransomware* con el que se han cifrado sus archivos, en

otras ocasiones puede suceder que la nota no tenga esta información. Para esto se debe examinar la extensión de cifrado, toda vez que cada una pertenece a un *ransomware* en específico.

En el caso que el resulte afectado por una infección de este tipo se debe considerar:

- No realizar el pago del rescate, dado que no existen garantías de que los ciberdelincuentes o creadores del *ransomware* proporcionen el acceso a los datos cifrados o le entreguen la clave para descifrarlos.

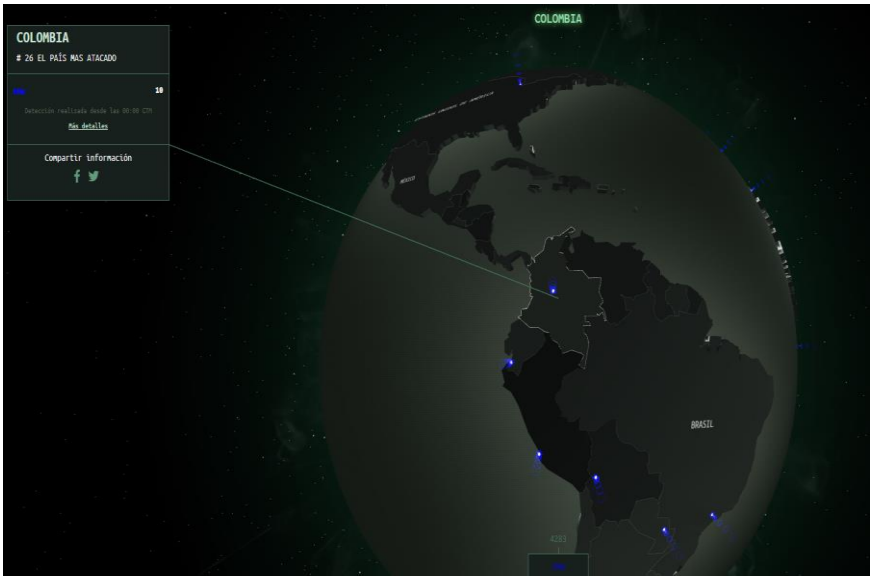
- Ubicar las copias de seguridad que estén disponibles y considerar que se mantengan las copias de seguridad en ubicaciones seguras.

- En caso de no contar con copias de seguridad, debe intentar recuperar o descifrar los datos bloqueados utilizando herramientas de descifrado de *ransomware* disponibles, las cuales se mencionan en el Anexo A.

Normalmente un rescate exigido por los ciber delincuentes no es barato y adicionalmente no hay garantía de que la información sea liberada. Por lo tanto, es conveniente si se es víctima de *ransomware*, probar herramientas de descifrado gratuitas y tratar de recuperarse del incidente sufrido.

5.8.2 Mapa de *Ransomware* en tiempo real. Esta herramienta les permite a los usuarios visualizar en tiempo real los ataques relacionados con *ransomware* detectados por esta firma de antivirus. En la siguiente imagen se puede evidenciar según la herramienta de *kaspersky*, que Colombia se encuentra en el número 26 a nivel mundial de países más atacados por *ransomware*.

Figura 16. Mapa de *ransomware* en tiempo real



Fuente:https://cybermap.kaspersky.com/special/ransomware/es?utm_source=twitter&utm_medium=social&utm_campaign=es_cibermapa_as0071&utm_content=sm-post&utm_term=es_twitter_organic_71zd7p5fd5vw688

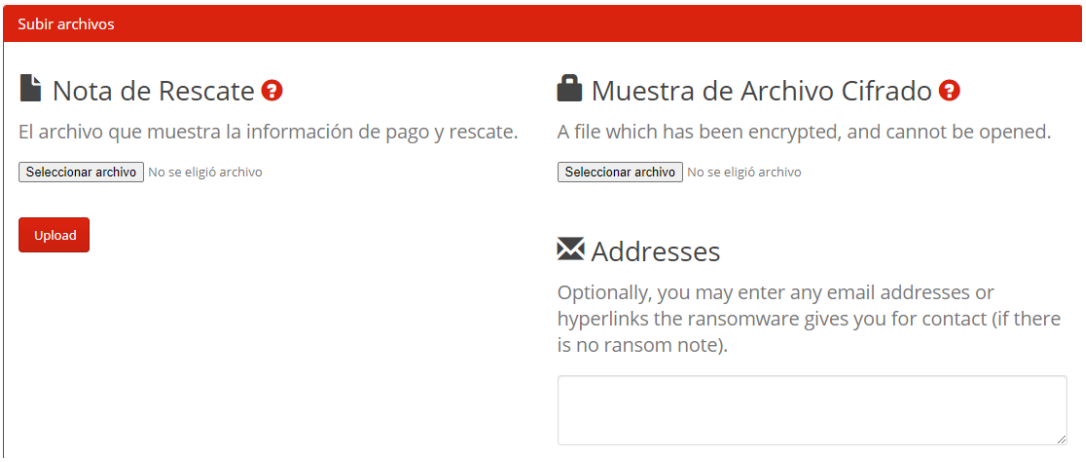
De igual forma esta firma presenta un mapa en tiempo real en donde se pueden visualizar los ataques que detecta la herramienta en tiempo real, en la siguiente imagen se observa que al momento de tomar el pantallazo Alemania es el país más atacado.

Figura 17. Mapa de ciber amenazas en tiempo real

Fuente: https://cybermap.kaspersky.com/es

5.8.3 *ID Ransomware*. Este servicio de internet permite identificar el *ransomware* que ha infectado el equipo de la víctima, esto con el fin de tomar las acciones pertinentes de acuerdo con el resultado que se obtenga de la consulta, la siguiente imagen muestra la interfaz de la aplicación, en donde es posible subir la nota de rescate o el archivo cifrado. En la figura 18 se evidencia la interfaz de la aplicación.

Figura 18. Identificar *ransomware*



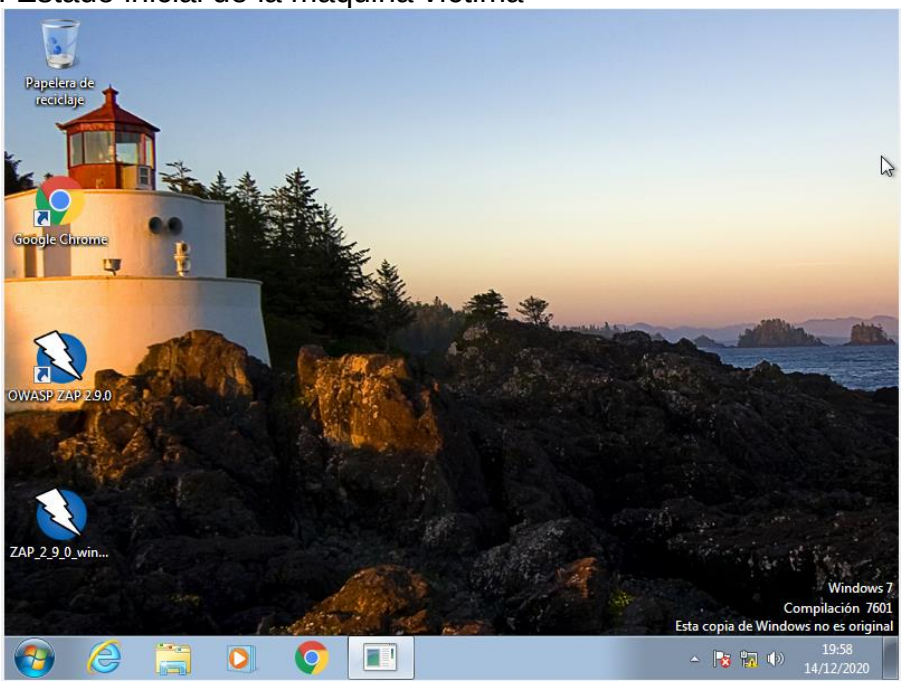
Fuente: https://id-ransomware.malwarehunterteam.com/

5.9 DEMOSTRACIÓN INFECCIÓN CON *RANSOMWARE "WANNACRY"*

WannaCry es un *ransomware* que se propagó rápidamente en mayo de 2017. Después de infectar un computador con sistema operativo *Windows*, cifra todos los archivos en el disco duro del equipo, lo que imposibilita el acceso a la información y luego exige un pago de rescate en bitcoin para obtener la clave de descifrado.

