ANÁLISIS DEL IMPACTO DE LOS ATAQUES DE RANSOMWARE EN LAS ORGANIZACIONES COLOMBIANAS COMO BASE DE CONOCIMIENTO PARA LA DETERMINACIÓN DE NUEVOS MECANISMOS DE PROTECCIÓN Y MINIMIZACIÓN DE RIESGOS CIBERNÉTICOS.

JHON JAIRO PINZÓN RUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
INÍRIDA
2021

ANÁLISIS DEL IMPACTO DE LOS ATAQUES DE RANSOMWARE EN LAS ORGANIZACIONES COLOMBIANAS COMO BASE DE CONOCIMIENTO PARA LA DETERMINACIÓN DE NUEVOS MECANISMOS DE PROTECCIÓN Y MINIMIZACIÓN DE RIESGOS CIBERNÉTICOS.

JHON JAIRO PINZÓN RUIZ

Proyecto de Grado – Monografía presentado para optar por el titulo de
ESPECIALISTA EN SEGURIDAD INFORMATICA

YENNY STELLA NÚÑEZ ÁLVAREZ
Directora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
INÍRIDA
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Este proyecto va dedicado a mi hijo Santiago Andrés Pinzón Gualdrón, quien ha sido mi motivación para escoger caminos de superación, que a su vez me impulsan a ser mejor persona cada día.

AGRADECIMIENTOS

Doy gracias en primer lugar a Dios quien es el que me ha dado salud y sabiduría, también a mi familia por el apoyo que me ha brindado, a los amigos y compañeros de la universidad por compartir sus conocimientos, y al cuerpo docentes de la universidad por el acompañamiento en el crecimiento y desarrollo de todo el proceso de formación académica.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: "Se entiende por activo de Información todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información"[1].

ANÁLISIS DE RIESGOS: "Uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información"[2].

CONFIDENCIALIDAD: Asegurar que la información está disponible solamente para los usuarios autorizados a tener acceso a dichos datos[3].

CONTROL: Una forma para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal[4].

DISPONIBILIDAD: Asegurar que los usuarios tengan, en todo momento, la información a la cual tienen derecho[5].

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas[6].

INFORMACIÓN: es un conjunto organizado de datos[7].

INTEGRIDAD: Asegurar que la información es adecuada y apropiada para su procesamiento[8].

---

[1] MANUAL DE POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN. Departamento Administrativo Para la Prosperidad Social. 2015. p.7.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.

SEGURIDAD DE LA INFORMACIÓN: Salvaguardar la confidencialidad, integridad y disponibilidad de la información[9].

SPAM: Correo no deseado de tipo basura o potencialmente peligroso[10].

USUARIO: Colaborador que hace uso de un equipo computacional o de un sistema de información[11].

[9] Ibid.
[10] Ibid.
[11] Ibid.

RESUMEN

El ransomware es un tipo de ataque cibernético ejecutado a través de un software malicioso que se asegura de cifrar los archivos evitando que el usuario pueda acceder a estos, dejando como alternativa, el pago por un rescate de la información. El ransomware ha ido evolucionando y cada día van apareciendo nuevas variantes que se adaptan a los distintos tipos de sistemas y dispositivos informáticos pero el modo de operación basado en criptografía es el mismo.

En este documento se mencionan los eventos de seguridad cibernética más importantes de los dos últimos años y los problemas de seguridad que se están presentando en las empresas teniendo en cuenta que la gran mayoría no cuenta con protocolos de respuesta a incidentes de seguridad, además presenta vulnerabilidades dentro de su infraestructura tecnológica lo que incrementa el riesgo de ser víctimas de estos eventos cibernéticos.

En Colombia el impacto ha sido alarmante las estadísticas muestran que el delito informático le está costando al país grandes sumas de dinero. Mediante este análisis se pretende dar a conocer el impacto que está generando el ransomware, y crear mecanismos de prevención para minimizar el daño de ataques cibernéticos futuros y fortalecer la postura de seguridad en el país.

ABSTRACT

Ransomware is a type of cyber attack executed through malicious software that ensures that files are encrypted, preventing the user from accessing them, leaving as an alternative, the payment of a ransom for the information. Ransomware has evolved and new variants appear every day that adapt to different types of computer systems and devices, but the cryptography-based mode of operation is the same.

This document mentions the most important cybersecurity events of the last two years and the security problems that they are presenting in companies, taking into account that most of them do not have protocols for responding to security incidents, and also present vulnerabilities within its technological infrastructure, which increases the risk of being victims of these cyber events.

In Colombia the impact has been alarming, statistics show that cybercrime is costinglarge sums of money. Through this analysis, it is intended to publicize the impact that ransomware is generating, and create prevention mechanisms to minimize future damage from cyber attacks and strengthen the security posture in the country.

INTRODUCCIÓN

Unos de los activos más importantes de una empresa es la información, por eso es fundamental identificar las amenazas y vulnerabilidades que determinen la probabilidad de que sucedan desastres que afecten la integridad de este activo, y así estimar sus consecuencias estableciendo estrategias para atender las emergencias que provengan de estas amenazas; a nivel empresarial en los últimos años ha crecido el proceso de comercio electrónico, los consumidores emplean con más frecuencia canales digitales para realizar compras y transacciones, y las empresas se van sumando a esta estrategia de mercadeo; es aquí donde puntualmente se identifica que la mayor necesidad que afrontan las organizaciones es la implementación de ciberseguridad, un proceso que ayuda a las empresas a ser más eficientes.

Nos encontramos en un mundo cada día más interconectado, en el cual el principal reto de la ciberseguridad es la protección de la información; la importancia está centrada en contar con un esquema y una arquitectura robusta que les permita a las empresas asegurar su información, ya que constantemente las organizaciones están siendo objeto de ciber ataques lo que les ha costado a muchas empresas la perdida de grandes sumas de dinero e incluso la continuidad de negocio.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Uno de los activos más importantes de las organizaciones es la información, esta es una razón suficiente para que los ciberdelincuentes busquen sacar provecho haciendo uso de ransomware para lucrarse por medio de esta práctica delictiva, una vez logran secuestrar la información, los delincuentes empiezan a ejercer presión sobre las victimas exigiendo dinero por el rescate de esta, y amenazando con eliminar o publicar el contenido de los datos.

El creciente aumento de los ciberataques de ransomware hace que el riesgo sea cada vez mayor y las empresas se hacen vulnerables a este problema sobre todo si no se tiene conocimiento de la amenaza o no hay sensibilización sobre el manejo de canales digitales y seguridad de la información, además hay que tener en cuenta que muchos de los programas antivirus convencionales no detectan inicialmente la infección, no existe un descifrador adecuado para muchos de estos ataques , los archivos quedan encriptados y la recuperación se hace imposible para el usuario. Aún no existen métodos eficientes para romper los secuestros del ransomware, cuando los datos ya están encriptados.

El software malicioso se propaga con mucha facilidad a través de la red, así como por medios de discos duros individuales o compartidos, cada vez se incrementan los riesgos, por lo que la amenaza crece de forma acelerada, el delito se vuelve más recurrente y las estadísticas de este tipo de ataque tienden a subir; podemos afirmar que el uso de ransomware es una práctica difícil de controlar y las organizaciones siguen estando expuestas a la perdida de datos y mucho dinero.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la comprensión del impacto y el conocimiento de los vectores de ataque de Ransomware facilita el establecimiento de los mecanismos de prevención de riesgos cibernéticos en las organizaciones?

2 JUSTIFICACIÓN

El estudio sobre ransomware nos permite aportar conocimiento acerca de esta técnica de ataque cibernético que se encuentra en crecimiento, y que tiene como principal objetivo las organizaciones.

Parte del éxito que ha tenido los ciberdelincuentes que se dedican a esta práctica, es por la vulnerabilidad que existe dentro de las organizaciones, y es que cada vez van apareciendo nuevos métodos de ataque cibernético por lo que se debería tomar conciencia en este asunto y empezar a fortalecer la infraestructura tecnológica y seguridad de la información; sin embargo en la actualidad este tema no es prioridad en muchas empresas tal vez por falta de conocimiento sobre el crimen cibernético o falta de presupuesto económico, y no es considerado como una potencial amenaza, cuando en realidad el nivel de riesgo es alto y las consecuencias pueden ser desbastadoras, ya que un secuestro de datos puede ocasionar daño de infraestructura TI, perdida de información o perdida de dinero.

Un análisis sobre el impacto de ataques por ransomware permitirá tener una idea de las consecuencias que conllevan los ciberataques en las organizaciones y el riesgo que se está corriendo si no se cuenta con buenas políticas de seguridad informática y procedimientos seguros en la infraestructura tecnológica.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el Impacto de los Ataques de Ransomware en las Organizaciones Colombianas como base de conocimiento para determinación de nuevos mecanismos de protección y minimización de riesgos cibernéticos a partir de reportes sobre las amenazas y eventos de seguridad informática de los últimos 2 años.

3.2 OBJETIVOS ESPECÍFICOS

1. Describir las generalidades, características, familias, variantes y evolución del código malicioso Ransomware.

2. Analizar a partir de reportes existentes, el impacto, vectores de infección e índice de crecimiento de ransomware de Colombia en los últimos 2 años.

3. Identificar las principales vulnerabilidades y riesgos informáticos presentes en las infraestructuras tecnológicas.

4. Proponer una guía de buenas prácticas con medidas prevención y mecanismos de protección contra ataques de ransomware para las organizaciones colombianas.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Los ataques con software informático se usan con fines maliciosos que busca alterar el funcionamiento de sistemas informáticos o perdida de información, una de las novedades que se observa en el mundo de la ciberdelincuencia es el aumento de casos en el secuestro de datos al interior de las organizaciones, una técnica que tiene por motivación en los delincuentes recoger grandes sumas de dinero a través del rescate de la información. Se trata de un ataque a través del uso de software extorsivo, que tiene como finalidad impedir que el usuario tenga acceso a la información hasta que haya realizado el pago por un rescate de esta, la modalidad de ataque por ransomware se encuentra entre los ciberdelitos más recurrentes de la actualidad lo que les ha costado a muchas empresas la perdida de grandes sumas de dinero.

Esta modalidad se ha estado incrementando y se ha constituido en retos difíciles a los que se están enfrentando el sector de la ciberseguridad, ya que la identificación de nuevas tácticas criminales se va conociendo precisamente durante el proceso de materialización del delito, es decir que la delincuencia puede ir avanzando a pasos agigantados.

Son muchos los métodos que usan los atacantes para robar datos o alterar el funcionamiento de los sistemas, pero el ransomware es uno de los problemas más graves a nivel de ciberseguridad, y está generando gran impacto en la continuidad del negocio en las organizaciones; la revolución de software, mejoras tecnológicas y las herramientas de comunicación han sido elementos cruciales usados por los piratas informáticos para la propagación del delito, además el uso de mecanismos como criptomonedas difíciles de rastrear también lo han facilitado.

Para el análisis del comportamiento de este tipo de ataque se requiere conocer las técnicas utilizadas por los cibercriminales que cada vez son mejoradas en las variantes de ransomware, aunque generalmente, el único objetivo de un ransomware en una máquina de destino es cifrar archivos, lo que implica la necesidad de conocer el funcionamiento y modo de operación de este, además el

estudio de las modalidades de operación en esta técnica delictiva ayuda a la detención temprana para minimizar el riesgo e integrar nuevas políticas de seguridad y tratamiento de riesgos; la identificación de ransomware se basa fundamentalmente en análisis estadísticos de las bases de datos de firmas. Esto genera alertas para estar preparados y mantener los equipos siempre seguros; los análisis del comportamiento de este delito informan cuál es la entrada más habitual de software malicioso y de esta forma saber cómo protegerse[12].

Básicamente hay dos tipos diferentes de ransomware (con algunas variantes), encriptadores y lockers, los encriptadores trabajan como ransomware de cifrado, que contienen algoritmos avanzados de cifrado, bloqueando archivos importantes, y aunque el funcionamiento del equipo de cómputo no se ve afectado la víctima no logra acceder a la información, generalmente cuando esto sucede inmediatamente aparece un mensaje donde se exige el pago de un monto de dinero a cambio de desbloquear los documentos afectados. Es importante mencionar que ante esta situación muchas de las victimas terminan pagando el dinero que le exigen, sin embargo, el hecho de pagar el monto no garantiza que la información sea rescatada. por otra parte existe la modalidad de lockers o ransomware de bloqueo que trabaja de forma distinta, en este caso la victima pierde el control del equipo de cómputo, aunque con esta técnica los archivo no se encuentran cifrados es difícil acceder a la información por que los ciberdelincuentes tienen el control del equipo, generalmente se habilita un formulario o ventana mediante la cual el ciberdelincuente solicita el pago por el proceso de desbloqueo, en todo caso con este método quedan posibilidades de rescatar la información por otros medios ya que esta no ha sido encriptada[13].

Las técnicas usadas bajo estas modalidades tienen ciertas características, los archivo no se pueden descifrar por cuenta propia, el ransomware es un software sofisticado con la capacidad de cifrar cualquier tipo de archivo y puede codificar nombres de archivos; el pago exigido por el rescate de la información debe hacerse en Bitcoins, un tipo de criptomoneda que no puede ser rastreada; en el ejercicio de este ataque se ejerce presión a las víctimas con mensajes de límite de tiempo y amenazas como destruir o publicar la información.

---

[12] LEMMOU, Yassine ; LANET, Jean-Louis y SOUIDI, El Mamoun. A behavioural in-depth analysis of ransomware infection. *IET information security*. 2021, Vol.15 (1), p.38-58. Disponible en: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ise2.12004

[13] HORNET SECURITY. Ransomware. ¿Qué es ransomware? ¿cómo protergerse? [Sitio web]. España. Disponible en: https://www.hornetsecurity.com/es/knowledge-base/ransomware/

La piratería informática cada vez se encuentra más organizada, no se dejan detectar fácilmente por los antivirus convencionales ya que cuenta con técnicas sofisticadas de evasión, y sus ataques se extienden con facilidad a través de la red.

El ransomware cada vez integra nuevas variables lo que lo convierte en una de las amenazas más peligrosas en el ciberespacio, entre otras cosas la motivación para los piratas informáticos es que se ha convertido en un negocio que le ha venido dejando buenas ganancias debido al valor que representa la información en las empresas.

El éxito de prevención de ataques depende en gran manera de la preparación sobre amenazas cibernéticas, constantemente se ven amenazas emergentes y los ciberdelincuentes buscan el momento oportuno para tratar de materializar esos ataques, lo que significa que las prácticas de seguridad deben estar dirigidas para afrontar ataques tradicionales y emergentes. Conocer el modo de operación de los eventos marca la diferencia entre la exposición y protección de datos. Estar preparados para afrontar ataques necesita de estar monitoreando el panorama de amenazas continuamente; esto también significa entre más sofisticado sean los ataques, la detención de amenazas deber ser más sólida.

El cambio del sistema laboral en muchas empresas que adoptaron la modalidad de teletrabajo causó un impacto negativo en la seguridad de la infraestructura de las organizaciones, debido a protecciones inadecuadas de datos confidenciales que se fueron gestionando a través de equipos personales y dispositivos móviles, en redes de conectividad en el hogar con límites de seguridad; este cambio fue muy brusco para la mayoría de las personas y organizaciones, luego que se pasó de un campo laboral protegido dentro de instalaciones de las redes empresariales a entornos improvisados e inseguros, lo que incrementa significativamente la fuga de seguridad y el índice de ataques a la información. se estima el 20% de fuga de información desde que empezó la pandemia se atribuye al trabajo remoto[14].

Los usuarios se vieron afectados por una serie de ataques cibernéticos que surgieron durante la incertidumbre de la pandemia COVID-19, los delincuentes aprovechaban la situación para engañar a las víctimas en intentaban instalar

[14] BLACKBERRY. Perspectivas sobre la seguridad cibernética. *Informe de amenazas 2021.* 2021. P.7. Disponible en: https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report-sp.pdf

aplicaciones de supuesto seguimiento al COVID-19, pero estas contenían código malicioso que ejecutaba ransomware CovidLock que impedía el acceso a los dispositivos móviles.