Para demostrar el proceso de infección con el *ransomware wannacry* se toma una máquina virtual con sistema operativo *Windows* 7 SP2 32 bits, se parte del supuesto que la víctima ha recibido un correo electrónico donde se adjuntan unas fotografías en un archivo comprimido.

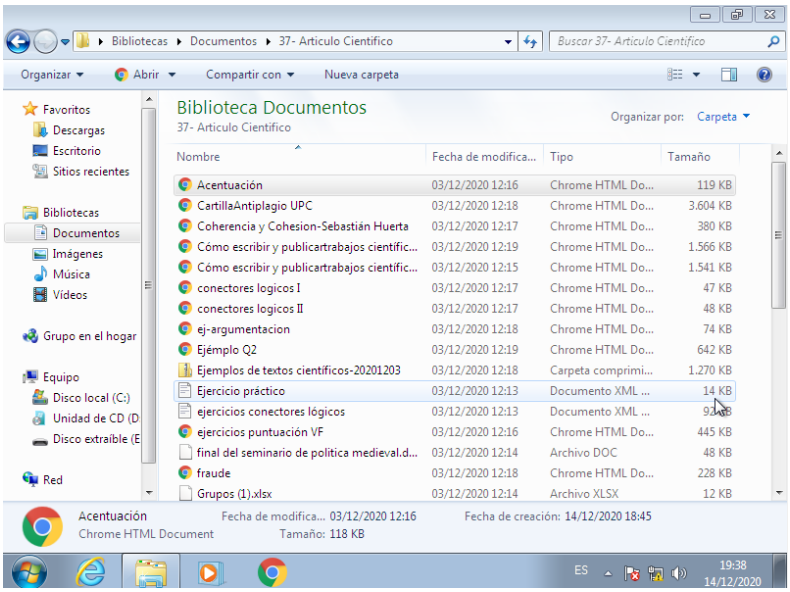
Figura 19. Estado inicial de la máquina víctima



Fuente: Elaboración propia

En la siguiente imagen se puede evidenciar el estado inicial de los documentos que se encuentran almacenados en una carpeta dentro de mis documentos.

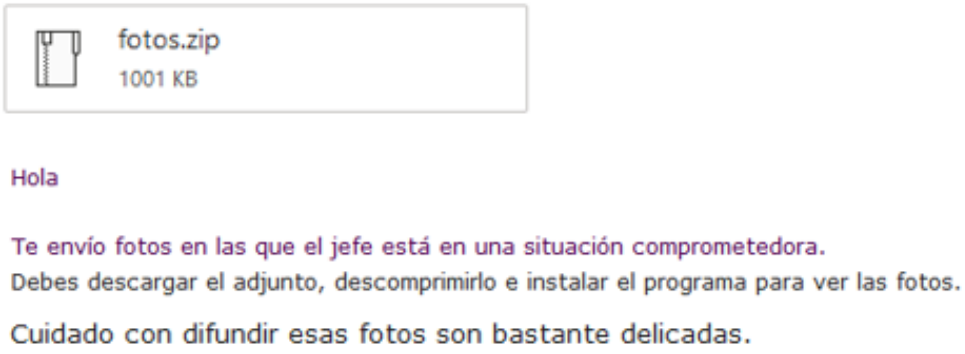
Figura 20. Estado inicial de los archivos en mis documentos



Fuente: Elaboración propia

A la víctima se le envía un email que contiene un archivo adjunto comprimido que supuestamente contiene varias fotos, como se puede evidenciar en la imagen el atacante hace creer que las fotos son de una situación comprometedora, lo que despierta la curiosidad en la persona que recibe el correo.

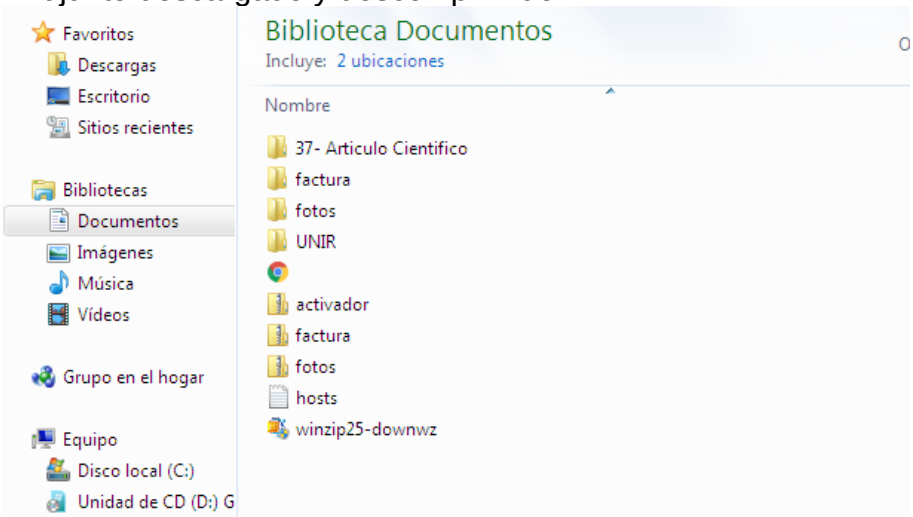
Figura 21. Mensaje de correo con el adjunto malicioso



Fuente: Elaboración propia

Una vez la víctima ha descargado el archivo adjunto procede a descomprimirlo para así poder visualizar el contenido, en el mensaje de correo el atacante da unas indicaciones para que puedan ser visualizadas las fotografías, que evidentemente no existen, el fin es lograr que el usuario ejecute el .exe

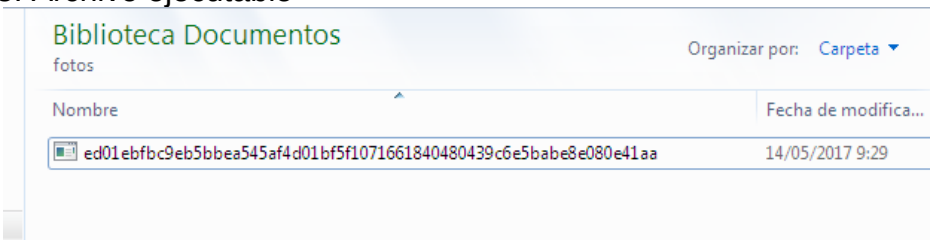
Figura 22. Adjunto descargado y descomprimido



Fuente: Elaboración propia

Una vez se ha descomprimido el archivo dentro de la carpeta se encuentra un archivo ejecutable, el cual supuestamente es un programa que permitirá visualizar las fotografías.

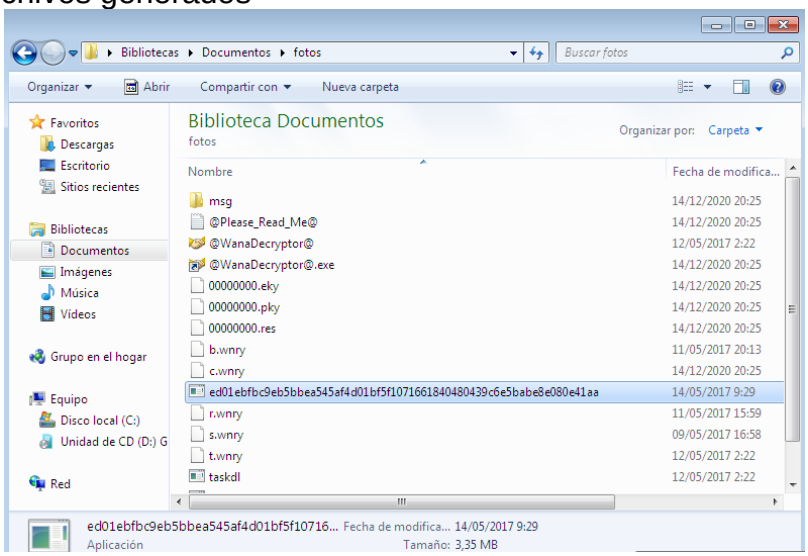
Figura 23. Archivo ejecutable



Fuente: Elaboración propia

Al ejecutar el archivo, automáticamente aparecen otros archivos en la misma carpeta, dentro de los cuales se encuentran la nota de rescate y las instrucciones para recuperar la información. Archivo *Read_Me*.

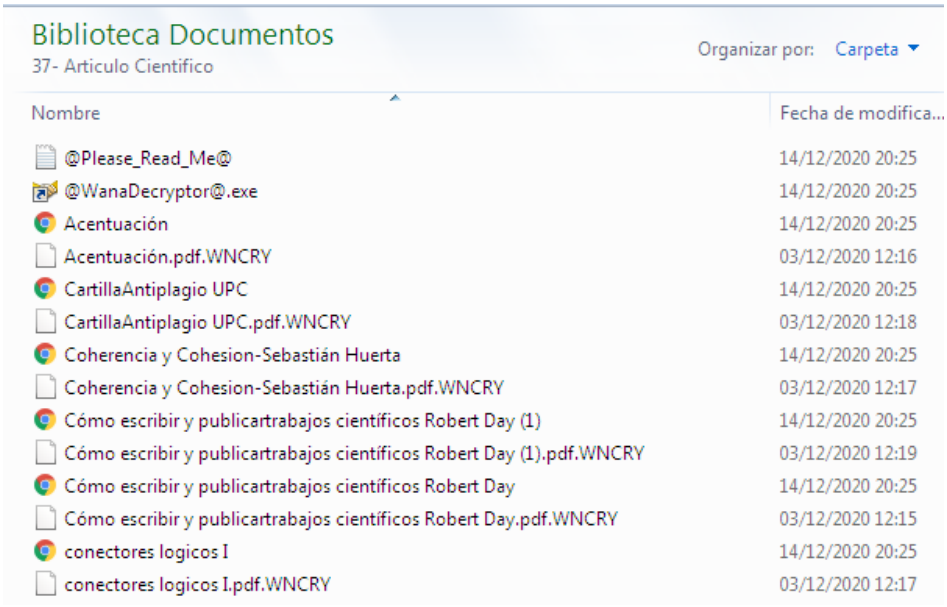
Figura 24. Archivos generados



Fuente: Elaboración propia

Al ingresar a la carpeta donde se encuentran los archivos personales, todos los documentos aparecen con la extensión .WNCRY

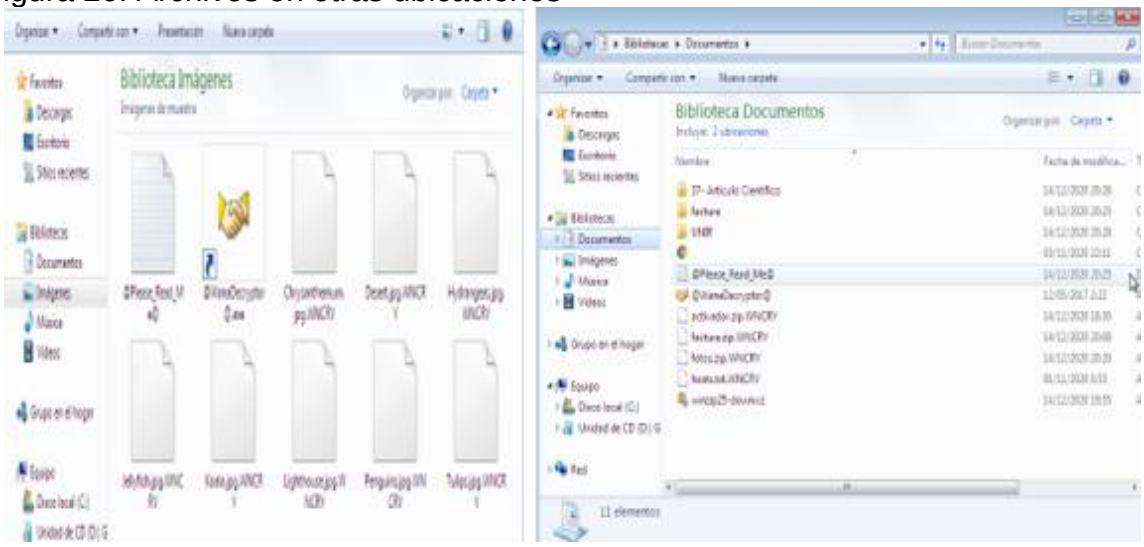
Figura 25. Archivos cifrados



Fuente: Elaboración propia

Esto no solamente en la carpeta que contiene los archivos del usuario, sino que también en otras carpetas, como: mis documentos o mis imágenes.

Figura 26. Archivos en otras ubicaciones



Fuente: Elaboración propia

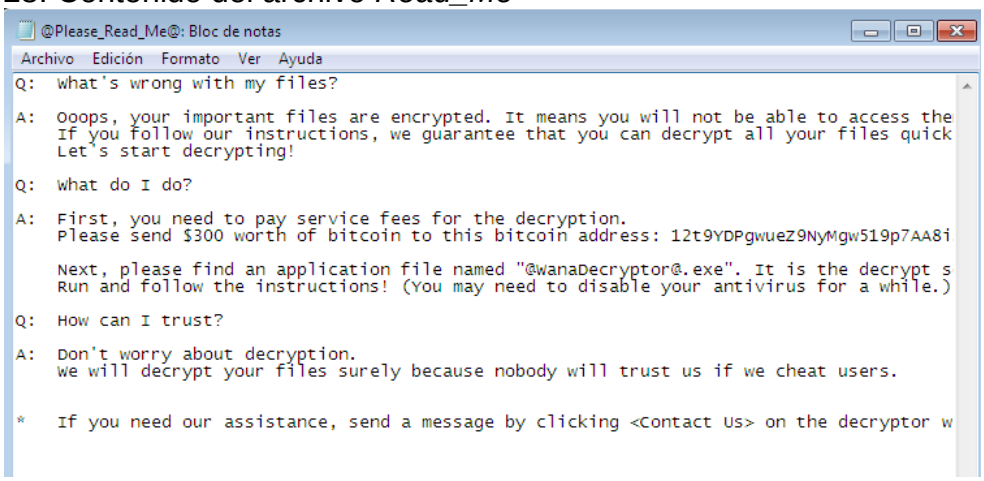
Posteriormente empieza a aparecer con frecuencia una ventana emergente que contiene en detalle las instrucciones para recuperar la información, en este caso el valor a pagar son 600 dólares en bitcoin.

Figura 27. Ventana emergente

Fuente: Elaboración propia

En el archivo léeme, se dan las indicaciones a la víctima sobre cómo puede recuperar el acceso a su información.

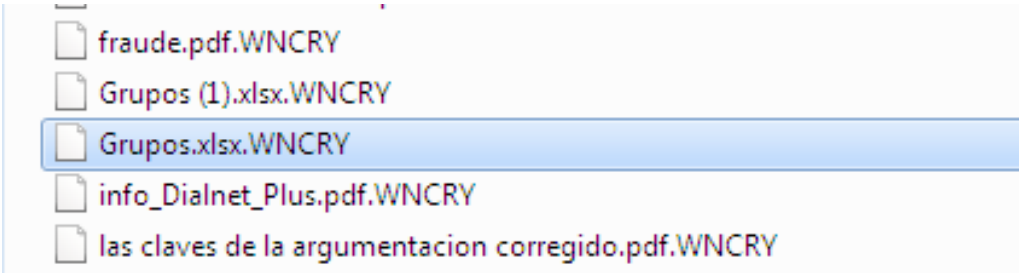
Figura 28. Contenido del archivo *Read_Me*



Fuente: Elaboración propia

Cuando el usuario intenta abrir alguno de los archivos que están encriptados, simplemente el sistema operativo no encuentra programa que le permita acceder, puesto que han sido cifrados.