El estado actual de amenazas por ransomware muestra acciones que les permite avanzar cada día en el desarrollo de estas prácticas delictivas, entre estas encontramos los siguientes datos:

Los grupos de malware que distribuyen ransomware Ryuk hacen uso de Adfind con el objetivo de hallar información que permite moverse dentro del entorno afectado.

Para mapear relaciones que se pueden ocultar dentro de un dominio hace uso de SharpHound, otra funcionalidad de enumeración de Active Directory. Estos procedimientos le facilitan el camino al delincuente para poder obtener privilegios de administrador, SharpHound se presenta en diferentes formatos incluyendo archivos ejecutables. exe de DotNet y scrip de PowerShell.

Sociedades de colaboración y cruce de información entre grupos de ciberdelincuentes dedicados a desarrollar ransomware y otros grupos de atacantes como los que ejecutan Azorult, Emotet y Trickbot.

Extracción de datos lo cual es aprovechado por los atacantes para generar amenazas a las víctimas sobre exponer la información confidencial es sitios públicos lo cual ejerce presión para acelerar el pago del rescate.

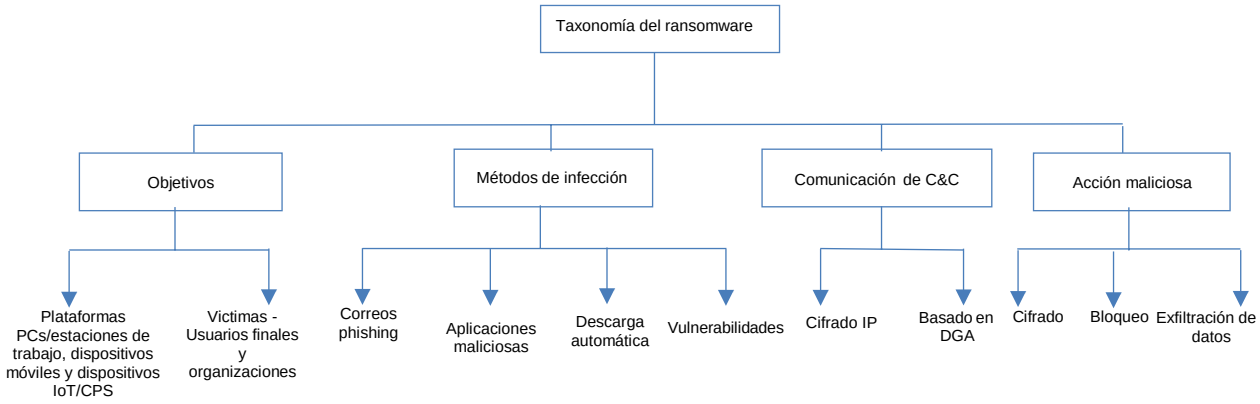
Las campañas de ransomware como servicio (RasS) han estado ganado fuerza sobreponiéndose al ransomware genérico que se han implementado años atrás. La caja de herramientas exploits se sigue implementando en campañas de malspam y Cobalt Strike.

En los dos últimos años se alcanzaron alzas significativas en el precio de criptomonedas lo que impulsó el incremento de ataques ransomware y cryptojacking.

Con este estudio se pretende minimizar el riesgo de incidentes cibernéticos a futuro y motivar al fortalecimiento de la seguridad de la información.

La clasificación del ransomware se da básicamente por objetivos, método de infección, comunicación de C&C y acción maliciosa.

Figura 1. Taxonomía del ransomware.



Fuente: A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. [2022]. P.7. Disponible en: https://arxiv.org/pdf/2102.06249.pdf

Clasificación por objetivos

Con relación a los objetivos del ransomware se conocen dos clases las cuales son victima objetivo y plataforma objetivo, a su vez las victimas objetivos se dividen en dos categorías usuarios finales y organizaciones.

Inicialmente el ransomware se ejecutaba específicamente en usuarios finales, la falta de conocimientos sobre prácticas de ciberseguridad ocasionaba que las primeras familias de ransomware tuvieran éxito en los usuarios finales[15]. El ransomware criptográfico puede entrar a los equipos de estos usuarios y cifrar los archivos que se encuentran almacenados; por otro lado las variantes de casillero tienen la capacidad de bloquear el acceso a los equipos de estos usuarios, aun así el precio que se les exige a los usuarios finales en mucho menor comparado con las sumas de dinero que se les exige a las organizaciones debido a su capacidad de pago, sin embargo un solo ransomware está en la capacidad de atacar a miles de usuarios finales[16].

Como se ha mencionado, las primeras familias de ransomware estaban dirigidas a

[15] Symantec. 2015. The evolution of ransomware. https://its.fsu.edu/sites/g/files/imported/storage/images/informationsecurity-and-privacy-office/the-evolution-of-ransomware.pdf. [Online; accessed 13-October-2020].

[16] A. Atapour-Abarghouei, S. Bonner, and A. S. McGough. 2019. Volenti non fit injuria: Ransomware and its Victims.
In 2019 IEEE International Conference on Big Data (Big Data). 4701–4707.

tacar usuarios finales, sin embargo, con la evolución y aparición de nuevas variantes el objetivo se fue centrando también a las organizaciones esto con la motivación de obtener un mejor pago, en este sentido el sistema de ataque se ha ido robusteciendo con el fin de lograr la mayor interrupción posible. El ransomware de bloqueo puede lograr detener la operación de toda una organización siempre y cuando logre bloquear el acceso a los dispositivos [17]. Del mismo modo el ransomware criptográfico puede detener la operación cifrando la información y haciéndola inaccesible, incluso en el uso de ransomware criptográfico se emplean técnicas que prácticamente hacen imposible descifrar archivos y recuperar los datos [18].

Plataformas objetivo

Básicamente los ataques por ransomware van dirigidos a PCs/estaciones de trabajo, dispositivos móviles y dispositivos IoT/CPS; los objetivos más comunes están dirigidos a PCs/estaciones de trabajo teniendo en cuenta que estos equipos son los más usados en cuanto al manejo y almacenamiento de información[19] la mayor parte de estos ataques están centrados en PC y estaciones de trabajo de Windows aunque algunas variantes se dirigen a Linux y macOS, la principal amenaza para estas plataformas es el ransomware criptográfico. En relación con los dispositivos móviles los ataques están centrados en Android e iOS debido a la cantidad de usuarios que poseen esta clase de equipos, sin embargo los usuarios de Apple no se han visto tan afectados debido a que la empresa cuenta con un sistema que examina a fondo las aplicaciones antes de su disponibilidad; en cuanto al sistema Android el ransomware representa una gran amenaza, de hecho el primer caso que surgió fue en el año 2013 con la aparición de Android-Defender, luego de esto en el 2014 sale el ransomware criptográfico conocido como Simplocker[20], la principal amenaza para estas plataformas es el ransomware de bloqueo. Por otro lado, los dispositivos IoT y CPS no se ven tan amenazados actualmente, aunque esta clase de equipos está tomando más fuerza en el mercado lo que puede ocasionar que en un futuro surjan variantes dirigidas a estas plataformas.

[17] WIRED. 2018. Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare. Disponible en: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[18] F. Tang, B. Ma, Jinku Li, F. Zhang, J. Su, and J. Ma. 2020. RansomSpector: An introspection-based approach to detect
crypto ransomware. Computers & Security 97 (2020).

[19] Statista. 2019. Desktop OS market share 2013-2018 | Statista. https://www.statista.com/statistics/218089/globalmarket-
share-of-windows-7/. [Online; accessed 13-October-2020].

[20] L. Štefanko R. Lipovský and G. Braniša. 2016. The Rise of Android Ransomware.
http://www.neotericnetworks.com/wp-content/uploads/2016/11/Rise-of -Android-Ransomware.pdf

Clasificación por vectores de infección

Básicamente los métodos de infección empleados en ransomware se clasifican en cinco: correos electrónicos maliciosos, SMS o mensajes instantáneos (IM), aplicaciones maliciosas, descarga automática y vulnerabilidades.
Los vectores de infección más usados en este tipo de ataque son los correos electrónicos maliciosos, en este caso los atacantes hacen llegar el malware a través de correos tipo spam[21], el contenido del correo puede tener un adjunto con el malware o un enlace que conlleve a la descarga del mismo. En cuanto a los dispositivos móviles los atacantes suelen hacer llegar el malware a través de mensajería SMS redirigiendo a la víctima algún sitio malicioso diseñado para la descarga del ransomware otra de las grandes amenazas presentes en dispositivos móviles con las aplicaciones maliciosas, en este caso los ciberdelincuentes desarrollan aplicaciones móviles e introducen el malware para cuando sean descargadas estas aplicaciones, se ejecute el ransomware en los dispositivos. También tenemos la presencia de descarga automática, esta se da cuando el usuario sin darse cuenta accede a un sitio malicioso y se produce la descarga e instalación del malware. Por último, tenemos la explotación de vulnerabilidades, en este caso los atacantes aprovechan las vulnerabilidades que presentan los sistemas operativos, software o navegadores[22] y con uso de kit de explotación instalan el contenido malicioso.

Clasificación por comunicación C&C

Un servidor de comando y control (C&C) opera de forma remota en el dominio del delincuente[23] estos se emplean básicamente para la comunicación y configuración del malware, con relación al ransomware estos servidores son usados con el propósito de enviar y recibir las claves de cifrado del ransomware criptográfico; estas variantes usan principalmente los protocolos HTTP Y HTTPS pueden conectarse por medio de direcciones IP o dominios codificados, o a través de dominios generados dinámicamente (DGA).

---

[21] Lindsey O'Donnell. 2019. ThreatList: Top 5 Most Dangerous Attachment Types. https://threatpost.com/threatlist-top-5-most-dangerous-attachment-types/144635/

[22] D. Kao, S. Hsiao, and R. Tso. 2019. Analyzing WannaCry Ransomware Considering the Weapons and Exploits. In 2019 21st International Conference on Advanced Communication Technology (ICACT).

[23] TrendMicro. [n.d.]. Command and Control Server. https://www.trendmicro.com/vinfo/us/security/definition/commandand-control-server. [Online; accessed 13-October-2020].

IPs/Dominios codificados

Lograr la conexión con el servidor de C&C se puede lograr a través de direcciones IP o dominios codificados, en este sentido la dirección IP será la misma para cada ataque lo que significa comunicación estable para el ciberdelincuente; en todo caso estos datos pueden ser utilizados en materia de ciberseguridad por las firmas de detención como mecanismo de defensa.

Dominios dinámicos

Una manera de contactar con los servidores C&C de forma dinámica es a través de algoritmos de generación de dominios (DGA), de esta forma los cortafuegos no pueden detectar la comunicación ya que cada comunicación tiene un único nombre de dominio[24].

Clasificación por acción maliciosa

Encriptación es un método de cifrado usado por muchas variantes del ransomware que básicamente lo que logra es que los archivos sean inaccesibles, para lo cual prepara las claves públicas y privadas de acuerdo a las técnicas que se utilice; en este sentido las técnicas de cifrado que existes son tres simétricas, asimétricas o híbridas.

En el proceso de cifrado de clave simétrica consiste en el uso de una sola clave para cifrar y descifrar los archivos por lo que a través de este método se puede cifrar mayor cantidad de archivos en comparación con el proceso de clave asimétrica, el algoritmo de cifrado AES es más usado con este método, la clave de cifrado se envía al ciberdelincuente mediante la comunicación C&C; en cambio el proceso de cifrado de clave asimétrica se caracteriza por el uso de dos clave distintas, es decir una publica para cifrar los archivos y una privada para descifrarlos, este método es más seguro por la protección de las claves aunque no se puede cifrar tantos archivos como el método de cifrado simétrico, el algoritmo de cifrado RSA es más usado con esta técnica. Por otra parte, también existe el método de cifrado híbrido en el cual los delincuentes realizan la combinación de las dos técnicas mencionadas

[24] S. Salehi, H. Shahriari, M. M. Ahmadian, and L. Tazik. 2018. A Novel Approach for Detecting DGA-based Ransomwares.
In 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology
(ISCISC)

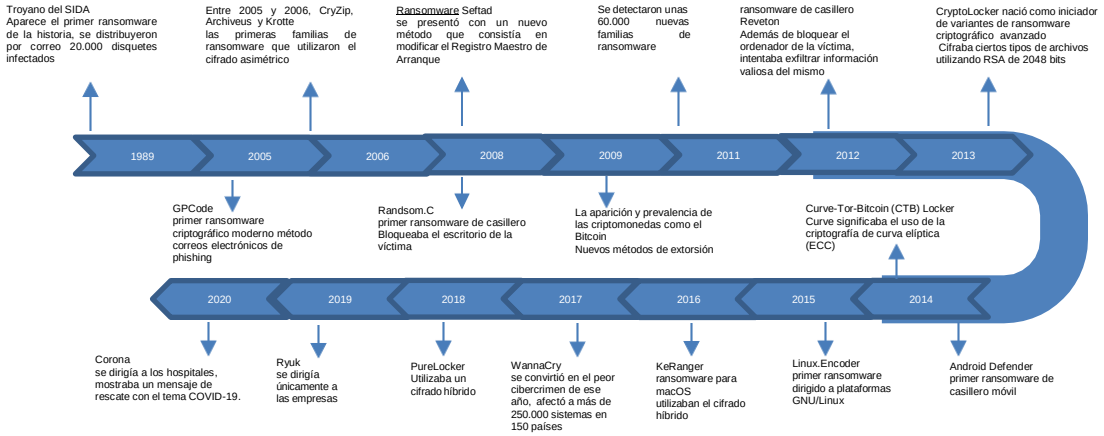
anteriormente cifrando los archivos con el uso de clave simétrica luego cifra la clave simétrica con la clave pública del atacante; este tipo de ataque por lo general no tienen comunicación con el servidor C&C.

Las variantes de ransomware de bloqueo actúan de tres maneras en la ejecución de sus ataques, existe bloqueo de pantalla, de navegador y de registro de arranque maestro; el ransomware de bloqueo de pantalla hace uso de distintos métodos como crear un nuevo escritorio, descargar imágenes o páginas HTML de servidores C&C que actúan como barreras que impiden el acceso a los dispositivos mientras muestran el mensaje de anuncio de secuestro, en cuanto al bloqueo de navegadores logran redirigir a las víctimas a sitios maliciosos con código JavaScript, normalmente este tipo de ataques vienen acompañados con mensajes relacionados a bloqueos por violación de la ley o semejantes con el propósito de crear susto en los usuarios. Por otra parte, las variantes que bloquean el sistema de arranque maestro impiden que el sistema cargue el código de arranque logrando cifrar el MBR original y sustituirlo por uno falso.

Otra modalidad maliciosa es la exfiltración de datos, las variantes recientes de ransomware además de secuestrar la información, tienen como objetivo robar información de valor con el fin de exigir un pago adicional a cambio de hacer pública la información, de este modo crean presión sobre las victimas ya que la publicación de datos sensibles puede dañar la reputación y ocasionar problemas legales.
Al igual que distintas técnicas de ataque en el secuestro de información, los atacantes también usan diferentes métodos de extorsión, como por ejemplo mensajes de texto o vales de prepago como la tarjeta Paysafe, aunque en la actualidad con el fin de buscar el anonimato, el método de preferencia es a través del sistema de criptomonedas teniendo en cuenta lo difícil de rastrear este proceso.

Evolución de las principales familias de ransomware desde 1989 hasta 2020.

Figura 2. Línea de tiempo del ransomware.



Fuente: A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. [2022]. P.6. Disponible en: https://arxiv.org/pdf/2102.06249.pdf

"Como se puede ver en la evolución del ransomware, esta famosa amenaza comenzó como una amenaza débil en 1989 al carecer de técnicas de cifrado fuertes y rápidas, diversos vectores de infección, métodos de pago (pseudo)anónimos y una amplia variedad de objetivos. Sin embargo, a medida que la tecnología fue evolucionando, los autores del ransomware aprendieron de los intentos fallidos anteriores y de los avances tecnológicos, logrando así convertir el ransomware en la ciber amenaza número uno[25]".