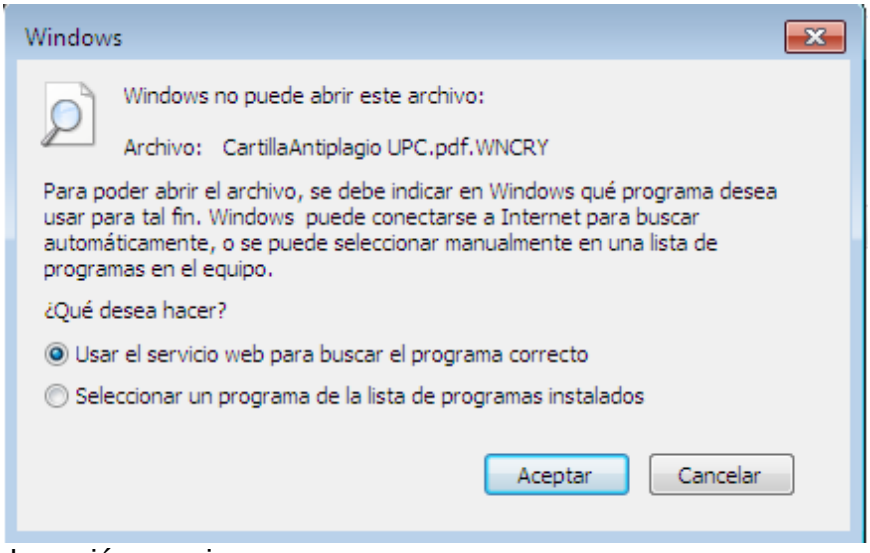
Figura 29. Archivos cifrados



Fuente: Elaboración propia

Como se menciona anteriormente el sistema operativo no puede abrir los archivos que terminan con la extensión *.WNCRY* lo que no deja muchas opciones a la víctima, ya que si son archivos con alto valor para el usuario o para una empresa, el impacto generado es muy alto.

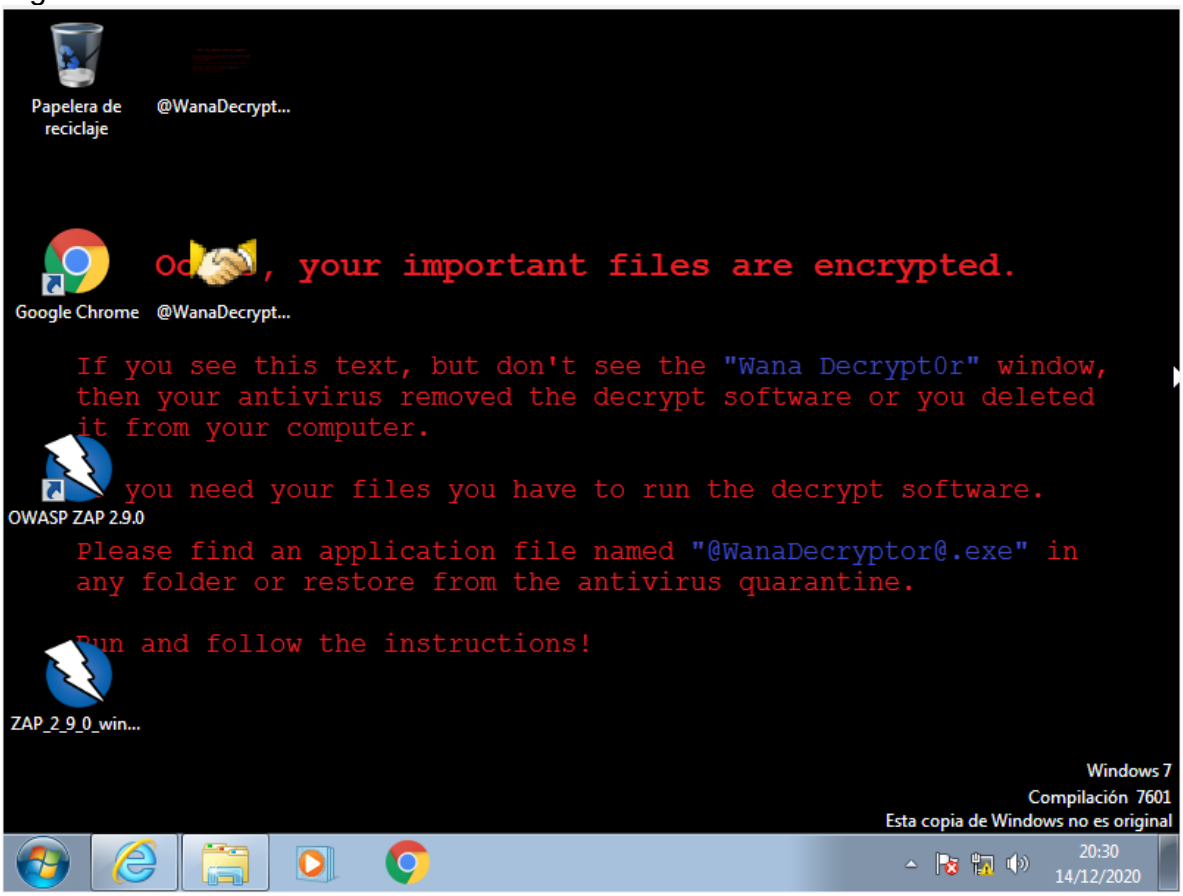
Figura 30. Windows no reconoce los archivos



Fuente: Elaboración propia

Posteriormente, en el escritorio el fondo de pantalla es cambiado y aparece el siguiente mensaje:

Figura 31. Escritorio de *Windows*



Fuente: Elaboración propia

La vulnerabilidad que *WannaCry* explota radica en la implementación de *Windows* del protocolo *Server Message Block* (SMB). Una vez que un sistema se infecta, el *ransomware* se propaga a través de la red, infectando otros dispositivos vulnerables, sin necesidad de la participación del usuario[38].

Cómo se ha podido comprobar un ataque de *ransomware* puede afectar a cualquier usuario solamente con hacer clic en un enlace o ejecutar un archivo adjunto que contiene código malicioso, muchas veces el sentido común es la herramienta más poderosa para evitar ser víctimas de estos ataques.

[38] EUROPOL. WannaCry Ransomware. [Sitio web]. [Consulta: 12 de diciembre 2020]. Disponible en: https://www.europol.europa.eu/wannacry-ransomware

5.10 COMPILADO DE BUENAS PRÁCTICAS EN CUANTO A LA PREVENCIÓN DEL *RANSOMWARE*

Uno de los objetivos del presente trabajo es generar un compilado de buenas prácticas para contribuir a la prevención de ataques de ransomware, que pueda ser útil tanto para las organizaciones como para las personas. Las recomendaciones se plantean proponiendo una serie de concejos de acuerdo con los medios más comunes de propagación de esta amenaza:

5.10.1 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 debe considerar:

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.

5.10.2 URL maliciosas. Haciendo uso del correo electrónico los atacantes envían este tipo de enlaces maliciosos, de tal forma que al igual que el método 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*.

5.10.3 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.

Consejos de prevención

- Aunque ya suene repetitivo, utilice 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.

5.10.4 MSP Y RMM. Algunos servicios resultan ser vulnerables y esta ventaja es aprovechada 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.

5.10.5 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.

5.10.6 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.

5.10.7 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.

5.10.8 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.

5.10.9 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 le *ransomware* no es la excepción y también se utiliza este medio. Por otra parte, si se permite la conexión a la red de un equipo portátil que ya este 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.
- Utilice 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.

5.10.10 *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.

- Instale 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 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.

5.11 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 al *ransomware*. En caso de sufrir un ataque de *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 no sea mayor, se debe apagar el sistema que se 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 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 sino 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 que ha sucedido realmente y que tipo de *ransomware* fue el que impacto 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.

6. 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 aspecto 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 de 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. Aunque 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 la ejecutar este tipo de ataques, desarrollan estrategias elaboradas con el único propósito de alcanzar el mayor número de víctimas que sea posible, puesto que cuanta más gente reciba el *malware* mayor será la probabilidad de infectar equipos, incluso los atacantes ofrecen el *ransomware* como servicio, en donde 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.

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, son aspectos fundamentales a tener en cuenta por los usuarios sin importar el ámbito en el que se desenvuelva, 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, implementar una solución *anti-spam*, 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 dirección, 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, con lo cual basta para que empiece el proceso de cifrado de la información y de esta manera los mantiene hasta que la víctima realice el pago.

7. RECOMENDACIONES

Para que un ataque de *ransomware* tenga éxito y logre su cometido, se basa en algo muy concreto: impedir que la víctima pueda tener acceso a sus propios archivos. Para que esto suceda previamente es necesario que el usuario intervenga en el proceso; es decir, abra el correo y ejecute el archivo adjunto. A partir de este punto ya empieza el proceso de compromiso del sistema. Una buena práctica para evitar pagar el rescate y tener toda la información disponible, es tener un respaldo de los archivos. Por tal motivo, es fundamental realizar copias de seguridad de todos los archivos importantes con regularidad.

El *ransomware* es una amenaza que ha logrado persistir en el tiempo. Desde su aparición ha ido evolucionando, utilizando métodos y algoritmos de cifrado cada vez más complejos. Por desgracia, mientras esta amenaza continúe tan rentable para los cibercriminales, estos irán perfeccionando las técnicas y se adaptaran a nuevos escenarios. De todas maneras, estas mismas técnicas de propagación seguirán vigentes: engaños, archivos adjuntos en correos electrónicos y explotación de vulnerabilidades.

Las formas de propagación del *ransomware* son diversas y cada vez los atacantes encuentran una nueva forma de engañar al usuario para que se infecte de este tipo de *malware*. Algunos de los vectores de ataque más comunes, como lo son: los archivos adjuntos maliciosos en correos electrónicos, los enlaces de phishing y los dispositivos extraíbles, se basan en errores humanos, por otra parte, la publicidad maliciosa, las descargas no autorizadas y la propagación por la red, son bastante efectivos sin requerir ninguna intervención por parte del usuario.

Sin importar la manera mediante la cual se propague el *ransomware*, existen diferentes medidas que contribuyen a reducir el riesgo de infección y mitigar los efectos de un ataque. Realizar copias de seguridad de la información relevante

periódicamente y ser muy cuidadoso con los clics, no se debe confiar en todo lo que llega a los buzones de correo, esto puede ser de gran ayuda para proteger los datos y mantener el sistema libre de *ransomware*.

Un ataque de *ransomware* fácilmente pueden paralizar una organización completamente. Puede afectar la capacidad de acceder a la información o dependiendo el tipo *ransomware* puede evitar que el usuario pueda ingresar al equipo de cómputo, lo cual causa indisponibilidad de la información o en el caso de las empresas también pueden generar que los servicios de red (página web, aplicaciones web) no estén disponibles.

BIBLIOGRAFÍA

ALLSOPP, Wil. Advanced Penetration Testing: Hacking the World's Most Secure Networks. San Francisco: John Wiley & Sons, Incorporated. 2017. p.147. ISBN 9781119367680

ANTONUCCI. Domenic. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. San Francisco: John Wiley & Sons, Incorporated. 2017. p.137. ISBN 9781119308805

ACSIS. Entendiendo el Ransomware. [Sitio web]. Bogotá: BELLO VIEDA, Jaime Andrés. [Consulta: 5 de mayo 2020]. Disponible en: https://acis.org.co/archivos/JornadaSeguridad/Memorias/15.pdf

ALLEN, Jeffrey. Surviving ransomware. American Journal of Family Law. 2017, vol. 31, no. 2, s. 65. ISSN 0891-6330.

ALMASHHADANI, Ahmad. A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware. IEEE Access. 2019, vol. 7, s. 47053-47067. ISSN 2169-3536.

BALBOA-ROMERO. Francisco José. Ransomware, hacking y phishing: conducta típica del delito de daños informáticos [en línea]. [Consulta: 22 de noviembre de 2020]. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/6929/BALBOA%20ROMERO%2c%20FRANCISCO%20JOS%c3%89.pdf?sequence=1&isAllowed=y

BBC. Guide: What is Bitcoin and how does it work? [Sitio web]. [Consulta: 15 de enero 2021]. Disponible en: https://www.bbc.co.uk/newsround/25622442

BERRUETA, Eduardo et al. A Survey on Detection Techniques for Cryptographic Ransomware. IEEE Access. 2019, vol. 7, s. 144925-144944. ISSN 2169-3536.

BITDEFENDER. What is an exploit? [Sitio web]. [Consulta: 15 de enero 2021]. Disponible en: https://www.bitdefender.com/consumer/support/answer/10556/

Cámara Colombiana de Informática y Telecomunicaciones. Ransomware, una ciberamenaza subestimada en Colombia [Sitio web]. [Consultado: 05 mayo 2020]. Disponible en internet: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

CARTWRIGHT, Anna Y CARTWRIGHT, Edward. Ransomware and Reputation. Games. 2019, vol. 10, no. 2, s. 26. ISSN 2073-4336.

CCN-CERT. Actualizado el Informe sobre medidas de seguridad contra el Ransomware. [Sitio web]. [Consulta: 1 de mayo 2020]. Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4251-actualizacion-del-informe-de-medidas-de-seguridad-contra-el-Ransomware.html

--------. Informe código dañino: Ransom.CryptoWall [Sitio web]. [Consulta: 1 de mayo 2020]. Disponible en internet: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1569-ccn-cert-id-15-16-ransom-cryptowall/file.html

--------. Informe código dañino: Ryuk [Sitio web]. [Consulta: 1 de mayo 2020]. Disponible en internet: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4217-ccn-cert-id-26-19-ryuk-1/file.html

--------. Informe código dañino: TrickBot [Sitio web]. [Consulta: 1 de mayo 2020]. Disponible en internet: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4189-ccn-cert-id-24-19-trickbot/file.html

--------. Medidas de seguridad contra el Ransomware [Sitio web]. [Consulta: 1 de mayo 2020]. Disponible en internet: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

CERT.BE. Ransomware Whitepaper. [Sitio web]. [Consulta: 15 de abril 2020]. Disponible en: https://www.cert.be/files/ransomware_whitepaper.pdf

CHAUHAN, Sudhanshu y KUMAR, Nutan. Hacking Web Intelligence: Open Source Intelligence and Web Reconnaissance Concepts and Techniques. Amtersdam: Elsevier Science & Technology Books. 2015. p.206. ISBN 9780128018675

COINTELEGRAPH. Colombia Is the Ransomware Capital of Latin America. [Sitio web]. [Consulta: 07 de enero 2021]. Disponible en: https://cointelegraph.com/news/colombia-is-the-ransomware-capital-of-latin-america

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. no. 47219. p. 1-12.

--------.-------- Ley 1273 (5, enero, 2009). "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

--------.-------- Ley 1928. (24, julio, 2018). Por medio de la cual se aprueba el «CONVENIO SOBRE LA CIBERDELINCUENCIA», Adoptado el 23 de noviembre de 2001, en Budapest. Diario Oficial. Bogotá, D.C., 2018. no. 50.664. p.1-49.

COLLIER. Roger. NHS ransomware attack spreads worldwide. Canadian Medical Association Journal (CMAJ). 2017, vol. 189, no. 22, s. E786-E787. ISSN 0820-3946.

CROKE, Lisa. Protecting your organization from e-mail phishing and ransomware attacks. AORN Journal. 2020, vol. 112, no. 4, s. P10-P12. ISSN 0001-2092.