Tabla 1. Las familias de ransomware más importantes

Familia	Visto por primera vez	Infección	Plataforma	Características						
				C&C Comm.	Cifrado	Destrucción	Exfiltración	Bloqueo	Del. Sombra	Extorsión
PC CYBORG	1989	Phishing	Windows	Ninguno	Personalizado	Sobrescribir				Efectivo
GPCode	2008	Drive-by-download	Windows	Ninguno	RSA	Sobrescribir				Vales de prepago
Archivous	2008	Drive-by-download	Windows	Ninguno	RSA	Borrar				Vales de prepago
Randsom.C	2008	Spam	Windows	Ninguno	Ninguno	Ninguno	X			SMS
Seftad	2008	Spam	Windows	Ninguno	MBR	Sobrescribir		X		Vales de prepago

[25] A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. [2022]. P.7. Disponible en: https://arxiv.org/pdf/2102.06249.pdf

Krotten	2008	Spam	Windows	Ninguno	RSA	Sobrescribir				Vales de prepago
Urausy	2009	Phishing	Windows	Ninguno	Ninguno	Ninguno		X		Vales de prepago
Winlock	2010	Spam	Windows	Cifrado	Ninguno	Ninguno	X		X	SMS
Reveton	2012	Phishing	OS-Agnostic	Ninguno	Ninguno	Ninguno	X	X		Vales de prepago
CryptoLocker	2013	Phishing	Windows	Cifrado	RSA	Sobrescribir	X		X	Bitcoin
CryptoWall	2013	Phishing	Windows	Cifrado	RSA	Sobrescribir			X	Vales de prepago
FakeDefender	2013	Aplicación maliciosa.	Android	Ninguno	Ninguno	Ninguno		X		Vales de prepago
Lockdroid	2014	Aplicación maliciosa.	Android	Ninguno	Ninguno	Ninguno		X		Vales de prepago
SimpLocker	2014	Aplicación maliciosa.	Android	Cifrado	AES	Sobrescribir				Bitcoin
TorrentLocker	2014	Phishing	Windows	Dominios dinámicos	AES+RSA	Borrar			X	Vales de prepago
TrolDesh	2014	Phishing	Windows	Cifrado	AES	Borrar			X	Bitcoin
CryptoDefense	2014	Phishing	Windows	Ninguno	RSA	Borrar			X	Bitcoin
CTBLocker	2015	Phishing	Windows	Ninguno	ECC	Borrar			X	Bitcoin
TeslaCrypt	2015	Kits de explotación	Windows	Cifrado	AES	Borrar				Bitcoin
Fusob	2015	Phishing	Android	Ninguno	Ninguno	Ninguno		X		Tarjetas de regalo
Quimera	2015	Phishing	Windows	Cifrado	AES	Borrar			X	Bitcoin
LinuxEncoder	2015	Vulnerabilidad	Linux	Cifrado	AES+RSA	Borrar				Bitcoin
Ransom32	2016	Anuncio publicitario	OS-Agnostic	Cifrado	AES	Sobrescribir			X	Bitcoin
Dharma	2016	RDP	Windows	Cifrado	AES	Borrar			X	Bitcoin
Locky	2016	Phishing	Windows	Dominios dinámicos	AES+RSA	Borrar			X	Bitcoin
Cerber	2016	Phishing	Windows	Ninguno	AES	Sobrescribir				Bitcoin
Jigsaw	2016	Phishing	Windows	Cifrado	AES+RSA	Borrar			X	Bitcoin
KeRanger	2016	Aplicación maliciosa.	macOS	Cifrado	AES+RSA	Borrar			X	Bitcoin
Petya	2016	Kits de explotación	Windows	Cifrado	AES	Sobrescribir		X		Bitcoin
DMALocker	2016	Kits de explotación	OS-Agnostic	Cifrado	AES	Borrar			X	Bitcoin
Sage	2017	Drive-by-download	Windows	Cifrado	AES+RSA	Borrar				Bitcoin
BadRabbit	2017	Drive-by-download	Windows	Dominios dinámicos	AES+RSA	Borrar				Bitcoin
WannaCry	2017	Vulnerabilidad	Windows	Cifrado	AES+RSA	Borrar				Bitcoin

GoldenEye	2017	Kits de explotación	Windows	Cifrado	AES	Sobrescribir			X	Bitcoin
SamSam	2018	RDP	Windows	Cifrado	RSA	Borrar			X	Bitcoin
GandCrab	2018	Drive-by-download	OS-Agnostic	Cifrado	AES	Sobrescribir			X	Bitcoin
Sodikonibi	2019	Kits de explotación	Windows	Cifrado	AES+ECC	Sobrescribir		X	X	Bitcoin
Robbinhood	2019	RDP	Windows	Cifrado	AES+RSA	Borrar	X		X	Bitcoin
Laberinto	2019	Kits de explotación	OS-Agnostic	Cifrado	AES+RSA	Sobrescribir			X	Bitcoin
Ryuk	2019	RDP	OS-Agnostic	Cifrado	AES+RSA	Sobrescribir			X	Bitcoin
MegaCortex	2019	Exploit-kits	OS-Agnostic	Cifrado	AES	Sobrescribir			X	Bitcoin
LockerGaga	2019	Phishing	Windows	Ninguno	AES+RSA	Borrar			X	Bitcoin
Ekans	2019	Vulnerabilidad	ICS	Cifrado	AES+RSA	Borrar			X	Bitcoin
PureLocker	2020	Vulnerabilidad	OS-Agnostic	Dominios dinámicos	AES	Borrar			X	Proton
Tycoon	2020	Vulnerabilidad	Windows	Dominios dinámicos	AES	Borrar			X	Proton
CovidLock	2020	Aplicación maliciosa.	Android	Ninguno	Ninguno	Ninguno		X		Bitcoin
Corona	2020	Phishing	Windows	Ninguno	AES+RSA	Sobrescribir	X		X	Bitcoin

Fuente: A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. [2022]. P.13. Disponible en: https://arxiv.org/pdf/2102.06249.pdf

En la tabla anterior se observa las familias de ransomware que más se notaron durante el periodo 1989 y 2020; algunas de estas familias fueron evolucionando y surgieron nuevas variantes con capacidades superiores que hacían más efectiva la operación de los delincuentes. Se puede identificar que la mayor parte de los casos se presentó por medio correos electrónicos de phishing, el 33% de las variantes realizan los ataque a través de este método, los otros métodos más usados corresponden a kits de explotación, descargas automáticas y aplicaciones maliciosas. El 50% de las familias hacen uso de dirección IP o dominios codificados, en cambio una pequeña parte hace uso de dominios generados dinámicamente.

La mayor parte de ataques es realizada en las plataformas Windows, esto teniendo en cuenta que es el sistema operativo que más usuarios posee, y se puede identificar que la mayor parte de ransomware utiliza técnicas de cifrado es decir criptográfico, sin embargo, durante el periodo 2009 a 2013 hubo un aumento significativo en ransomware de casillero. El porcentaje más alto de ataque a plataformas PC es con ransomware criptográfico en cambio en equipos móviles es con ransomware casillero; el método de pago más usado en ransomware criptográficos por criptomonedas mientras en las plataformas móviles es a través

de SMS.

Hay más casos de cifrado de clave simétrica que cifrado de clave asimétrica y cifrado híbrido, solamente el 20% de ataques hacen uso de clave asimétrica; los algoritmos de cifrado los más empleados son ECC, AES y RSA.

4.2 MARCO CONCEPTUAL

Ransomware

El ransomware es un software malicioso que se asegura de bloquear un equipo de cómputo evitando que el usuario pueda acceder a este; es una amenaza común y en aumento. Los objetivos del ransomware han pasado de ser personas al azar a organizaciones más críticas y más grandes, como las de la industria de la atención de la salud.
También hubo un cambio reciente en las tácticas de ransomware para incluir intentos de extorsión. Los atacantes pasaron de simplemente intimidar a sus víctimas con una pérdida de datos catastrófica a amenazas que involucraban la publicación de datos exfiltrados con el fin de dañar su marca. Amenazar con publicar datos robados incrementa la probabilidad de obtener el pago del ransomware[26].

Cryptohacking

Un ataque de cryptohacking tiene como objetivo generar criptomonedas por medio de comandos computacionales de un tercero.
El Bitcoin (y, en consecuencia, la minería de criptomonedas) existen desde 2009. Los criptomineros reciben bitcoin al verificar transacciones y resolver problemas de hashing numéricos. La velocidad a la que se mina bitcoin se reduce a la mitad cada cuatro años. Esta reducción afecta de manera inversa la dificultad de minar y por lo tanto, la potencia informática que se necesita para minar bitcoin eficazmente. Los mineros modernos necesitan invertir en unidades de procesamiento de gráficos (GPU) o circuitos integrados de aplicación específica (ASIC) si tienen esperanzas de ser competitivos e, incluso entonces, están peleando una batalla cuesta arriba[27].

Cifrado Asimétrico

El cifrado asimétrico o de clave publica se basa en la utilización de dos claves distintas, la primera para el procedimiento de cifrado y la segunda para el procedimiento de descifrado. La idea de este proceso es que únicamente pueda ser descifrado por la clave privada.

---

[26] BLACKBERRY. Perspectivas sobre la seguridad cibernética. *Informe de amenazas 2021.* 2021. P.8. Disponible en: https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report-sp.pdf

[27] Ibid.

Para el proceso de cifrado la idea es hacer uso de funciones matemáticas de manera que la operación directa sea sencilla y su inversa muy complicada, un ejemplo los algoritmos o la potenciación.
La clasificación de los sistemas asimétricos se presenta en función del método usado: factorización entera, logaritmo discreto y curva elíptica.
La factorización entera fue el primero en surgir dentro del proceso de calve publica, basándose en que no existe método eficiente para factorizar un numero procedente de la multiplicación de dos números primos. Un ejemplo de este sistema es el RSA, un algoritmo que hace uso de un numero obtenido de dos números primos entre 100 y 300 cifras.
El logaritmo discreto es un algoritmo asíncrono de calve privada, seguro y de solución sencilla en una única dirección; este algoritmo calcula un numero x que verifica h=g. los numero h y g son identificado y g surge de la expresión modular g =pMOD(q)[28].

4.3 MARCO HISTÓRICO

Desde su aparición el ransomware ha ido evolucionando y creando múltiples variables, desde herramientas simples hasta organizaciones robustas que se dedican a esta actividad desde la clandestinidad.

El primer caso de ransomware conocido se remota al año 1989 y se conoce como el Troyano del SIDA, su distribución fue a través de disquetes decían llevar información asociada a bases de datos sobre el virus del SIDA y factores asociados a esta enfermedad. Cuando se activaba el sistema de malware, este desactivaba el acceso del usuario a la mayor parte del disco. El ransomware pedía como rescate una suma de dinero que debía enviarse a un buzón de correo en Panamá[29].

Según el Centro de Denuncias por delitos de Internet, en el año 2015 las víctimas de este delito perdieron más de 24 millones de dólares en casi 2500 ataques de ransomware.

[28] Criptografía clásica y moderna. Miguel García, Roberto . Disponible en: https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/102985?page=72
[29] ESET. Ransomware ¿Cómo protegerte? Conoce cómo evitar el secuestro de datos. [Sitio web]. España. Disponible en: https://www.eset.com/es/caracteristicas/ransomware/

En el año 2016 en los Estados Unidos el Centro de Denuncias por delitos de Internet registraba aproximadamente 7700 casos (denuncias públicas) asociados al ransomware desde el año 2005, con un total de 57.6 millones en daños.

De los eventos más impactantes se tiene registro es el WannaCry ocurrido en el año 2017, el cual se viralizó rápidamente aprovechando vulnerabilidades del sistema operativo Windows, en esta ocasión miles de empresas fueron afectadas por el ataque cibernético y el daño ocasionado fue significativamente alto, pues las pérdidas fueron de miles de millones de dólares.

En noviembre del año 2020, en el país de Brasil se produjo un ataque de ransomware al Tribunal Superior de Justicia, dejando sin servicio el sitio web y afectando la infraestructura de TI. Se bloqueó el acceso a los datos cifrándolos, y se detuvieron las operaciones por una semana[30].

[30] KASPERSKY. Ransomware: los ataques más resonantes de 2020. [Sitio web]. [2021]. Disponible en: https://latam.kaspersky.com/resource-center/threats/top-ransomware-2020

4.4 MARCO LEGAL

Aspectos generales de la ley 1273 de 2009

La ley 1273 de 2009 que rige en Colombia menciona los procesos relacionados al delito informático que atenta contra la protección de la información y de los datos. Se denomina acceso abusivo a un sistema informático, todo proceso que viole y atente contra la integridad de la información de una empresa, tal acto puede tener como consecuencia hasta 96 meses de privación de la libertad según el artículo 269 A de esta ley; igualmente se le considera delito a la obstaculización e interceptación de datos informáticos, toda vez que se violenta la seguridad, y confidencialidad de los datos poniendo en riesgo el funcionamiento de una empresa, por lo cual las personas que sean sorprendidas en estas prácticas deben ser privadas de la libertad.

La ley 1273 busca combatir la delincuencia basada en los ataques informáticos, como los ocasionados por el uso de software malicioso, la suplantación de sitios web y violación de datos personales que vulneren y deterioren el desarrollo normal de las actividades y producción de las entidades ocasionando perjuicios en las mismas o en sus usuarios (Art 269 E, F, G).

Además se le considera delito informático al hurto de medios informáticos y suplantación de usuarios accediendo y vulnerando las credenciales de autentificación a correos electrónicos y aplicativos propios de las empresas, poniendo en riesgo la integridad de los mismos usuarios o terceras personas y atentando contra los recursos y activos de la empresa. Tales actos delictivos tienen como consecuencia privación de la libertad y multas económicas de acuerdo al nivel de gravedad de los actos realizados (Art 269 I).

Adicionalmente con la ley 1273 se debe implementar en las políticas de seguridad de la información y las políticas de tratamiento de datos personales de las instituciones, buscando garantizar la protección de los derechos fundamentales en el tratamiento de datos personales con calidad y transparencia velando la protección integral de los usuarios para que no se no se afecte su intimidad y de esta forma asegurar la validez de la información en tiempo, forma y distribución[31].

[31] ALCALDÍA DE BOGOTÁ. Régimen legal de Bogotá D.C. Ley 1273 de 2009 Nivel Nacional. [Sitio web]. Bogotá. [23 de enero 5 de 2009]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

“Cada 24 horas son reportados a la Fiscalía General de la Nación en promedio 67 casos nuevos de infracciones a la ley de delitos informáticos (Ley 1273 de 2009). Este creciente nivel de afectación tiene una relación directa con el incremento de casos de phishing denunciados durante el primer trimestre de 2020, cuya cifra ya supera 804 casos registrados y una variación porcentual de +240% respecto a los 235 casos reportados en 2019”[32].

[32] Cámara Colombiana de Informática y Telecomunicaciones. El TicTac presenta su informe: Tendencias del Cibercrimen en Colombia; primer trimestre de 2020. [Sitio web]. Colombia. [2020]. Disponible en: https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/

5 GENERALIDADES, CARACTERÍSTICAS, FAMILIAS, VARIANTES Y EVOLUCIÓN DEL CÓDIGO MALICIOSO RANSOMWARE

Un gran número de ataques que están comprometiendo la seguridad de las organizaciones, están asociados a alguna variante de malware. Una amplia variedad de acciones maliciosas está siendo dirigidas a un gran espectro de plataformas usadas en ordenadores, dispositivos móviles, y dispositivos IoT; lo que comprueba que el ciberdelito a través de esta práctica es uno de los métodos más usados por los atacantes.

El ransomware es un tipo de ciber ataque que tiene muchas formas. Desde sus inicios esta clase de malware se ha vuelto con el tiempo más destructivo y sofisticado. Algunos están agrupados a otras clases de malware que se dedican a robar información como credenciales de ingreso a cuentas bancarias, instalan botnets e incluso abren puertas traseras. Además, tiene la capacidad de personalizar sus mensajes al lenguaje de las víctimas. Al principio impedían el acceso al navegador o al sistema operativo a cambio de un precio bajo, este cobro se hacía a través de un SMS a un numero de extensión corta similar a las líneas de emergencias, o por transferencia a un monedero electrónico. Este sistema fue evolucionando en la medida que las autoridades fueron desmantelando estos métodos de pago. El sistema se fue robusteciendo con la aparición de las criptomonedas, toda vez que con esta nueva forma de pago podían cobrar por los rescates de información de manera anónima[33].