CYWARE. Satan Ransomware: An overview of the ransomware's variants and exploits. [Sitio web]. [Consulta: 07 de octubre 2020]. Disponible en: https://cyware.com/news/satan-ransomware-an-overview-of-the-ransomwares-variants-and-exploits-35acecd3

DATACENTER KNOWLEDGE. Ransomware has crippled your data center – now what? [Sitio web]. [Consulta: 5 de febrero 2021]. Disponible en: https://tmt.knect365.com/uploads/DCK-datacenter-ransomware-guide2019-9afd99804b7529633e4a7d8972eb86f2.pdf

DANS. Enrique. El ransomware como amenaza creciente [Sitio web]. [Consulta: 07 de octubre 2020]. Disponible en: https://bv.unir.net:2257/docview/2430066216?pq-origsite=summon

DAY, Graham. Security in the Digital World: For the home user, parent, consumer and home office. Londres: IT Governance Ltd, 2017. p.64. ISBN 9781849289610

DIGITAL GUARDIAN. What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing. [Sitio web]. [Consulta: 20 de enero 2021]. Disponible en: https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

ESCRIVÁ GASCO, Gema, et al. Seguridad informática. Madrid: MacMillan Iberia, 2013. p.7. ISBN 978-841-56-5664-7

ESET. Guía de Ransomware. [Sitio web]. [Consulta: 07 de mayo 2020]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/10/guia-ransomware-eset.pdf

EUROPOL. No-More-Ransom. [Sitio web]. [Consulta: 22 de abril 2020]. Disponible en internet: https://www.nomoreransom.org/

--------. WannaCry Ransomware. [Sitio web]. [Consulta: 12 de diciembre 2020]. Disponible en internet: https://www.europol.europa.eu/wannacry-ransomware

FEDERAL BUREAU OF INVESTIGATION. Incidents of ransomware on the rise: protect yourself and your organization. [Sitio web]. [Consulta: 22 de abril 2020]. Disponible en internet: https://www.fbi.gov/news/stories/ransomware-on-the-rise

FORCEPOINT. What is Scareware? Scareware Defined, Explained, and Explored. [Sitio web]. [Consulta: 17 de enero 2021]. Disponible en: https://www.forcepoint.com/es/cyber-edu/scareware

HADNAGY, Christopher y WILSON, Paul, Ingeniería social: El arte de la piratería humana. New York. John Wiley & Sons, Incorporated, 2010. p.40. ISBN 9780470639535

HERNANDEZ-CASTRO, J., A. CARTWRIGHT a E. CARTWRIGHT. An economic analysis of ransomware and its welfare consequences. Royal Society Open Science. 2020, vol. 7, no. 3, s. 190023-190023. ISSN 2054-5703.

HERRERA SILVA, Juan A. Dataset de Ransomware basado en análisis dinámico. RISTI: Revista Ibérica De Sistemas e Tecnologías De Informação. 2019, no. E23, s. 248-261. ISSN 1646-9895.

HUNGRIA. CONSEJO DE EUROPA. (23, noviembre, 2001). Convenio sobre la ciberdelincuencia. Serie de tratados europeos. Budapest, Hungría. 2001. No. 185. P. 1-26.

INCIBE. Qué es el Ransomware y cómo recupero mi información. [Sitio web]. Madrid: Instituto Nacional de Ciberseguridad. [Consulta: 15 de marzo de 2020]. Disponible en internet: https://www.incibe.es/protege-tu-empresa/blog/el-ransomware-y-recupero-mi-informacion

--------. Ransomware: una guía de aproximación para el empresario. [Sitio web]. Madrid: Instituto Nacional de Ciberseguridad. [Consulta: 15 de marzo de 2020] Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

INFO CHANNEL. Ataques de ransomware se disparan: Kaspersky Lab. [Sitio web]. México: Staff High Tech Editores. [Consulta: 1 de mayo 2020]. Disponible en: https://www.infochannel.info/ataques-de-ransomware-se-disparan-kaspersky-lab

INTSIGHTS. El Lado Oscuro de América Latina. [Sitio web]. [Consulta: 07 de mayo 2020]. Disponible en: https://wow.intsights.com/rs/071-ZWD-900/images/Span_El%20Lado%20Oscuro%20de%20Ame%CC%81rica%20Latina.pdf

LA TERCERA. CMF inició supervisión in situ en BancoEstado por ataque de ransomware y la estatal instruyó a sus ejecutivos a no conectarse a la red. [Sitio web]. [Consulta: 06 de enero 2021]. Disponible en: https://www.latercera.com/pulso/noticia/cmf-inicio-supervision-in-situ-en-bancoestado-por-ataque-de-ransomware-y-la-estatal-instruyo-a-sus-ejecutivos-a-no-conectarse-a-la-red/2QEL4J43HZF6BJ5ENWKRJAJXVQ/

LAHMAN, Sean. ransomware: Cyber threats against small businesses on the rise. Rochester Democrat and Chronicle [Sitio web]. [Consulta: 30 de octubre de 2020]. Disponible en internet: https://bv.unir.net:2257/docview/1962714832?pq-origsite=summon

LAZOR. David. Ransomware [Sitio web]. [Consulta: 15 de noviembre de 2020]. Disponible en internet: https://bv.unir.net:2257/docview/1888660059?pq-origsite=summon

LIU, Wanping. Modeling Ransomware Spreading by a Dynamic Node-Level Method. IEEE Access. 2019, vol. 7, s. 142224-142232. ISSN 2169-3536.

LUO. Robert, Awareness Education as the Key to Ransomware Prevention. [en línea]. [Consulta: 15 de octubre de 2020]. Disponible en: https://www.researchgate.net/publication/220450120_Awareness_Education_as_the_Key_to_Ransomware_Prevention

KASPERSKY. Historia y evolución del Ransomware: datos y cifras. [Sitio web]. [Consulta: 15 de marzo de 2020]. Disponible en internet: https://blog.kaspersky.com.mx/Ransomware-blocker-to-cryptor/7295/

MÁRQUEZ DÍAZ, A. Jairo. Riesgos y vulnerabilidades de la denegación de servicio distribuidos en internet de las cosas. [Sitio web]. [Consulta: 15 de abril de 2020]. Disponible en internet: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200006&lang=es

MARTINEZ-GARCIA. Holzen Atocha, MOO MEDINA. Melquizedec y CHUC US. Ligia Beatriz. Origen y evolución del Cryptovirus Ransomware. [Sitio web]. [Consulta: 25 de marzo de 2020]. Disponible en internet: https://www.researchgate.net/publication/312490181_ORIGEN_Y_EVOLUCION_DEL_CRYPTOVIRUS_RANSOMWARE

MCAFFE. Understanding Ransomware and Strategies to Defeat it" [Sitio web]. Santa Clara. McAffe.[Consulta: 20 de marzo de 2020]. Disponible en: http://www.mcafee.com/it/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf

MILNER. The Smarter SMB's Guide to Ransomware. [Sitio web]. [Consulta: 5 de mayo 2020]. Disponible en: https://www.milner.com/docs/default-source/ebooks/milner-ebook_smb_ransomware_guide.pdf?sfvrsn=49ede358_6

MOHURLE, Savita Y PATIL, Manisha. A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science. 2017, vol. 8, no. 5, s. 1938.

NIST. Phishing definition. [Sitio web]. [Consulta: 17 de enero 2021]. Disponible en: https://csrc.nist.gov/glossary/term/phishing

NORTON. What is a Trojan? Is it a virus or is it malware? [Sitio web]. [Consulta: 20 de enero 2021]. Disponible en: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

NTT SECURITY. Solutionary SERT Q2 report: eighty-eight percent of all ransomware is detected in healthcare industry. July 26, 2016. [Sitio web]. [Consulta: 06 de noviembre 2020]. Disponible en: https://www.solutionary.com/threat-intelligence/threat-reports/quarterly-threat-reports/sert-threat-report-q2-2016/

OBSERVATORIO DE CIBERSEGURIDAD. Riesgos, avances y el camino a seguir en américa latina y el caribe. [En línea]. [Consulta: 07 de enero 2021]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

O'GORMAN. Gavin, y MCDONALD, Geoff. Ransomware: A Growing Menace. [Sitio web]. [Consulta: 12 de abril de 2020]. Disponible en internet: https://vxug.fakedoma.in/papers/Ransomware-growing-menace-12-en.pdf

PANDA SECURITY. Informe #Wannacry. [Sitio web]. Madrid: Panda. [Consulta: 2 de mayo 2020]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/05/1705-Informe_WannaCry-v160-es.pdf

PHYS.ORG. About the malicious software known as ransomware [Sitio web] Rosenberg, M. Joyce. [Consulta: 18 de marzo de 2020]. Disponible en: https://phys.org/news/2015-04-qa-malicious-software-ransomware.html