Por otro lado, las nuevas tecnologías y técnicas de cifrado permitieron evolucionar su mecanismos de extorsión, encriptando los datos almacenados en discos duros y otros sistemas, lo que les facilitó el aumento del precio por el rescate de la información. también se fue incrementando los ataques a las empresas.

La historia de este tipo de ataque se divide en dos: antes y después del cifrado. Primero fueron los bloqueadores y luego llegaron los cifradores modernos, al comienzo el ransomware estaba dirigido especialmente a los usuarios domésticos, sin embargo, con las técnicas de cifrado comenzaron atacar de forma masiva a las empresas.

[33] CN-CERT. Informe de Amenazas. Medidas de seguridad contra ransomware. España. [2017]

Con estos nuevos mecanismos algunas variantes logran cifrar no solo el equipo infectado sino también los equipos y unidades de almacenamiento que se encuentran dentro de la misma red; además van apareciendo variantes con capacidad de infectar dispositivos móviles y IoT.

Fueron apareciendo familias de ransomware que le han causado perdida de millones de dólares a las organizaciones, algunas de esta familias son: Jigsaw, Apocalypse, Kozy.Jozy, MIRCOP, Locky, TeslaCrypt, Xorist, CryptorBit, CriptXXX, Crysis, BlackShades, MSIL o Samas (SAMSAM), FLocker, RAA, Criptowall y CTB-Locker[34].

Los delincuentes utilizan distintas tácticas para alcanzar sus objetivos, por ejemplo, con el Cryptoloker logran cifrar los archivos de un ordenador con una clave que únicamente el delincuente conoce, por otra parte, con el Winloker solamente bloquea el sistema, aunque los datos no quedan cifrados[35].

Los ciberdelincuentes hacen uso de técnicas sofisticadas como ingeniería social para activar el software malicioso a través del envío de correos electrónicos con contenido adjunto infectado, en extensiones. doc, .xls, .pdf entre otros, o a través de enlaces publicitarios en sitios web, una vez el usuario caiga en la trampa, se activa el sistema y el daño es inevitable, se puede decir que en ese momento el usuario pierde todos los derechos de administrador del PC y sus archivos, y ahí es cuando comienza el pedido de dinero por el rescate, que en ultimas es el objetivo de la técnica de secuestro de datos.

En estos ataques normalmente se presenta un mensaje extorsivo en el equipo afectado (suele aparecer algún tipo de ventana emergente), donde se le solicita a la víctima el pago de un monto de dinero por el rescate de la información, normalmente se solicita que el pago sea realizado a través de la moneda digital

[34] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Ransomware una guía de preparación para el usuario. [Sitio web]. España. [2017]. P.8. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

[35] KASPERSKY. Identificación de ransomware: en qué se diferencian los troyanos de cifrado. [Sitio web]. Disponible en: https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Bitcoins, lo que le permite al delincuente permanecer en el anonimato[36]; en caso de realizarse el pago, el usuario afectado recibe un mensaje con la clave para descifrar los archivos y tener acceso al sistema nuevamente.

Los ciberdelincuentes son cada vez más organizados, ya que cuentan con una estructura administrativa y herramientas sofisticadas, no solo para alcanzar la intrusión a los sistemas sino para seguir todo el proceso hasta cobrar el dinero y restaurar la información nuevamente, entre otras cosas prestan un servicio de asistencia técnica todo el tiempo para que la víctima realice el paso a paso del proceso que le corresponde hasta restablecer su sistema y archivos. Los grupos delictivos forman estructuras empresariales y sus miembros cumplen con ciertos perfiles y determinadas funciones; algunos se dedican a detectar las vulnerabilidades, otros trabajan creando código, otros se encargan de la distribución de software malicioso, otros realizan el contacto para negociar el rescate y toros coordinan el sistema de pago. Realmente se ha creado un modelo de negocio bastante organizado de estructura criminal, que está logrando poner a las víctimas contra la espada y la pared y haciendo entender que el pago de la extorsión es la única opción.
La propagación de ransomware es muy similar a otras clases de malware, por ejemplo correos electrónicos de phishing, drive-by y wáter holing entre otros; solo para objetivos de perfil alto usan técnicas más sofisticadas de ataque dedicado.

El ransomware regularmente se ejecuta mediante correos electrónicos de phishing con contenido malicioso adjunto, o a través de descargas; en el momento en que un usuario visita una página web infectada, puede descargar un archivo que se instala de forma automática ejecutando el malware en el ordenador.

Las grandes ganancias que ha venido dejando el ransomware ha ocasionado la multiplicación de variantes destructivas como por ejemplo CryptoLoker, CryptorBit o Xorist; algunas de estas tienen la capacidad de cifrarlos equipos infectados junto con los dispositivos conectados en la red , estas variantes son altamente destructivas, los archivos quedan inservibles hasta que se logre el descifrado a través del rescate.

[36] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Ransomware una guía de preparación para el usuario. [Sitio web]. España. [2017]. P.25. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

La variante Locky se ha dedicado a infectar equipos en hospitales y empresas del sector salud, su propagación ha sido mediante correos electrónicos tipo spam con adjunto maliciosos en carpetas comprimidas o documentos office, estos archivos vienen con macros JavaScript que descargan el Ransomware-Locky.

La variante Samas aprovecha vulnerabilidades de servidores web para propagarse y posteriormente infectar las redes de las organizaciones.

La variante Web Exploit Kits aprovecha vulnerabilidades en los plugins instalados, en este sentido si la victima visita una página web comprometida, un iframe realiza la redirección hacia otro sitio web malicioso en el que se encuentra presente un Web Exploit Kits que se encargará de explotar todas las vulnerabilidades del navegador. El ransomware criptográfico se encarga de cifrar archivos aprovechando vulnerabilidades en los servidores para acceder a las redes, otros métodos utilizados con esta variante son por medio de redes sociales y aplicaciones de mensajería instantánea[37].

En Colombia han sido detectado principalmente cinco tipos de clases de ransomware:

Tabla 2. Principales tipos de ransonware en Colombia

VARIANTE	DESCRIPCIÓN
Ransomware de cifrado	Cifra archivos personales y documentos, hojas de cálculo, imágenes y videos.
Lock Screen Ransomware	WinLocker Bloquea la pantalla del PC y solicita el pago.
Master Boot Record (MBR) Ransomware	Es la parte del disco duro del PC que permite iniciar el sistema operativo.
Ransomware de cifrado de servidores web	Su objetivo son los servidores web y cifrar sus archivos.
Ransomware de dispositivos móviles	Los dispositivos móviles (principalmente Android) pueden infectarse mediante descargas no oficiales.

[37] CN-CERT. Informe de Amenazas. Medidas de seguridad contra ransomware. España. [2017]. P.28. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1974-ccn-cert-ia-03-17-medidas-seguridad-ransomware-1/file.html

Fuente: Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia [29 de octubre de 2019]. P.36. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Principales amenazas en los diferentes sistemas operativos

Principales amenazas para MAC

EvilQuest

Es un tipo de ataque dirigido a MacOS que fue descubierto en el año 2020. Este ransomware se ha encontrado en copias ilegitimas de sistema operativo MacOS. El malware realiza solicitudes de privilegios de administrador y cuenta con una utilidad para ejecutar código remoto capaz de extraer datos como certificados de usuario[38].

AppleJeus

Es un tipo de ataque que tiene por objetivo clientes que comercializan criptomonedas. Los ciberdelincuentes cuentan con un sistema de compra y venta de criptomonedas que contiene componentes de instalación para Windows y macOS. El ejecutarse este instalador da al atacante acceso al host. Tan pronto es ejecutado el malware realiza una recopilación de datos del sistema y la extrae a su servidor[39].

NuksSped

Apareció como una aplicación de criptomonedas en la cual los delincuentes falsificaban información y una plataforma de inicio con apariencia de legitimidad, que hacía la distribución de la aplicación maliciosa. Esta amenaza tiene la capacidad de recopilar datos del sistema y conectividad de red para poder materializar el ataque[40].

Principales amenazas para LINUX

[38] BLACKBERRY. Perspectivas sobre la seguridad cibernética. Informe de amenazas 2021. 2021. P.14. Disponible en: https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report-sp.pdf
[39] Ibid.
[40] Ibid., P.13.

Tsunami

Esta botnet es conocida por realizar ataques dirigidos a IoT y realizar comunicación a través del protocolo IRC. Tsunami hace uso de vulnerabilidades como credenciales administrativas con codificación fija[41].

Mirai

Esta botnet ataca las vulnerabilidades de hardware de redes como routers y dispositivos IoT; realiza a taques con diccionarios para ingresar a sistemas vulnerables. Además, tiene la capacidad de realizar ataques de denegación de servicio /DDoS)[42].

FritzFrog

Es un ataque dirigido a servicios SSH que busca acceder a credenciales a través de fuerza bruta para ingresar a los sistemas, FritzFrog hace uso de diccionarios robustos con el fin de abarcar una red más amplia. Esta botnet hace uso de protocolo p2p personalizado, y los procesos son realizados en la memoria para no utilizar el sistema de archivos[43].

Principales amenazas para WINDOWS

BazarLoader

Es un tipo de ataque que se hace uso de correos electrónicos de phishing y spam para infectar los equipos, cuando el malware es ejecutado busca conectarse con un dominio .bazar del servidor de control para realizar otra descarga de malware desde el servidor del atacante que le permite tener el control total de la maquina víctima[44].

Bladabindi

También se conoce con el nombre de njRAT, este malware tiene la capacidad de activar cámaras web, realizar capturas de pantalla, captura de digitaciones en el

[41] Ibid., P.15.
[42] Ibid.
[43] Ibid., P.16.
[44] Ibid., P.17.

teclado, captura de contraseñas y control remoto. El malware esta creado en . NET y ejecuta funciones de keylogging y RAT de Bladabindi.
El sistema se conforma por una cadena de valor de 32 caracteres y es ejecutado cuando el malware es instalado en inicio automático en la siguiente ruta:

'HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ab1c039a01d925ae481774f412396f5e'
y
'HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion
\Run\ab1c039a01d925ae481774f412396f5e'
con el valor de la ruta del malware almacenado en
%TEMP%, %APPDATA%, %USERPROFILE%,%ALLUSERSPROFILE%[45].

Wacatac

Es un tipo de ataque que tiene la capacidad de ejecutar actividades como la recopilación de datos, personales y bancarios, y acceso a control remoto; el malware puede alojarse en la carpeta de inicio del usuario y con frecuencia puede instalar archivos en el directorio %APPDATA%. La ejecución de Wacatac también se asocia al ransomware DeathRansom teniendo en cuenta la clave de registro HKEY_CURRENT_USER\SOFTWARE\Wacatac que se crea[46].

Los ciberdelincuentes también hacen uso de herramientas sofisticadas para escanear dispositivos de forma masiva buscando servicios de terminal server e intentar ingresar a través de ataques por diccionario.
Algunas de las estrategias usadas por los ciberdelincuentes para motivar el pago del rescate, es a través de amenazas de publicación de datos dado el caso que en muchos lugares existe leyes de protección y no divulgación de datos personales, lo que puede incurrir en sanciones legales para las empresas; todo parece indicar que no hay otra opción más que pagar cuando se sufre un ataque de estos, sin embargo no existe garantía de que el delincuente se abstenga de publicar los datos o de darle otros usos indebidos, independientemente si se paga por el rescate. Ahora las cosas se van poniendo más difíciles en la medida que aumenta la presión, primero el temor de perder la información, segundo el riesgo de exposición de los datos, y como si

[45]Ibid., P.18.
[46] Ibid., P.22.

fuera poco la nueva estrategia para agilizar el cobro es agregando ataques de denegación de servicio, mientras no se pague la extorsión las plataformas de la empresa estarán caídas[47].

"Este año, los atacantes continuarán con sus ataques de ransomware mientras recurren a la doble extorsión para presionar a la víctima a fin de que pague el rescate. Durante 2020, los delincuentes cibernéticos robaron estratégicamente datos de las víctimas antes de cifrarlos, y a continuación amenazaban con publicar la información robada o incluso dársela a un competidor. Esta táctica se usa para obligar a la víctima a pagarle al atacante (o al menos, contactarse con él) para recuperar los datos. La estrategia incrementó el monto promedio de los pagos de rescate durante 2020, aunque no existen garantías de que el atacante elimine las copias de datos de la víctima que tiene en su poder. Se detectaron casos en que los atacantes publicaron igualmente los datos de la víctima después de recibir el pago del rescate"[48].

Últimamente las acciones destructivas de este tipo de ataque han evolucionado hacia una nueva generación de ransomware conocida como File encryotors, que tiene como función cifrar la mayor cantidad de archivos de los dispositivos; de igual forma como es su modo de operación se inicia una extorsión con el fin de que el usuario obtenga una clave para poder descifrar estos archivos, dependiendo del tipo de ransomware así mismo varia la complejidad del cifrado; algunos hacen uso de recursos de terceros como WinRar o LockDir, mientras que otros usan algoritmos de cifrado interno como AES o RSA.

También dependiendo de la complejidad y técnicas utilizadas se presenta el nivel de destrucción, por ejemplo CryptoLoker tiene la capacidad de combinar cifrado simétrico y asimétrico para impedir otras formas de restauración de ficheros, estos normalmente son sobrescritos a través de herramientas de seguridad para dificultar su restauración mediante técnicas de informática forense. De otra forma muchas variantes hacen uso de clientes de red I2p2 o TOR1 para tratar de impedir la comunicación de los servidores de control en la red.

---

[47] SOPHOS. EL ESTADO DEL RANSOMWARE 2021. [Sitio web]. [2021]. P.18. Disponible en: https://secure2.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-state-of-ransomware-2021-wp.pdf

[48] BLACKBERRY. Perspectivas sobre la seguridad cibernética. *Informe de amenazas 2021.* 2021. P.46. Disponible en: https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report-sp.pdf

Los ataques ransomware se han venido centrado más hacia las organizaciones por un gran motivo, las organizaciones tienen grandes volúmenes de información que representan bastante dinero, adicionalmente un ataque dirigido a una organización puede terminar afectando también al grupo de proveedores de esta, lo cual representa una motivación más para gestionar el pago. De hecho otra de las técnicas usadas para crear vulnerabilidades es a través de proveedores o terceros de confianza, ya que si se recibe un correo remitido por un proveedor no se genera ningún tipo de sospecha, aun así puede crearse un canal de comunicación para introducir malware al ordenador.

Una vez que el ciberdelincuente logre ingresar a los sistemas, puede pasar muchos días revisando e inspeccionando la información que tenga más valor para la empresa antes de proceder con el cifrado, además se toman el tiempo para crear puertas traseras con el fin de volver a ingresar y tener la posibilidad de ejecutar otro ataque.

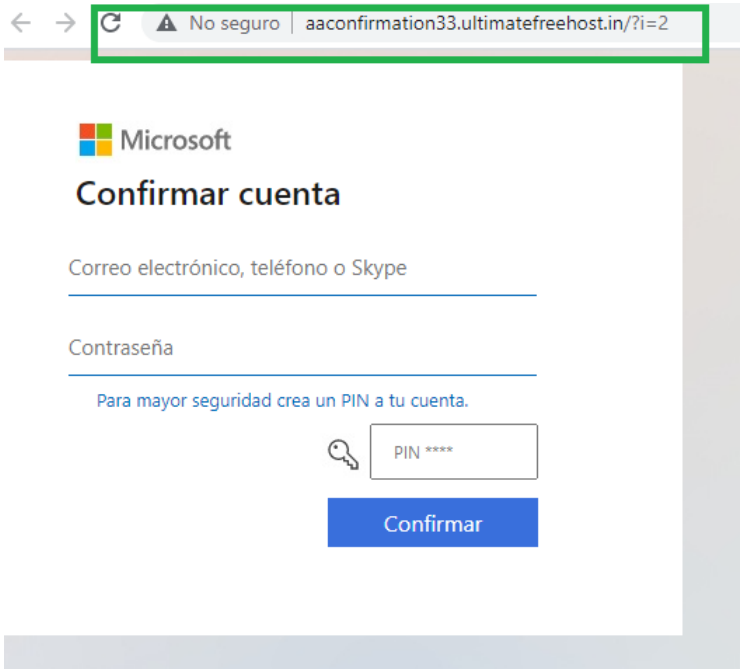
Muchos de los eventos cibernéticos en los sistemas pueden deberse a una mala acción o falta de conocimiento por parte del usuario al momento de presentarse el intento de ataque, el uso de ingeniería social, mensajería spam o phishing es el vector más usado en esta técnica de secuestro de datos. Una de las formas de iniciar el ataque es enviando un correo alertando a la persona sobre cambios en alguna cuenta o brindando promociones, en este sentido los piratas informáticos simulan la interface de las plataformas creando una réplica similar o exacta de estas, cuando un usuario ingresa la información a estos formularios están entregando datos de vital importancia que le pueden costar grandes pérdidas.