PONS GAMÓN. A. Vicente. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. [en línea]. [Consulta: 22 de marzo de 2020]. Disponible en: https://www.redalyc.org/jatsRepo/5526/552656641007/index.html

POPE. Justin. Ransomware: Minimizing the Risks [en línea]. [Consulta: 15 de noviembre de 2020]. Disponible en: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5300711/

PUENTE. Miriam. Riesgos y retos de ciberseguridad y privacidad en IoT [en línea]. [Consulta: 15 de marzo de 2020]. Disponible en: https://www.certsi.es/blog/riesgos-y-retos- ciberseguridad-y-privacidad-iot

RESEARCH GATE. Ransomware Attacks: Critical Analysis, Threats, and Prevention methods. [Sitio web]. IMAJI Asibi, [Consulta: 12 de abril 2020]. Disponible en: https://www.researchgate.net/publication/332551447_Ransomware_Attacks_Critical_Analysis_Threats_and_Prevention_methods

REVISTA IBERO-LATINOAMERICANA DE SEGUROS. Los seguros de 'cyber risk'. (A propósito del ciberataque mundial de fecha 12 de mayo de 2017). Bogotá: Universidad Javeriana, 2017, nro. 47 ISSN 0123-1154

RICHARDSON. M. Ronny y NORTH. M. Max. Ransomware: Evolution, Mitigation and Prevention. [en línea]. [Consulta: 28 de marzo de 2020]. Disponible en: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

ROBERTO. Carlos. Tecnología pyme - Weblogs SL: Cifrado de archivos, cambio de contraseñas y amenaza de publicar datos si no pagas, la última extorsión del ransomware [Sitio web]. [Consulta: 5 de octubre 2020]. Disponible en: https://bv.unir.net:2257/docview/2369417134?pq-origsite=summon

STUPIA. Pamela, Iniciativa global contra el Ransomware. [Sitio web]. ITSITIO. [Consulta: 1 de mayo 2020]. [Consulta: 15 de octubre 2020]. Disponible en: https://www.itsitio.com/py/iniciativa-global-contra-el-ransomware/

SOPHOS. Cómo protegerse del Ransomware. [Sitio web]. Abingdon: Sophos. [Consulta: 5 de mayo 2020]. Disponible en: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophosransomwareprotectionwpna.pdf?la=es-ES

SYMANTEC. The Evolution of Ransomware [Sitio web]. California. SAVAGE. Kevin, COOGAN. Peter y LAU. Hon. [Consulta: 15 de marzo de 2020]. Disponible en: https://its.fsu.edu/sites/g/files/imported/storage/images/information-security-and-privacy-office/the-evolution-of-ransomware.pdf

THE UNITED STATES DEPARTMENT OF JUSTICE. How to protect your networks from ransomware. [Sitio web]. [Consulta: 06 de noviembre 2020]. Disponible en: https://www.justice.gov/criminal-ccips/file/872771/download

TOLMAN, William Howe. Social Engineering. Charleston: BiblioBazaar Publisher, 2010. p.4. ISBN 978-05-5933-064-3

TRENDMICRO TRENDLABS. Economics Behind Ransomware as a Service: A Look at Stampado's Pricing Model. [Sitio web]. [Consulta: 5 de abril de 2020]. Disponible en: http://blog.trendmicro.com/trendlabs-security-intelligence/the-economicsbehind-Ransomware-prices/

TREND MICRO. Proteja su organización del ransomware. [Sitio web]. Tokio: Trend Micro. [Consulta: 5 de mayo 2020]. Disponible en: https://resources.trendmicro.com/rs/945-CXD-062/images/Solution_Brief_Ransomware_Enterprise.pdf

TRIGO. Santiago, CASTELLOTE. Martín y PODESTÁ. Ariel. Ransomware: seguridad, investigación y tareas forenses. [Sitio web]. [Consulta: 15 de marzo de 2020]. Disponible en: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs

US-CERT. Ransomware and Recent Variants. [Sitio web]. [Consulta: 29 de marzo de 2020]. Disponible en: https://www.us-cert.gov/ncas/alerts/TA16-091A

VARONIS. CryptoLocker: Everything You Need to Know. [Sitio web]. [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.varonis.com/blog/cryptolocker/

VACZI, Daniel Y SZADECZKY, Tamas. A Threat for the Trains: Ransomware as a New Risk. Interdisciplinary Description of Complex Systems. 2019, vol. 17, no. 1, s. 1-6. ISSN 1334-4684.

WELIVESECURITY. Ataque de ransomware afectó al Ministerio de Desarrollo Social de Panamá. [Sitio web]. [Consulta: 06 de enero 2021]. Disponible en: https://www.welivesecurity.com/la-es/2021/01/12/ataque-ransomware-afecta-ministerio-desarrollo-social-panama/

WIRED. 4 Ways to Protect Against the Very Real Threat of Ransomware [Sitio web]. Washington: ZETTER, Kim. 2016. [Consulta: 15 de marzo de 2020]. Disponible en: https://www.wired.com/2016/05/4-ways-protect-ransomware-youre-target/

--------. Android Ransomware Has Picked Up Some Ominous New Tricks. [Sitio web]. Washington: NEWMAN, lily. 2020. [Consulta: 30 de octubre de 2020]. Disponible en: https://www.wired.com/story/android-ransomware-worrying-evolution/

ANEXOS

Anexo A. Herramientas de descifrado disponibles en: nomoreransom.org

Herramientas de descifrado				
777 Ransom	Crypt32 Ransom	Globe3 Ransom	Merry X-Mas Ransom	Simplocker Ransom
AES_NI Ransom	Crypt888 Ransom	GlobeImposter Ransom	MirCop Ransom	SpartCrypt Ransom
Agent.iih Ransom	CryptON Ransom	GoGoogle Ransom	Mira Ransom	Stampado Ransom
Alcatraz Ransom	CryptXXX V1 Ransom	Gomasom Ransom	Mole Ransom	Syrk Ransom
Alpha Ransom	CryptXXX V2 Ransom	HKCrypt Ransom	Muhstik Ransom	Teamxrat/Xpan Ransom
Amnesia Ransom	CryptXXX V3 Ransom	Hakbit Ransom	Nemty Ransom	TeslaCrypt V1 Ransom
Amnesia2 Ransom	CryptXXX V4 Ransom	HiddenTear Ransom	Nemucod Ransom	TeslaCrypt V2 Ransom
Annabelle Ransom	CryptXXX V5 Ransom	HildaCrypt Ransom	NemucodAES Ransom	TeslaCrypt V3 Ransom
Aura Ransom	CryptoMix Ransom	Iams00rry Ransom	Nmoreira Ransom	TeslaCrypt V4 Ransom
Aurora Ransom	Cryptokluchen Ransom	InsaneCrypt Ransom	Noobcrypt Ransom	Thanatos Ransom
AutoIt Ransom	Cyborg Ransom	Iwanttits Ransom	Ouroboros Ransom	ThunderX Ransom
AutoLocky Ransom	DXXD Ransom	JSWorm 2.0 Ransom	Ozozalocker Ransom	Trustezeb Ransom
Avest Ransom	Damage Ransom	JSWorm 4.0 Ransom	PHP ransomware Ransom	TurkStatic Ransom
BTCWare Ransom	Democry Ransom	Jaff Ransom	Paradise Ransom	VCRYPTOR Ransom
BadBlock Ransom	Derialock Ransom	JavaLocker Ransom	Pewcrypt Ransom	WannaCryFake Ransom
BarRax Ransom	Dharma Ransom	Jigsaw Ransom	Philadelphia Ransom	Wildfire Ransom
Bart Ransom	DragonCyber Ransom	Kokokrypt Ransom	Planetary Ransom	XData Ransom
BigBobRoss Ransom	ElvisPresley Ransom	LECHIFFRE Ransom	Pletor Ransom	XORBAT Ransom
Bitcryptor Ransom	EncrypTile Ransom	LambdaLocker Ransom	Popcorn Ransom	XORIST Ransom
CERBER V1 Ransom	Everbe 1.0 Ransom	Lamer Ransom	Professeur Ransom	Yatron Ransom
CheckMail7 Ransom	FenixLocker Ransom	Linux.Encoder.1 Ransom	Puma Ransom	ZQ Ransom
Chernolocker Ransom	FilesLocker v1 and v2 Ransom	Linux.Encoder.3 Ransom	Pylocky Ransom	ZeroFucks Ransom
Chimera Ransom	FortuneCrypt Ransom	Loocipher Ransom	Rakhni Ransom	Zorab Ransom
Coinvault Ransom	Fury Ransom	Lortok Ransom	Rannoh Ransom	djvu Ransom
Cry128 Ransom	GalactiCryper Ransom	MacRansom Ransom	Ransomwared Ransom	
Cry9 Ransom	GandCrab (V1, V4,V5, V5.2 versions)	Magniber Ransom	RedRum Ransom	
CryCryptor Ransom	GetCrypt Ransom	Mapo Ransom	Rotor Ransom	
CrySIS Ransom	Globe Ransom	Marlboro Ransom	SNSLocker Ransom	
Cryakl Ransom	Globe/Purge Ransom	Marsjoke aka Polyglot Ransom	Shade Ransom	
Crybola Ransom	Globe2 Ransom	MegaLocker Ransom	SimpleLocker Ransom	