En este caso a manera de ejemplo en la siguiente imagen se ve un intento de fraude en donde el atacante se hace pasar por un soporte de Microsoft y envía una alerta sobre la supresión de la cuenta de correo electrónico.

Figura 3. Método de ataque por phishing imagen 1.

Fuente: Autor.

Figura 4. Método de ataque por phishing imagen 2.



Fuente: Autor.

Aquí se ve claramente que el correo procede de una cuenta que no pertenece al soporte de Microsoft y el enlace se dirige a un formulario sospechoso que intenta captar las credenciales de la cuenta de correo electrónico.
Además, Se puede evidenciar que el dominio donde se encuentra el formulario no pertenece a Microsoft.

Como se ha mencionado anteriormente el phishing mediante correos electrónico o mensajes falsificados es uno de los métodos más usados para instalar malware y ejecutar ransomware. Es por eso que se resalta la importancia de capacitación al talento humano sobre el manejo que se le debe dar a este tipo de mensajes, identificar la procedencia, abstenerse de descargar archivos adjuntos y no enviar ningún tipo de datos a través de estos formularios que solicitan información.

La siguiente ilustración muestra el ciclo de vida típico de un ataque de phishing con consentimiento mediante la cadena de ataque cibernético Lockheed Martin.

Figura 5. ciclo de vida típico de un ataque de phishing.

Fuente: BLACKBERRY. Perspectivas sobre la seguridad cibernética. *Informe de amenazas 2021.* 2021. P.35. Disponible en: https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report-sp.pdf

Es importante conocer el dominio de los sitios web oficiales, para poder identificar los enlaces fraudulentos y de esta forma minimizar el riesgo de ser víctimas de esta técnica de ciberataques. Revisar detalladamente la redacción del mensaje y la ortografía. Para casos específicos de suplantación se recomienda implementar y configurar adecuadamente una política "reject", este control mitiga en gran proporción la suplantación de dominios.

6 IMPACTO, VECTORES DE INFECCIÓN E INDICE DE CRECIMIENTO DE RANSOMWARE DE COLOMBIA EN LOS ÚLTIMOS 2 AÑOS.

Los ataques por ransomware representan un riesgo para las organizaciones que les está costando miles de millones de dólares; en este documento se va a tratar el impacto de ataques de virus ransomware en organizaciones colombianas, sin embargo a modo de introducción para tener una idea de la magnitud del problema que se está presentando, vamos a revisar la experiencia de una empresa con presencia en varios países del mundo, se trata de Travelex una empresa de cambio de divisas, que fue objeto de un ataque por ransomware en enero de 2020, por el rescate de la información los delincuentes pedían la suma de 6 millones de dólares, de los cuales aparentemente la empresa logró pagar 2,3 millones; en esta ocasión los piratas informáticos manifestaban tener el control de 5 GB de información perteneciente a Travelex y amenazaba con eliminar los datos si no se pagaba por el rescate. Aunque la empresa logró reactivar sus operaciones después de dos semanas del evento, unos meses después fue declara en bancarrota y atribuyó las razones al efecto que causó el ataque cibernético y la pandemia COVID-19[49].

"El cibercrimen ha experimentado un crecimiento durante los últimos años casi de forma paralela al uso de las nuevas tecnologías y las pérdidas generadas por los ciberataques sitúan a esta problemática como una de las principales economías ilegales en el País. El impacto que sufren las empresas colombianas luego de un ciberataque trasciende el coste económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones a la productividad, daños reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y data sensible. En Colombia, el monto promedio de las cifras de pérdidas por ataque puede oscilar entre 300 millones y 5.000 millones de pesos, según el tamaño de la empresa afectada"[50].

Los responsables de tecnologías de la información o infraestructura tecnológica de las empresas deben estar revisando y evaluando las nuevas características de protección y detección de ransomware con el objetivo de identificar plataformas de

[49] KASPERSKY. Ransomware: los ataques más resonantes de 2020. [Sitio web]. [2021]. Disponible en: https://latam.kaspersky.com/resource-center/threats/top-ransomware-2020

[50] Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia [29 de octubre de 2019]. P.1. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

copia de seguridad, toda vez que los ataques de ransomware cada vez son más sofisticados y están siendo dirigidos a funciones de administrador y datos de copias de seguridad, ya que estos buscan comprometer los sistemas críticos y las funciones administrativas.

En el año 2020 la multinacional especializada en ciberseguridad Sophos realizó una gran encuesta a 5000 responsables de TI, sobre sus experiencias con el ransomware, en 26 países del mundo entre ellos Colombia[51].

El 51% de las organizaciones fueron atacadas por ransomware.
El 73% de los ataques lograron cifrar los datos, el 26% de las victimas pagaron por el rescate de la información.
el 95 % de las organizaciones que pagaron el rescate recuperaron sus datos (473 de las 496 organizaciones que lo pagaron).
El 24% lograron detener el ataque antes de ser cifrados.
El 94% de las organizaciones que tuvieron datos cifrados, lograron recuperar la información, de estos el 56% por medio de copias de seguridad[52].

En el año 2020 los ataques fueron dirigidos mayormente hacia los servidores, probablemente porque el contenido de estos activos puede ser de más valor, lo que puede resultar más lucrativo para los delincuentes.

En los últimos 12 meses el 19% de las empresas en el país se vieron afectadas por ransomware, aun así, el promedio mundial es del 37%, lo que quiere decir que el país ha tenido un menor índice de ataques en comparación con otros países, esto puede ser porque el producto interno bruto en Colombia es bajo al igual que otros países de la región, por lo que las probabilidades o disponibilidad de pago es menor. Aun así en Colombia se han realizado más de 3.700 millones de intentos de ataques cibernéticos, las ciudades más afectadas son Bogotá, Medellín y Cali; en toda América Latina se registraron aproximadamente 91.000 millones de intentos de ataques durante el mismo periodo[53].

---

[51] SOPHOS.EL ESTADO DEL RANSOMWARE 2020.Resultado del studio independiente realizado a 5000 directores de TI en 26 países. 2020. P.18. Disponible en: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

[52] Ibid

[53] SEMANA. El 37 % de las empresas a nivel mundial fue atacado con ransomware en el último año. [Sitio web]. Colombia. [2021]. Disponible en:

“El 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis meses luego de sufrir un ciberataque importante. Esto demuestra que los factores en torno a los Ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías”[54].

De los países objetos de ataques cibernéticos, Colombia ocupa el cuarto lugar en Latinoamérica superado por México, Brasil y Perú[55]; el incremento de uso masivo de dispositivos IoT y aplicaciones digitales empleados para reuniones y clases virtuales ha causado un amento en posibilidades de intentos de intrusión a los sistemas de información, alguna de las vulnerabilidades se presentan porque la mayoría de las instituciones no provee capacitaciones sobre el manejo seguro de la información en la metodología de teletrabajo (servicios en la nube, reuniones remotas, escritorios virtuales, información de trabajo colaborativo, VPN, canales digitales).

Se estima que en Colombia el promedio de ataques en el mes de junio de 2021 se multiplicó por 10 en comparación con el mismos periodo del año anterior lo que indica un aumento significativo periódicamente. Los ataques fueron dirigidos mayormente al sector de telecomunicaciones, seguido por el sector de administración pública, aun así, el ransomware es un problema a nivel de ciberseguridad que afecta a todos los sectores[56].

https://www.semana.com/economia/capsulas/articulo/el-37-de-las-empresas-a-nivel-mundial-fue-atacado-con-ransomware-en-el-ultimo-ano/202122/

[54] Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia [29 de octubre de 2019]. P.36. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[55] ENTER.CO. Siguen incrementando los ciberataques en Colombia. [Sitio web]. Colombia. [16 de septiembre de 2021]. Disponible en: https://www.enter.co/empresas/seguridad/siguen-incrementando-los-ciberataques-en-colombia/

[56] DATA CENTER MARKET. El ransomware se multiplica por diez en el último año y se centra en sectores críticos. [Sitio web]. [8 de septiembre de 2021]. Disponible en: https://www.datacentermarket.es/tendencias-tic/noticias/1128063032809/ransomware-se-multiplica-diez-ultimo-ano-y-se-centra-sectores-criticos.1.html

Según datos del centro cibernético de policía nacional, los ataques cibernéticos aumentaron hasta un 150% en un periodo de 9 meses. Se estima que en Colombia se registran 87 intentos de ataques malware por minuto[57].

Según un estudio realizado por Tendencias del Cibercrimen en Colombia, el 83% de las organizaciones no cuentan con protocolos de respuesta a incidentes de seguridad; adicionalmente la piratería está presente en dispositivos personales y empresariales, lo cual está creando puertas de acceso a los cibercriminales; la gran cantidad de programas piratas es un factor que está impulsando de forma acelerada el ciberdelito, permitiendo así el control total de los equipos a los delincuentes. Por el hecho de no hacer uso de software licenciado, no se está instalado los parches de seguridad oficiales y como resultado se ha estado incrementando las infecciones por ransomware[58].

En los últimos meses las amenazas se han venido aplicando más a los dispositivos móviles debido a la migración de teletrabajo y el uso de plataformas a través de estos equipos, sin embargo el software pirata también se encuentra en servidores que guardan los datos de las organizaciones, según datos de la compañía Kaspersky durante en el año 2021 se ha logrado detener más de 1000 intentos de infección maliciosas asociadas a Criptomonedas y WannaCry dirigidos a servidores Windows[59].

Los ataque por ransomware han detenido cadenas de suministros de muchas empresas en Colombia, esto ha causado impacto negativo en el comercio y la productividad, lo que significa pérdidas financieras incurridas para restablecer sistemas y datos, y daño potencial a la reputación de las empresas; el ransomware puede acabar con organizaciones enteras si no se cuenta protocolos de respuesta a incidentes de seguridad.

[57] VALORA ANALITIK. Actividad maliciosa en internet aumentó en un 150 % en Colombia durante aislamiento. [Sitio web]. Colombia. [2021]. Disponible en: https://www.valoraanalitik.com/2021/02/27/actividad-maliciosa-en-internet-aumento-un-150-durante-el-aislamiento/

[58] Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia [29 de octubre de 2019]. P.13. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[59] KASPERSKY. Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [Sitio web]. [2021]. https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

La compañía internacional de seguridad informática Kaspersky asegura el 30% de las víctimas de ransomware en Colombia, terminaron pagando por el rescate de la información, de estas víctimas que realizaron el pago solo el 35% pudo restablecer toda la información, esto confirma que pagar por el rescate no da garantía de recuperar los datos cifrados[60].

Tabla 3. Datos de empresas afectadas en Colombia

CONCEPTO	**RESULTADO**
Monto promedio de pérdidas económicas Por empresa a causa de ataques cibernéticos	Entre 300 y 5000 millones de pesos
Intentos de ataques malware por minuto	87
Cuidades más afectadas	Bogotá, Madelin y Cali
Empresas que no cuentan con protocolos de respuesta a incidentes de seguridad	83%
Empresas afectadas por ransomware en los últimos 12 meses	19%
Víctimas que han pagado por el rescate de la información	30%
De las víctimas que realizaron el pago se logró restablecer toda la información	35%

Pagar el rescate no garantiza la liberación de los archivos cifrados; solo garantiza que los malintencionados reciban el dinero de la víctima y, en algunos casos, su información bancaria. Además, descifrar archivos no significa que se haya eliminado la infección de malware.

A razón de la presencia del Covid-19 y el confinamiento que inició en el año 2020 en Colombia y el mundo entero, las actividades cotidianas se han direccionado más hacia el teletrabajo o trabajo remoto; de esta forma se ha ido centrando el crimen desde la virtualidad, razón por la cual ha venido surgiendo la necesidad de contar con productos, servicios y procedimientos que permitan proteger unos de los activos con más valor en las empresas, que es la información. En este sentido es importante centrar esfuerzos para lograr un ecosistema digital seguro.

[60] VANGUARDIA. Tres de cada 10 víctimas de 'ransomware' en Colombia pagan el rescate. [Sitio web]. Colombia. [2021]. Disponible en: https://www.vanguardia.com/tecnologia/tres-de-cada-10-victimas-de-ransomware-en-colombia-pagan-el-rescate-CY3652307

De esta forma hay que asimilar que gran parte de la vida de los seres humanos se está desarrollando a través de plataformas digitales y que del mismo modo que el mundo físico representan riesgo y requiere cuidados, el mundo virtual es un escenario similar pero con la desventaja que muchas personas no son conscientes de esto y no saben cómo protegerse.

El gobierno colombiano al igual que algunas empresas ha venido realizando esfuerzos para darle prioridad a la seguridad digital creando campañas y cursos dirigidos al sector empresarial con el fin de fortalecer las prácticas de ciberseguridad.

En el mes de mayo de 2021 la Fiscalía General de la Nación informó que en Colombia hubo más de 20.000 noticias criminales en los primeros meses del año, y que con relación al mismo periodo del año anterior hubo un incremento del 35%. Un reporte que genera alertas a las empresas sobre lo que está aconteciendo en el país[61].

Según datos reportado por el programa Seguridad Aplicada al Fortalecimiento Empresarial (del Tanque de Análisis y Creatividad de las TIC), en el último año el ciberdelito se ha incrementado en un 35% con relación al año anterior, se tiene información de más 20502 noticias criminales reportadas entre enero y mayo 2021, y 15705 en el mismo periodo de 2020[62].

En Colombia el 9 de noviembre de 2021 el Departamento Administrativo Nacional de Estadística (DANE) se vio afectado por ciber secuestro de datos.

“Una de las incógnitas que es materia de investigación de la Fiscalía es a quién le sirve la información que se vulneró. Hipótesis hay varias, pero una es que se trata de un secuestro de datos en el que el supuesto atacante pretendió recibir a cambio 25.000 dólares.

[61] CCIT. Evaluacion, retos y amenazas a la Ciberseguridad. [Sitio web]. [2021]. P.13. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

[62] CCIT. Evaluacion, retos y amenazas a la Ciberseguridad. [Sitio web]. [2021]. P.16. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

No obstante, EL COLOMBIANO conoció que la Fiscalía evalúa una presunta pérdida de al menos 200 teras con información que se habría llevado el atacante y la afectación a 420 servidores.

La ingeniera Martha Sánchez, Ph.D en derecho internacional del ciberespacio y docente de la Universidad Javeriana, quien analiza que, teniendo en cuenta que el atacante pidió una recompensa de 25.000 dólares, se puede considerar un secuestro que, de paso, pone en entredicho la seguridad cibernética con la que cuenta el Estado.

En ese sentido, páginas como el Dane deben añadir capacitaciones para que sus funcionarios aprendan a reconocer, “con claridad y a detalle”, qué tipo de malware, o programa malicioso, puede llegar a través de un enlace o una publicación. Según la experta, ese tipo de mensajes llegan en correos o mensajes que conocen detalles personales de sus víctimas. “Suelen ser supuestos procesos, multas o declaraciones de renta pendientes, por ejemplo. Entonces la persona da click por curiosidad o descarga el documento y, sin darse cuenta, da acceso al hacker”, detalla.

En todo caso, la relevancia de este “secuestro” va más allá de los datos que los hackers hayan podido recolectar. “Acá está en riesgo también la reputación de esa entidad y su seguridad cibernética ¿Qué podemos esperar como ciudadanos si nuestros datos no están seguros?”, concluyó Sánchez.[63]”

Los principales ataques están relacionados con phishing, filtración de datos personales, ransomware. Según la calificación de las denuncias recibidas en primer lugar se encuentra el delito de violación de datos personales, en segundo lugar, se tiene la suplantación de sitios web, en tercer lugar, se tiene el acceso abusivo a sistemas informáticos y en cuarto lugar el secuestro de datos o ransomware[64].

Las modalidades más usadas para estos ataques sigue siendo a través de correos electrónicos masivos con técnicas de phishing enviados a cuentas personales y

[63] EL COLOMBIANO. El cibersecuestro de datos que tiene en jaque al Dane. [Sitio web]. Colombia. [17 de noviembre de 2021]. Disponible en https://www.elcolombiano.com/colombia/secuestro-a-informacion-del-dane-en-colombia-IE16031966

[64] CCIT. Evaluacion, retos y amenazas a la Ciberseguridad. [Sitio web]. [2021]. P.18. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

corporativas; muchos de estos contienen enlaces para redireccionar la victima a páginas web fraudulentas con el objetivo de recolectar datos personales y de esta forma acceder a información para actividades de suplantación y robo de identidad.

Algunas de las entidades del gobierno han logrado ser suplantadas con estos fines ya que estas páginas pueden generar mayor confianza, por ejemplo, paginas asociadas al programa de del Gobierno Nacional “Ingreso Solidario” han resultado ser falsas con formularios creados para el robo de información.

Figura 6. Imagen página falsa

Fuente: PROSPERIDAD SOCIAL. ¡Cuidado! Falsas páginas prometen inscripción a programa Ingreso Solidario. [Sitio web]. Colombia. [2021]. Disponible en: https://prosperidadsocial.gov.co/Noticias/cuidado-falsas-paginas-prometen-inscripcion-a-programa-ingreso-solidario/

Los enlaces maliciosos siguen siendo empleados para infectar sistemas aprovechando vulnerabilidades de fallas de seguridad, aplicaciones y sistemas operativos desactualizados.

El temas de transformación digital y el incremento de tramites a través de canales virtuales ha provocado un enfoque por parte de la delincuencias hacia nuevos objetivos, una nueva modalidad identificada está dirigida a infectar los botones de pago electrónico en los portales comerciales, explotando vulnerabilidades en la fase de desarrollo de estos canales.

Según datos de FortiGuard durante el año 2021 en Colombia se ha logrado detectar cerca de 80000 exploits, que se utilizan para ingresar a los sistemas de información y materializar amenazas como el ransomware. La mayor parte de exploits por

vulnerabilidades informadas están enfocadas al lenguaje programación PHP uno de los más usados en el país[65].

"Estos se vuelven parte de las herramientas usadas por atacantes dentro de sus técnicas y tácticas para conseguir acceder a sistemas que luego se convierten en la materialización de las amenazas como el ransomware o malware persistente que es aprovechado en situaciones críticas como la pandemia u otros, teniendo como resultados pérdidas de dinero, golpes de opinión y en algunos casos críticos impactos a nivel de ciudades o países."[66]:

Los exploits más comunes durante el primer trimestre del 2021 en Colombia son los siguientes:

Tabla 4. Exploits más comunes en Colombia

Conteo total Exploit: 79.822	**% Global Exploit 1.68%**
PHPUnit.Eval-stdin.PHP.Remote.Code.Exe	40.13%
ThinkPHP.Controller.Parameter.Remote.Co	40.09%
NETGEAR.DGN1000.CGI.Unauthenticated	39.19%
Dasan.GPON.Remote.Code.Execution	38.56%
D-Link.Devices.HNAP.SOAPAction-Header	37.17%
PHP.CGI.Argument.Injection	35.71%
PHP.Diescan	35.4%
Drupal.Core.Form.Rendering.Component.R	34.29%
vBulletin.Routestring.widgetConfig.Remote	33.98%
ThinkPHP.Request.Mehot.Remote.Code.E	33.94%

Fuente: [1] CCIT. Evaluacion, retos y amenazas a la Ciberseguridad. [Sitio web]. [2021]. P.29. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

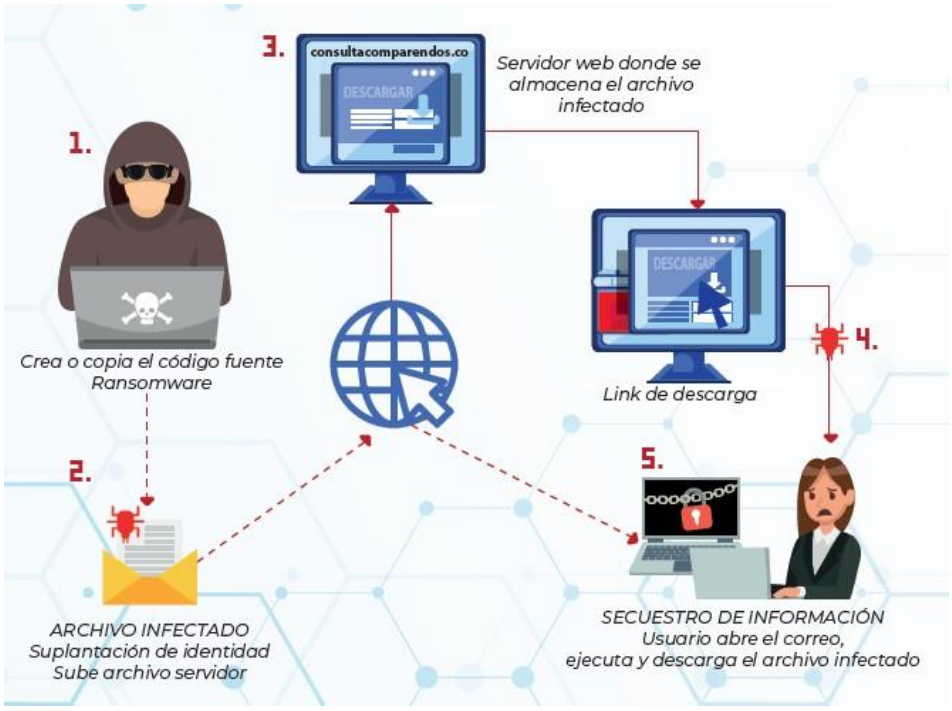
Dada la gran cantidad de amenazas a las que se encuentran expuestas las organizaciones , y teniendo en cuenta las preocupaciones existentes, es importante identificar los principales vectores por los que se materializan estos incidentes, y así tomar las medidas adecuadas para salvaguardar la información; por ejemplo un gran número de incidentes en el último año fueron ejecutados a través de ingeniería

[65] CCIT. Evaluacion, retos y amenazas a la Ciberseguridad. [Sitio web]. [2021]. P.29. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf
[66] Ibid.

social, haciendo uso de campañas por medio de correo electrónico, mensajería SMS y WhatsApp.

“Los vectores utilizados por los cibercriminales apuntan generalmente al envío masivo de correos electrónicos con llamativos y alarmantes asuntos que consiguen en un porcentaje muy alto que las víctimas den clic sobre los enlaces incluidos en los mensajes que notifican. El principal medio de propagación del Ransomware de tipo Lockscreen (caracterizado por impedir el acceso y el uso del equipo mediante una pantalla de bloqueo), sigue siendo el correo electrónico, puesto que una vez engañado el usuario es dirigido a un servidor para descargar el malware. Una vez ejecutado el archivo infectado, esta cifra la información, evitando cualquier acción por parte de diferentes sistemas de seguridad como antivirus, Sandbox, firewall, para exigir una posterior suma de dinero a cambio de posiblemente restablecerla. ”[67].

Figura 7. Ilustración forma de ejecución del ataque ransomware.



[67] Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia [29 de octubre de 2019]. P.13. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Fuente: Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia [29 de octubre de 2019]. P.13. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Uno de los principales riesgos es que en la actualidad muchas personas manejan información de las empresas a través de los dispositivos móviles, y un hecho aún más preocupante es que la mayoría de estos dispositivos no cuentan con soluciones de seguridad.

También es importante mencionar que estas técnicas de ingeniería social van en constante proceso de evolución para aumentar la efectividad, por ejemplo, los piratas informáticos han logrado utilizar certificados SSL falsos haciendo creer que los sitios que ponen como trampa, son sitios seguros por que han incorporado el protocolo https, pudiendo suplantar incluso a empresas reconocidas.

7 PRINCIPALES VULNERABILIDADES Y RIESGOS INFORMÁTICOS PRESENTES EN LAS INFRAESTRUCTURAS TECNOLÓGICAS.

Uno de los grandes problemas a nivel de ciberseguridad que se está afrontando en la actualidad, es el incremento de casos de ataques cibernéticos a las organizaciones, este tema le está costando millones de dólares al mundo empresarial, e incluso se ha estado viendo afectado la continuidad de negocio; muchos de estos ataques se realizan mediante la explotación de vulnerabilidades, estas vulnerabilidades se pueden encontrar en el sistema operativo, software de aplicación, debilidad de hardware, configuraciones inadecuadas, uso incorrecto de los usuarios, debilidad en la infraestructura tecnológica, y falta de políticas de seguridad.

Un factor que incidió de forma extraordinaria en los últimos años sobre la vulnerabilidad de las empresas, fue la aparición del COVID-19, lo que condujo a operaciones de teletrabajo y uso masivo de plataformas digitales para intercambio información, lo cual no estaba integrado en los planes se seguridad de la información o planes de contingencia, y en efecto un gran número de personas generó muchas vulnerabilidades, siendo así una preocupación adicional considerando el riesgo de ataques de ingeniería social que puede comprometer la continuidad de las operaciones. Según una encueta realizada por la compañía ESET SECURITY, durante los últimos meses del año 2020 casi el 45% de usuarios encuestados recibió intentos de Phishing relacionados a actividades derivadas de la pandemia, y más del 50% aseguró que no recibieron herramientas de seguridad para migrar hacia el teletrabajo[68]. Este nuevo escenario laboral sumó grandes retos a las empresas, toda vez que se ha extendido considerablemente el perímetro a proteger.

“El desafío de asegurar y proteger datos y puntos finales no es un requisito nuevo, pero en la actualidad es más importante que nunca. Con una superficie de ataque en rápida expansión producto de la proliferación de nuevos tipos de puntos finales, que van desde dispositivos móviles a la Internet de las cosas (IoT), sumado a la ola de trabajadores remotos alrededor del mundo, se ha creado una tormenta perfecta.[69]”

Las vulnerabilidades son el resultado de fallas en el diseño del software, firmware y hardware, e incluso configuraciones incorrectas en los sistemas, que ha traído

[68] ESET. SECURITY REPORT. LATINOAMÉRICA 2020. [Sitio web]. España. [2020]. P.30. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

[69] BlackBerry Cyber Suite. Resumen de la solución. Cómo acortar la distancia entre Zero Trust y Zero Touch. 2020. p.2.

consecuencias desastrosas en múltiples activos de información a nivel general; estas vulnerabilidades constituyen un tipo especial de riesgo y las organizaciones requieren medios técnicos para evitarlas o eliminarlas ya que un atacante puede explotarlas para acceder a los sistemas de información con fines maliciosos.

Actualmente hay empresas de ciberseguridad que se están especializando en crear componentes de software para afrontar este tipo de ataques.

"Los componentes del paquete BlackBerry Cyber Suite trabajan en conjunto para proporcionar las bases para una arquitectura de seguridad empresarial de Confianza cero.
BlackBerry® Protect utiliza un enfoque automatizado que prioriza la prevención para detener al malware y evitar que se ejecute en los puntos finales de una organización. Previene las filtraciones como el ransomware polimorfo, los ataques de día cero y otros tipos de malware, e incluye las salvaguardas que protegen contra ataques basados en scripts, sin archivos, de memoria y basados en dispositivos externos. BlackBerry Protect logra todo esto sin intervención del administrador o los usuarios, una conexión a la nube, firmas, heurísticos o sandboxes"[70].

Es importante hacer uso de VPN, "los principales motivos para usar una VPN, es que nos permite establecer comunicaciones seguras, con autenticación y cifrado de datos para proteger toda la información intercambiada. IPsec es uno de los protocolos de seguridad más importantes, el cual proporciona una capa de seguridad a todas las comunicaciones IP entre dos o más participantes"[71].

Es recomendable el uso de firewall, "los firewalls son una herramienta fundamental para proteger adecuadamente tanto nuestros PC, el router y toda la red de intrusiones externas. Los firewalls nos permitirán controlar el tráfico desde y hacia un destino, incorporando diferentes reglas"[72].

Frecuentemente se producen ataques contra sistemas informáticos que tienen gran impacto en la práctica de seguridad, aquí es importante identificar la capacidad que tiene la empresa para afrontar el riesgo, controlarlo y estar preparadas para futuros e impredecibles ataques.

---

[70] BLACKBERRY CYBER SUITE. Resumen de la solución. *Cómo acortar la distancia entre Zero Trust y Zero Touch*. 2020. p.7.

[71] RedZone. Mejora la seguridad de tu VPN con el protocolo IPsec. [Sitio web]. [2021]. Disponible en: https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/

[72] Redeszone.net/. [Sitio Web]. Mejores prácticas para configurar cualquier firewall en cualquier sistema. [Consulta 11 septiembre 2021]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/configurar-firewall-mejores-practicas/

El ransomware es uno de los problemas más peligrosos para las empresas, aunque su alcance no es bien interpretado lo que lleva a prácticas de precaución inadecuadas, permitiendo ataques que pueden implicar en los sistemas informáticos instrucciones maliciosas tales como: Penetración en la red, robo de credenciales para cuentas críticas, ataques a la consola de administración de copias de seguridad, y robo de datos.

Las infiltraciones de esta naturaleza se han vuelto muy frecuentes, el ransomware se implementa para cifrar datos críticos, incluido el almacén de copias de seguridad, si es accesible en la red. Es posible que la recuperación total no se logre en absoluto.

La ingeniería social y la explotación de vulnerabilidades han sido los principales vectores que utilizan los piratas informáticos para comprometer los activos y servicios de las empresas, la tercera parte de los delitos que aprovechan vulnerabilidades usan agujeros en el protocolo de comunicación SMB, de la misma forma en que actúan con otras clases de malware los delincuentes utilizan estas vías para infectar los equipos.

Las principales vulnerabilidades que se encuentran en las empresas y que son aprovechadas por los ciberdelincuentes son las siguientes:

1. Falta de políticas de seguridad: muchas de las empresas aun no cuentan con lineamiento de políticas de seguridad, plan de gestión de riesgos ni plan de contingencia, este es uno de los problemas más comunes a nivel de ciberseguridad toda vez que las personas no se encuentran preparadas para salvaguardar la información y mucho menos para afrontar un evento de ataque cibernético.

2. Falta de capacitación: es muy importante socializar y capacitar el personal de las empresas sobre temas de ciberseguridad, de esta forma se va entrenando el talento humano sobre buenas prácticas y se va creando conciencia del significado que tienen los activos informáticos para la continuidad de negocio de la empresa. Muchas empresas no brindan capacitaciones sobre el manejo seguro información y documentos empresariales en la modalidad de trabajo a distancia.

3. Errores humanos: ya sea por negligencia o falta de capacitación, el talento humano ocupa un rol importante en el conjunto de vulnerabilidades que se encuentran en las empresas, el custodio y la gestión de la información es responsabilidad de cada usuario, cada persona debe tener cuidado con dar cumplimiento a prácticas de seguridad como uso debido del escritorio, cierre de sesión y apagado del equipo cuando se ausente del puesto de trabajo, uso debido de las cuentas institucionales, uso debido del servicio de internet, gestión y privacidad de contraseñas. Debido a que

muchas de estas prácticas no se realizan con responsabilidad se van creando puertas de acceso que los delincuentes pueden aprovechar.

4. Gestión de contraseñas: las cuentas institucionales y personales deben ser protegidas con contraseñas robustas estas deben cumplir con políticas de seguridad y no ser reveladas a terceros, sino se cumple con esto se están creando vulnerabilidades.