Anexo B. Resumen Analítica Especializado -RAE

Fecha de Realización:	10/04/2021
Programa:	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes.
Título:	EVOLUCIÓN E IMPACTO DEL *RANSOMWARE* EN AMÉRICA LATINA DESDE EL AÑO 2015
Autor(es):	FREDY YESID AVILA NIÑO
Palabras Claves:	*Ransomware, malware*, ataque, vulnerabilidad, amenaza.
Descripción:	*Ransomware* no es más que un programa malicioso (*malware*) diseñado para bloquear el acceso a los archivos o en algunos casos al sistema operativo, con esto el atacante consigue afectar uno de los tres pilares de la seguridad informática, la disponibilidad. Normalmente este tipo de ataque bloquea el acceso a través del cifrado de los archivos, cuya clave de cifrado solamente conoce el atacante, este a su vez, le solicita a la víctima cierta cantidad de dinero (en Criptomoneda) para conceder nuevamente el acceso a los archivos (clave de cifrado). En América Latina los ataques de *Ransomware* se posicionan como una de las amenazas más importantes, por esta razón es fundamental conocer su evolución e impacto desde el año 2015, entender el concepto y características, identificar los tipos de *Ransomware* que han aparecido en los últimos 5 años y describir los métodos de infección que se utilizan. Con esta información es posible generar recomendaciones para evitar ser víctima de este ataque.
Fuentes bibliográficas destacadas: ALLSOPP, Wil. Advanced Penetration Testing: Hacking the World's Most Secure Networks. San Francisco: John Wiley & Sons, Incorporated. 2017. p.147. ISBN 9781119367680	

ANTONUCCI. Domenic. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. San Francisco: John Wiley & Sons, Incorporated. 2017. p.137. ISBN 9781119308805

CHAUHAN, Sudhanshu y KUMAR, Nutan. Hacking Web Intelligence : Open Source Intelligence and Web Reconnaissance Concepts and Techniques. Amtersdam: Elsevier Science & Technology Books. 2015. p.206. ISBN 9780128018675

DAY, Graham. Security in the Digital World: For the home user, parent, consumer and home office. Londres: IT Governance Ltd, 2017. p.64. ISBN 9781849289610

EUROPOL. No-More-Ransom. [Sitio web]. [Consulta: 22 de abril 2020]. Disponible en internet: https://www.nomoreransom.org/

FEDERAL BUREAU OF INVESTIGATION. Incidents of ransomware on the rise: protect yourself and your organization. [Sitio web]. [Consulta: 22 de abril 2020]. Disponible en internet: https://www.fbi.gov/news/stories/ransomware-on-the-rise

INTSIGHTS. El Lado Oscuro de América Latina. [Sitio web]. [Consulta: 07 de mayo 2020]. Disponible en: https://wow.intsights.com/rs/071-ZWD-900/images/Span_El%20Lado%20Oscuro%20de%20Ame%CC%81rica%20Latina.pdf

LAZOR. David. Ransomware [Sitio web]. [Consulta: 15 de noviembre de 2020]. Disponible en internet: https://bv.unir.net:2257/docview/1888660059?pq-origsite=summon

THE UNITED STATES DEPARTMENT OF JUSTICE. How to protect your networks from ransomware. [Sitio web]. [Consulta: 06 de noviembre 2020]. Disponible en: https://www.justice.gov/criminal-ccips/file/872771/download

Contenido del documento:	INTRODUCCIÓN 1. DEFINICIÓN DEL PROBLEMA 1.1 ANTECEDENTES DEL PROBLEMA 1.2 FORMULACIÓN DEL PROBLEMA 2. JUSTIFICACIÓN 3. OBJETIVOS 3.1 OBJETIVOS GENERAL 3.2 OBJETIVOS ESPECÍFICOS 4. MARCO REFERNCIAL 4.1 MARCO TEÓRICO 4.2 MARCO CONCEPTUAL 5. DESARROLLO DE LOS OBJETIVOS 5.1 DEFINICION DE RANSOMWARE

	5.3 TIPOS DE RANSOMWARE LANZADOS DESDE 2015 5.4 METODOLOGIAS UTILIZADAS POR LOS ATACANTES 5.5 FORMAS DE IDENTIFICAR UN ARCHIVO ADJUNTO MALICIOSO 5.6 MEDIDAS QUE HAN TOMADO LAS ORGANIZACIONES Y LAS PERSONAS PARA PROTEGERSE DEL RANSOMWARE 5.7 COMPILADO DE BUENAS PRÁCTICAS EN CUANTO A LA PREVENCIÓN DEL RANSOMWARE 6. CONCLUSIONES 7. RECOMENDACIONES BIBLIOGRAFÍA ANEXOS
Marco Metodológico:	Se desarrolla la investigación bajo la metodología de tipo Exploratoria-Descriptiva, mediante la cual a partir de la recopilación y revisión de información primaria y secundaria se profundizará en la temática relacionada al *Ransomware* y de cómo este *malware* ha afectado a usuarios de Latinoamérica desde el año 2015, esto como base argumentativa para presentar el análisis descriptivo, y definir las características específicas de esta amenaza. Inicialmente se realiza la recopilación de la información, la revisión bibliográfica de datos proporcionados por agencias de gobierno y empresas de seguridad informática. Posteriormente, se realiza un compilado de todas las medidas que se han tomado para prevenir este tipo de incidentes para finalmente proponer un conjunto de buenas prácticas para prevenir el *ransomware*.
Conceptos adquiridos:	COMPILADO DE BUENAS PRÁCTICAS EN CUANTO A LA PREVENCIÓN DEL *RANSOMWARE.* Uno de los objetivos del presente trabajo es generar un compilado de buenas prácticas para contribuir a la prevención de ataques de *ransomware*, que pueda ser útil tanto para las organizaciones como para las personas. Las recomendaciones se plantean proponiendo una serie de concejos de acuerdo

	con los medios más comunes de propagación de esta amenaza.
Conclusiones:	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 aspecto 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*. Los ciberdelincuentes para la ejecutar este tipo de ataques, desarrollan estrategias elaboradas con el único propósito de alcanzar el mayor número de víctimas que sea posible, puesto que cuanta más gente reciba el *malware* mayor será la probabilidad de infectar equipos, incluso los atacantes ofrecen el *ransomware* como servicio, en donde 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. Con los incidentes relacionados al *ransomware* en aumento, y los algoritmos de cifrado que son empleados cada vez más sofisticados. El *ransomware* sin duda continúa siendo un gran desafío tanto para los profesionales de la seguridad de la información como para los investigadores, ya que las cepas futuras podrían ser inquebrantables y los métodos de cifrado más robustos, adicionalmente se incorporan técnicas de la ingeniería social para engañar a los usuarios, todo esto en conjunto hace que la amenaza sea aún más peligrosa.