5. Correo electrónico: el servicio de correo electrónico es uno de los canales más usados por los delincuentes para realizar ataques cibernéticos, es por eso que dentro de las políticas de seguridad se debe incluir el uso correcto de este medio de comunicación y sobre todo estar entrenado constantemente al talento humano sobre estas políticas.

6. Redes sociales: en la actualidad es muy común el uso de redes sociales como canales de comunicación en los entornos laborales, por ejemplo, en el escritorio de los ordenadores el servicio de mensajería como Whats app web y Telegram juegan un papel importante por la agilidad en la comunicación y envío de archivos, lo cual se constituye en una amenaza frecuente para infiltración de malware. Por otra parte, con relación a conocimiento sobre ciberseguridad, el 58 % de personas encuestadas desconoce cuándo los mensajes por WhatsApp son seguros. Del mismo modo, tan solo el 36 % reconoce correos electrónicos fraudulentos, el 64 % desconoce la forma de proteger sus datos en redes sociales. Gran parte de los empleados comparten documentos de las organizaciones por WhatsApp e incluso, contraseñas internas por este medio y por correo electrónico desprevenidamente.

7. Dispositivos móviles: en la actualidad muchas personas manejan información de las empresas a través de los dispositivos móviles, y un hecho aún más preocupante es que la mayoría de estos dispositivos no cuentan con soluciones de seguridad.

8. Teletrabajo: en los últimos años se ha incrementado el sistema de teletrabajo y un gran número de personas ha generado muchas vulnerabilidades por falta de configuraciones como conexiones cifradas, tiempos de sesión y autenticación a nivel de usuario, conexiones de tipo VPN (Virtual Private Network).

9. Instalación de programas piratas: un factor que ha estado impulsando el ciberdelito. Se ha logrado identificar familias de malware que dejan en evidencia que los usuarios le abren la puerta a las ciber amenazas, que se materializan a través de programas piratas, entregando el control de los equipos a los ciberdelincuentes, por el hecho de utilizar programas piratas, no se reciben los parches de seguridad oficiales.

10. Configuración de los equipos: hay varios aspectos a tener en cuenta para reducir el riesgo de que los equipos lleguen a ser vulnerados, lo primero es contar con el sistema operativo y todo el conjunto de software licenciado y actualizado, esto incluye antivirus y aplicaciones, lo segundo es limitar los permisos administrador y quitar usuarios que no sean necesarios dentro del equipo. Si no se cumple con esto el equipo estará desprotegido.

11. Configuración de red: es importante contar con una buena administración de red, contar con herramientas de última tecnología y procesos de seguridad que garanticen la estabilidad de toda la infraestructura de red; la gran mayoría de ataque se han podido ejecutar por malos procedimiento en las configuraciones de red.

Las amenazas son situaciones potenciales que existen y tienen la posibilidad de afectar un activo, generando afectación en la operación de una organización. Es un hecho que las amenazas siempre han existido y son inherentes en cualquier entorno corporativo, lo cual ha sido una preocupación para gerentes de cualquier organización, sin embargo, la amenaza como tal no genera ningún impacto negativo sino se puede materializar y para que esto pase, es necesario aprovechar una brecha o debilidad en el sistema.

Basado en lo anterior, lo ideal es adoptar una cultura de prevención, anticipándose a hechos adversos que puedan dañar un activo. En el campo de la seguridad de la información, día a día, ocurren eventos con consecuencias negativas para los activos de la información, los cuales en su mayoría pueden ser prevenidos si se aplican las salvaguardas correctas en el momento indicado.

8 GUÍA DE BUENAS PRÁCTICAS CON MEDIDAS PREVENCIÓN Y MECANISMOS DE PROTECCIÓN CONTRA ATAQUES DE RANSOMWARE PARA LAS ORGANIZACIONES COLOMBIANAS.

Conocer la situación actual de las organizaciones frente al estado de su información, permite tener una idea más clara sobre las acciones que están implementando en materia de seguridad informática, que están realizando para proteger la infraestructura y que preocupaciones tienen.

Está claro que el proceso de transformación digital ha crecido en los últimos años, sobre todo a raíz de la pandemia, ya que para lograr seguir con los procesos surgió la necesidad de contar con medios alternativos basados en herramientas tecnológicas. Estas nuevas condiciones involucran la necesidad de incorporar mecanismos de protección como soluciones de seguridad y buenas prácticas en toda la infraestructura tecnológica. Adicionalmente surge la necesidad de revisar, mejorar y fortalecer las políticas de seguridad informática, plan de riesgo y plan de continuidad para minimizar el riesgo.

Es importante adoptar un conjunto de buenas prácticas para poder protegerse de ataques ransomware, con el objeto de evitar que los sistemas sean técnicamente vulnerables y conocer los métodos y técnicas de esta clase de ciberdelito para evitar ser víctimas del mismo[73].

Mas del 50% de ataques con ransomware se realizan a través de ingeniería social, de este modo los atacantes logran engañar a los usuarios para conseguir credenciales de acceso a los sistemas informáticos e instalar malware.

Es muy importante que dentro de las organizaciones se generen y se empleen estrategias de formación y concientización capacitando periódicamente al talento humano sobre como reconocer y cómo actuar frente a estas situaciones; además poner en prácticas las políticas de seguridad de la información por ejemplo las

[73] LAI, Yeu-Pong ; HSIA, Po-Lun. Using the vulnerability information of computer systems to improve the network security. *Computer communications*, 2007, Vol.30 (9), p.2032-2047. Disponible en: https://www-sciencedirect-com.bdigital.sena.edu.co/science/article/pii/S014036640700117X?via%3Dihub

relacionadas a el uso de dispositivos y aplicaciones, el uso debido de internet, contraseñas, puestos de trabajo entre muchas otras.

Es importante promover la educación a los usuarios sobre aspectos de ingeniería social, una gran cantidad de ataques son ejecutados mediante mensajería instantánea correos electrónicos que motivan a los usuarios a ejecutar ficheros o visitar sitios web maliciosos; la educación sobre ciberseguridad es la manera más eficaz de prevenir y manejar estas situaciones.

Para evitar ser víctimas de este tipo de fraude de deben seguir unas pautas:

No abrir mensajes de cuentas de correo desconocidas que no se hayan solicitado, se debe proceder a eliminar estos correos. Para evitar el ransomware mediante la práctica de ingeniería social lo primero que se debe hacer es no confiar en mensajes recibidos que indiquen ofertas, sanciones, desactivación de cuentas, uso indebido del correo de la cuenta, ya sea por correo, SMS o redes sociales[74].

El correo electrónico es uno de los canales de comunicación más empleados por los ciberdelincuentes para realizar ataques de ingeniería social y acceder a los servicios a través de engaño, de esta forma lograr instalar malware o inducir a visitas de sitios web maliciosos. Por tal razón se debe seguir unas medidas de prevención. Implementar filtros de spam para impedir que los mensajes ingresen directamente la bandeja de entrada, esta gestión se debe estar realizando periódicamente, de esta forma se reduce la posibilidad de abrir enlaces y ficheros adjuntos peligrosos. No abrir correos sospechosos o no deseados.

Escanear los correos con el fin de detectar posibles amenazas y tener configurada la vista de extensiones en el sistema operativo, esto último hace más fácil identificar programas potencialmente maliciosos como, por ejemplo .exe .vbs y .scr.
Desconfiar de los enlaces acortados, antes de abrirlos usar algún servicio para expandirlos.

Desconfiar de los ficheros adjuntos así provengan de cuentas conocidas. Utilizar contraseñas que cumplan las políticas de seguridad. Las contraseñas deben ser robustas y los sistemas de información deben contar con políticas de bloqueo

[74] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Ransomware una guía de preparación para el usuario. [Sitio web]. España. [2017]. P.10. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

después de una cantidad de intentos fallidos al sistema; también se puede considerar el uso de doble factor de autenticación para asegurarse que la persona que intenta ingresar al sistema es el propietario de la cuenta.

De igual forma se recomienda hacer uso de lista de control de acceso ACL con el fin de limitar el acceso a esta clase de servicios desde equipos de confianza.
Los delincuentes hacen uso de herramientas y scripts con diccionarios robustos para tratar de descifrar las credenciales de usuario[75].

Asegurarse que los usuarios no cuenten con permisos de administrador. Los privilegios de seguridad y grupos deben estar al mínimo, es decir solo dar los permisos que necesita cada usuario incluyendo acceso a la información e instalación de controladores y software; de esta forma se evita fuga de información y acceso servicios que los usuarios no requieren para el desarrollo de sus actividades. Esto reduce la posibilidad de que por error se instale malware en los equipos, los privilegios de administrador solo pueden ser utilizado por los administradores del área de sistemas. De esta forma a los atacantes se le dificulta realizar instalaciones y tener control total del equipo. Dar restricción a estos privilegios bloquea la ejecución de malware o limita la capacidad de propagación en red.

También es importante deshabilitar las cuentas de usuarios que no se requieren y eliminar las cuentas de usuarios que ya no pertenezcan a la empresa, con esto se disminuye las fuentes de acceso a la red y los sistemas de información. Adicionalmente es recomendable deshabilitar el protocolo de accesos remoto a los sistemas que no se estén usando. Una gran cantidad de ataques ransomware se producen mediante el uso de escritorio remoto.

Para minimizar el riesgo de caer en un ciberataque además de llevar a cabo las medidas concienciación se deben adoptar procedimientos técnicos al interior de las empresas, esto con el propósito que los sistemas no tengan agujeros de seguridad y mantenerlos bien configurados y actualizados. También se debe asegurar la red para evitar exponer los servicios internos al exterior, en lo posible asegurarse que la información y la red interna no quede expuesta al exterior, en tal caso es una buena práctica separar los servidores privados de la organización, de los servidores

[75] CN-CERT. Informe de Amenazas. Medidas de seguridad contra ransomware. España. [2017]

accesibles desde el exterior por ejemplo aquellos a través de los cuales se ofrecen servicios por internet.

Para lograr esta segmentación de servicios y evitar que las redes queden desprotegidas se implementa el uso de cortafuegos con el fin de administrar los permisos y bloqueos de conexiones de entrada y salida de la red[76].
Adicional a esto para evitar alguna brecha de seguridad es recomendable implementar una configuración de red desmilitarizada (DMZ), es decir una red aislada de la red interna para ubicar los servidores de acceso a través de internet. De esta manera en caso de presentarse un ataque gran parte de la red quedará protegida[77].

En este sentido dentro de una zona de red desmilitarizada se podrían incluir servidores DNS, servidores VPN, servidores de correo y web mail.

Deshabilitar el HTML en las cuentas de correo ya que los ciberdelincuentes pueden hacer uso de código en JavaScript que terminan redirigiendo al usuario a sitios web maliciosos.

Se recomienda utilizar bloqueadores de JavaScript para el navegador, de tal forma que eviten la ejecución de los scripts que han sido creados para infectar los ordenadores. De esta forma se reduce las posibilidades de infección desde la web. Deshabilitar las macros de archivos adjuntos ya que en caso de una infección si se abre el documento adjunto y se habilita la macro se ejecuta el malware.

Hacer uso de soluciones de seguridad de confianza, aunque no todos ataques ransomware son detectados por los antivirus convencionales, aun así, hay soluciones que tienen la capacidad de bloquear un buen número de las familias de ransomware conocidas.

[76] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Ransomware una guía de preparación para el usuario. [Sitio web]. España. [2017]. P.14. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf
[77] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Ransomware una guía de preparación para el usuario. [Sitio web]. España. [2017]. P.15. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

Consultar noticias de ciberseguridad crea alertas para estar más prevenidos y conocer el funcionamiento de nuevos métodos y herramientas de que se están usando en estas prácticas delictivas.

Considerar guardar información sensible de forma cifrada a nivel de usuario.
Todo el conjunto de software debe mantenerse actualizado con los últimos parches, mantener los sistemas actualizados disminuye puntos de entrada de explotación dispuestos para el atacante, dado el caso que los sistemas desactualizados crean vulnerabilidades que son explotadas en el desarrollo de estas técnicas.

Es importante instalar software con licencia, muchos de los activadores gratuitos que se encuentran en la internet contienen malware que puede terminar vulnerando equipos de cómputo.

Mantener copias de seguridad de toda la información importante y guardarlas de forma aislada y sin conectividad con otros sistemas para evitar el contacto con equipos infectados.

Realizar las copias de seguridad es la medida más segura y efectiva para la recuperación continuidad de negocio en caso de ser víctima de ransomware, se aconseja tener como respaldo dos copias de seguridad todo el tiempo, toda vez que el back up también puede presentar fallas al momento de la restauración. Estas copias de respaldo se deben almacenar en sitios apartados de los servidores dado que el ransomware puede cifrar datos en las unidades de almacenamiento y equipos en red, lo más seguro es guardar las copias de seguridad en equipos no conectados en red o unidades de almacenamiento externo con DVD o discos extraíbles con previo custodio[78].

Hay que tener un protocolo bien definido sobre la restauración de copias de seguridad y comprobar que estas funcionen ya que también pueden corromperse.
Hacer uso de redes privadas preferiblemente ya que el tráfico es cifrado por este tipo de redes lo cual dificulta que los atacantes accedan, de esta forma podemos tener acceso a la información de los equipos de cómputo o intranet desde lugares distantes de la empresa, pero navegando de forma segura.

[78] CN-CERT. Informe de Amenazas. Medidas de seguridad contra ransomware. España. [2017]

Abstenerse de ingresar a páginas de contenido dudoso toda vez que estos sitios web pueden esconder exploit kits con el objeto de buscar vulnerabilidades y los navegadores de internet, que pueden ser aprovechadas para instalar malware en los equipos de cómputo, además hay que tener actualizados los navegadores de internet .

Verifique si el nombre de dominio en la URL coincide con el nombre de la Web, si tiene certificado de seguridad HTTPS y signos de conexión segura (icono de candado).

No introducir memorias USB o algún otro dispositivo de almacenamiento si desconoce la procedencia, estos dispositivos pueden contener malware que se activa con solo conectarse a los equipos de cómputo.

Teniendo en cuenta que estos ataques están dirigidos a los activos de información es fundamental asegurar las plataformas de copias de seguridad como parte del plan de contingencia; con respecto a esto hay proveedores de copias de seguridad que se están enfocando principalmente en tres áreas: Detención de ataques, protección del sistema de copias de seguridad, y recuperación de ataques.

El sistema de copias de seguridad está centrado en la detención de ataques de forma temprana, minimizando las probabilidades de activación del software malicioso, debido a que este tipo de sistemas es atacado con bastante frecuencia, la protección de todos sus componentes es fundamental para una recuperación exitosa. Aun así, este proceso puede ser complejo y tardar mucho tiempo.

La detección temprana de ataques es la principal línea de defensa, sin embargo, la mayoría de organizaciones realizan esta actividad a través de antivirus y software antimalware instalados en los equipos de cómputo y servidores de la entidad, aun así, depender únicamente de estas herramientas no es suficiente para protegerse contra el ransomware.

En todo caso es necesario activar mecanismos de defensa y prevención al interior de las organizaciones tales como restringir protocolos de uso compartido de red, aunque los protocolos de intercambio de redes, como el sistema de archivos de red (Network File System, NFS) y el sistema de archivos de Internet común (Common Internet File System, CIFS), son muy usados y se han empleado por muchos años para el intercambio de información, estos carecen se seguridad y crean vulnerabilidades al interior de la red que pueden exponer los datos, toda vez que

permiten que muchos equipos de cómputo puedan acceder a información confidencial y copias de seguridad lo cual puede exponer todo el sistema a un potencial ataque cibernético. En cambio, se puede hacer uso de métodos más seguros como plataformas de almacenamiento de datos con sus propia API de movimiento de datos.

Adicionalmente a todas las medidas preventivas de protección contra el ransomware se recomienda realizar un plan de respuesta a incidentes que contenga cuatro fases: 1) Preparación, 2) Detención y análisis, 3) Contención resolución, recuperación y 4) Acciones posteriores al cierre.

El plan debe identificar los siguientes factores:

En la fase de preparación definir los responsables de gestionar y coordinar el manejo de los incidentes dentro de la empresa, definir los protocolos de documentación necesaria sobre los sistemas y redes de las organizaciones, identificar la ruta a seguir, recopilar los datos de contacto de los actores involucrados y autoridades competentes[79].

En la fase de detención y análisis se debe estudiar el incidente, contar con una guía actualizada de clasificación para determinar si efectivamente se trata de ransomware; en esta fase se debe escalar el caso a un nivel más avanzado para poder tratar el evento con ayuda de expertos en el área.

En la fase de contención, resolución y recuperación se realizan varas acciones:

a. Poner los equipos infectados en aislamiento.
b. Clonar los discos duros de estos equipos.
c. Denunciar el incidente ante las autoridades competentes.
d. Realizar el cambio de las contraseñas de las redes y cuentas.
e. Desinfectar los equipos y tratar de restaurar los datos cifrados.
f. Antes de restaurar una copia de seguridad, verifica que no está infectada.
g. Reconecta los dispositivos a la red.

En la fase de acciones posteriores al cierre

[79] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Ransomware una guía de preparación para el usuario. [Sitio web]. España. [2017]. P.17. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

Tomar un registro detallado de todo el evento con el propósito de identificar mejoras en caso de repetirse otro incidente similar.

En caso de presentarse un ataque por ransomware prácticamente existen tres posibilidades: restaurar desde una copia de respaldo, pagar por el rescate de la información, o asimilar la perdida de información; en este sentido lo mejor que puede suceder es que se cuente con la copia de seguridad para poder restablecerse. En ningún caso se recomienda realizar el pago por el rescate de la información por varias razones, la primera es que no hay garantía de que en realidad se recupere esta información, la segunda es que los delincuentes pueden seguir la extorsión sabiendo que la empresa está dispuesta a pagar, y la tercera es que realizar un pago por extorsión es motivar a que los delincuentes sigan realizando ese tipo de actividad.

En estos casos lo mejor es activar la ruta del plan de respuesta a incidentes, si se cuenta con el respaldo de la información se procede a restablecer todo el sistema afectado, y realizar el reporte a las autoridades competentes.

La información es uno de los activos más importantes de una empresa, y para salvaguardarla y protegerla de este tipo de incidentes lo mejor que se puede hacer es aplicar todas las medidas de prevención y protección y sobre todo estar respaldando la información de forma continua.

9 CONCLUSIONES

El ransomware tiene múltiples variantes con el mismo modo de operación basado en técnicas de criptografía, donde se crean llaves de cifrado mediante logaritmos RSA y AES, estas variantes se adaptan a los distintos tipos de sistemas y dispositivos informáticos, como por ejemplo el tipo de sistema operativo, tipo de equipo (IoT, móvil, servidores, ordenadores, entre otros), pero el objetivo es el mismo, lograr el secuestro de datos con la finalidad de cobrar cierta cantidad de dinero por el rescate de esta.

Muchos de los antivirus convencionales no logran detectar este tipo de ataque, de hecho, no existe ningún componente físico ni lógico que logre eliminar el ransomware, la única forma de restablecer la información es con la llave privada del cifrado, aun así, hay empresas de ciberseguridad que se están especializando en crear componentes de software para afrontar este tipo de ataques.

En Colombia se presentan 87 intentos de ataques por minuto, en el ultimo año el 19% de las empresas fueron afectadas por ransomware, un ataque de este tipo le puede costar a una empresa entre 300 y 5000 millones de pesos.

En Colombia, el 83% de las organizaciones no cuentan con protocolos de respuesta a incidentes de seguridad.

La mayor parte de vulnerabilidades se encuentran en los sistemas operativos, software de aplicación, debilidad de hardware, configuraciones inadecuadas, uso incorrecto de los usuarios, debilidad en la infraestructura tecnológica, y falta de políticas de seguridad.

El modo de ataque más usado es el método de phishing, a través de correos electrónicos y redes sociales.

La mejor forma de evitar el ataque es la prevención, capacitaciones, aplicación de controles, monitoreo del panorama de amenazas.

Los ataques de ransomware han estado causando grandes afectaciones a los sistemas informáticos de las organizaciones colombianas, el incremento de esta práctica delictiva se debe a varios factores, entre los cuales se pueden identificar la

falta de conocimiento y la poca importancia que se le ha venido dando al tema ya que es considerado por muchas empresas como un riesgo mínimo; en todo caso este es un problema que va en crecimiento y en general le está costando mucho al mundo empresarial, por eso es el momento de buscar mecanismos para sensibilizar a las organizaciones de crear políticas de seguridad informática y control del riesgo, fortalecer la infraestructura tecnológica, y adoptar una cultura de prevención, anticipándose a hechos adversos que puedan dañar los activos de información.

La transformación digital y el incremento masivo de nuevas tecnologías, ha provocado cambios en la vida de las personas, el sistema empresarial y el desarrollo de distintas actividades como el trabajo, estudio, reuniones sociales, proceso médicos, procesos bancarios, compras entre muchas más; todo parece que al menos la mitad de los asuntos personales y empresariales se estarán gestionando a través de entorno virtuales, y que aunque la pandemia impulsó de forma acelerada esta tendencia, esta nueva normalidad ha llegado para quedarse. Así como va en crecimiento la revolución digital y que ha traído beneficios para el desarrollo del país, también ha crecido de forma desproporcionada las modalidades de delitos informáticos, que aprovechan vulnerabilidades presentes en las empresas para formar negocio a través del cibercrimen organizado. Lo que se ha vuelto una de las mayores preocupaciones y grandes problemas a nivel de ciberseguridad.

El ransomware es un delito que le está costando mucho al mundo empresarial lo que significa que es urgente tomar medidas como implementar políticas de seguridad y protocolos de respuesta a incidentes de ciberseguridad de lo contrario las empresas seguirán expuestas a la perdida parcial o total de negocio.

10 RECOMENDACIONES

Las amenazas están presentes diariamente en cualquiera de los aspectos del área informática por esto es recomendable llevar a cabo un plan de políticas de seguridad y tratamiento de riesgos que conlleve a estar preparados para afrontar cualquier anomalía presente, y tomar decisiones rápidas y efectivas según sea el caso requerido para dar solución oportuna a los problemas generados.

A todos los funcionarios, empleados, contratistas y terceras personas de la entidad u organización, se les debe proporcionar un nivel adecuado de concienciación, educación y capacitación en procedimientos de seguridad, especialmente en el correcto uso de los medios disponibles para el procesamiento de la información con fin de minimizar los riesgos posibles en la seguridad de la información.

Todos los funcionarios, empleados de la entidad u organización, en donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Estar monitoreando el panorama de amenazas continuamente y activar mecanismos de defensa y prevención al interior de las organizaciones tales como restringir protocolos de uso compartido de red.

Mantener copias de seguridad de toda la información importante y guardarlas de forma aislada y sin conectividad con otros sistemas para evitar el contacto con equipos infectados.

Promover la educación a los usuarios sobre aspectos de ingeniería social, una gran cantidad de ataques son ejecutados mediante mensajería instantánea correos electrónicos que motivan a los usuarios a ejecutar ficheros o visitar sitios web maliciosos; la educación sobre ciberseguridad es la manera más eficaz de prevenir y manejar estas situaciones.

11 BIBLIOGRAFÍA

A. Atapour-Abarghouei, S. Bonner, and A. S. McGough. 2019. Volenti non fit injuria: Ransomware and its Victims.
In 2019 IEEE International Conference on Big Data (Big Data). 4701–4707.

A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. [2022]. Disponible en: https://arxiv.org/pdf/2102.06249.pdf

ALCALDÍA DE BOGOTÁ. [Sitio web]. Régimen legal de Bogotá D.C. Ley 1273 de 2009 Nivel Nacional. Bogotá. [23 de enero 5 de 2009]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

BLACKBERRY. Perspectivas sobre la seguridad cibernética. *Informe de amenazas 2021.* 2021. P.53. Disponible en: https://www.blackberry.com/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report-sp.pdf

BLACKBERRY CYBER SUITE. Resumen de la solución. *Cómo acortar la distancia entre Zero Trust y Zero Touch*. 2020. p.7.

Cámara Colombiana de Informática y Telecomunicaciones. [Sitio web]. El TicTac presenta su informe: Tendencias del Cibercrimen en Colombia; primer trimestre de 2020. Colombia. [2020]. Disponible en: https://www.ccit.org.co/estudios/el-tictac-presenta-el-informe-de-tendencias-del-cibercrimen-en-colombia-primer-trimestre-de-2020/

CCIT. [Sitio web]. Evaluacion, retos y amenazas a la Ciberseguridad. [2021]. P.62. Disponible en: https://www.ccit.org.co/wp-content/uploads/diagramacion-estudio-safe-evaluacion-retos-y-amenazas-a-la-ciberseguridad.pdf

CN-CERT. Informe de Amenazas. Medidas de seguridad contra ransomware. España. [2017]. P.28. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1974-ccn-cert-ia-03-17-medidas-seguridad-ransomware-1/file.html

Criptografía clásica y moderna. Miguel García, Roberto . Disponible en: https://elibro-net.bdigital.sena.edu.co/es/ereader/senavirtual/102985?page=72

DATA CENTER MARKET. [Sitio web]. El ransomware se multiplica por diez en el último año y se centra en sectores críticos. [8 de septiembre de 2021]. Disponible en: https://www.datacentermarket.es/tendencias-tic/noticias/1128063032809/ransomware-se-multiplica-diez-ultimo-ano-y-se-centra-sectores-criticos.1.html

ENTER.CO. [Sitio web]. Siguen incrementando los ciberataques en Colombia. Colombia. [16 de septiembre de 2021]. Disponible en: https://www.enter.co/empresas/seguridad/siguen-incrementando-los-ciberataques-en-colombia/

ESET. [Sitio web]. Ransomware ¿Cómo protegerte? Conoce cómo evitar el secuestro de datos. España. Disponible en: https://www.eset.com/es/caracteristicas/ransomware/

ESET. SECURITY REPORT. LATINOAMÉRICA 2020. [Sitio web]. España. [2020]. P.30. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

EL COLOMBIANO. [Sitio web]. El cibersecuestro de datos que tiene en jaque al Dane. Colombia. [17 de noviembre de 2021]. Disponible en https://www.elcolombiano.com/colombia/secuestro-a-informacion-del-dane-en-colombia-IE16031966

D. Kao, S. Hsiao, and R. Tso. 2019. Analyzing WannaCry Ransomware Considering the Weapons and Exploits. In
2019 21st International Conference on Advanced Communication Technology (ICACT).

F. Tang, B. Ma, Jinku Li, F. Zhang, J. Su, and J. Ma. 2020. RansomSpector: An introspection-based approach to detect
crypto ransomware. Computers & Security 97 (2020).

Greene, Tim. Consortium helps define Web application firewalls. *Network world*, 2006, Vol.23 (3), p.20-20. Disponible en: https://www-proquest-

com.bdigital.sena.edu.co/docview/215973399?accountid=31491&pq-origsite=primo

HORNET SECURITY. [Sitio web]. Ransomware. ¿Qué es ransomware? ¿cómo protergerse? España. Disponible en: https://www.hornetsecurity.com/es/knowledge-base/ransomware/

Informe de las tendencias del cibercrimen en Colombia (2019-2020). [Sitio web]. Colombia [29 de octubre de 2019]. P.36. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD. . [Sitio web]. Ransomware una guía de preparación para el usuario España. [2017]. P.25. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

Jérôme Segura. 2020. WOOF locker: Unmasking the browser locker behind a stealthy tech support scam operation.
https://blog.malwarebytes.com/threat-analysis/2020/01/woof-locker-stealthy-browser-locker-tech-support-scam/

KASPERSKY. [Sitio web]. Comunicados de prensa. América Latina registra 5 mil ataques de ransomware por día. [14 de octubre de 2020]. Disponible en: https://latam.kaspersky.com/about/press-releases/2020_kaspersky-america-latina-registra-5-mil-ataques-de-ransomware-por-dia

KASPERSKY. [Sitio web]. Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [2021]. Disponible en: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

KASPERSKY. [Sitio web]. Identificación de ransomware: en qué se diferencian los troyanos de cifrado. Disponible en: https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

KASPERSKY. [Sitio web]. Ransomware: los ataques más resonantes de 2020. [2021]. Disponible en: https://latam.kaspersky.com/resource-center/threats/top-ransomware-2020

LAI, Yeu-Pong ; HSIA, Po-Lun. Using the vulnerability information of computer systems to improve the network security. *Computer communications*, 2007, Vol.30 (9), p.2032-2047. Disponible en: https://www-sciencedirect-com.bdigital.sena.edu.co/science/article/pii/S014036640700117X?via%3Dihub

LEMMOU, Yassine ; LANET, Jean-Louis y SOUIDI, El Mamoun. A behavioural in-depth analysis of ransomware infection. *IET information security*. 2021, Vol.15 (1), p.38-58. Disponible en: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ise2.12004

Lindsey O'Donnell. 2019. ThreatList: Top 5 Most Dangerous Attachment Types. https://threatpost.com/threatlist-top-5-most-dangerous-attachment-types/144635/

L. Štefanko R. Lipovský and G. Braniša. 2016. The Rise of Android Ransomware. http://www.neotericnetworks.com/wp-content/uploads/2016/11/Rise-of -Android-Ransomware.pdf

MANUAL DE POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN. Departamento Administrativo Para la Prosperidad Social. 2015. p.52.

PROSPERIDAD SOCIAL. [Sitio web]. ¡Cuidado! Falsas páginas prometen inscripción a programa Ingreso Solidario. Colombia. [2021]. Disponible en: https://prosperidadsocial.gov.co/Noticias/cuidado-falsas-paginas-prometen-inscripcion-a-programa-ingreso-solidario/

Redeszone.net/. [Sitio Web]. Mejora la seguridad de tu VPN con el protocolo IPsec. [Consulta 11 septiembre 2021]. Disponible en: https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/

Redeszone.net/. [Sitio Web]. Mejores prácticas para configurar cualquier firewall en cualquier sistema. [Consulta 11 septiembre 2021]. Disponible en: https://www.redeszone.net/tutoriales/seguridad/configurar-firewall-mejores-practicas/

S. Salehi, H. Shahriari, M. M. Ahmadian, and L. Tazik. 2018. A Novel Approach for Detecting DGA-based Ransomwares.
In 2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology
(ISCISC).

SEMANA. [Sitio web]. El 37 % de las empresas a nivel mundial fue atacado con ransomware en el último año. Colombia. [2021]. Disponible en: https://www.semana.com/economia/capsulas/articulo/el-37-de-las-empresas-a-nivel-mundial-fue-atacado-con-ransomware-en-el-ultimo-ano/202122/

SOPHOS. [Sitio web]. EL ESTADO DEL RANSOMWARE 2020.Resultado del studio independiente realizado a 5000 directores de TI en 26 países. [2020]. P.18. Disponible en: https://www.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

SOPHOS. [Sitio web]. EL ESTADO DEL RANSOMWARE 2021. [2021]. P.18. Disponible en: https://secure2.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-state-of-ransomware-2021-wp.pdf

Statista. 2019. Desktop OS market share 2013-2018 | Statista.
https://www.statista.com/statistics/218089/globalmarket-share-of-windows-7/. [Online; accessed 13-October-2020].
Symantec. 2015. The evolution of ransomware.
https://its.fsu.edu/sites/g/files/imported/storage/images/informationsecurity-and-privacy-office/the-evolution-of-ransomware.pdf. [Online; accessed 13-October-2020].

TrendMicro. [n.d.]. Command and Control Server.
https://www.trendmicro.com/vinfo/us/security/definition/commandand-control-server. [Online; accessed 13-October-2020].

VALORA ANALITIK. [Sitio web]. Actividad maliciosa en internet aumentó en un 150 % en Colombia durante aislamiento. Colombia. [2021]. Disponible en: https://www.valoraanalitik.com/2021/02/27/actividad-maliciosa-en-internet-aumento-un-150-durante-el-aislamiento/

VANGUARDIA. [Sitio web]. Tres de cada 10 víctimas de ‘ransomware’ en Colombia pagan el rescate. Colombia. [2021]. Disponible en: https://www.vanguardia.com/tecnologia/tres-de-cada-10-victimas-de-ransomware-en-colombia-pagan-el-rescate-CY3652307

WIRED. 2018. Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare. Disponible en: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/