ATAQUES DE RANSOMWARE MÁS RELEVANTES EN LOS ÚLTIMOS CINCO AÑOS QUE HAN AFECTADO A LAS ORGANIZACIONES COLOMBIANAS

ANGIE MILENA VIGOYA GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
AÑO 2024

ATAQUES DE RANSOMWARE MÁS RELEVANTES EN LOS ÚLTIMOS CINCO AÑOS QUE HAN AFECTADO A LAS ORGANIZACIONES COLOMBIANAS

ANGIE MILENA VIGOYA GONZÁLEZ

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

Christian Reynaldo Angulo Rivera
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
AÑO 2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., Fecha sustentación

DEDICATORIA

Con mucho amor dedico esta meta profesional a Dios quien ha sido mi guía y me ha dado la sabiduría para cumplir este logro profesional tan anhelado.

AGRADECIMIENTOS

Agradezco a mi hijo y a mis padres, quienes con su apoyo contribuyeron a mi interés y competencia para cursar el presente programa de formación.

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, en especial al Ingeniero Christian Reynaldo Angulo quien participó activamente en mi formación y me brindo todo el acompañamiento para cumplir a cabalidad este proceso de formación y lograr esta meta profesional.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

Pág.

GLOSARIO

Botnet: Es un grupo de equipos de cómputo de los cuales están controlados por un atacante cibernético de manera remota o a distancia con la finalidad de ejecutar ciberataques. También se conoce con el nombre de "red de computadoras zombie". Los delincuentes cibernéticos, por lo general, crean un Botnet en el que utilizan un malware que infecta un conjunto de computadoras de los cuales hacen parte de los botnet, y así lanzan los ciberataques en gran escala y para efectuar operaciones phishing. Botnet tiene tres etapas: Infección, expansión y ataque[1]

Cracker: Es un grupo de personas que tienen conocimientos informáticos su función es vulnerar los sistemas informáticos para acceder de manera ilícita. El propósito de esta banda criminal es realizar secuestro de la información como datos personales, tarjetas de crédito, datos financieros, credenciales de acceso a un sistema de información, con el objetivo de acceder a las cuentas bancarias robar el dinero de las víctimas, los crackers logran interrumpir un sistema hasta el punto de ocasionar un daño o destrucción de la infraestructura TI. También son llamados "Sombreros negros".[2]

Espionaje: Es una acción delictiva que consiste en acceder de manera ilícita a los sistemas informáticos de una entidad pública y privada, la forma de acceder es por medio de correos electrónicos engañosos. El propósito es acceder a la información de las organizaciones, con el propósito de divulgar la información e identifican las vulnerabilidades del sistema para atentar la seguridad de la infraestructura TI. [3]

Exploit: Es un software o una secuencia de comandos que se aprovecha de las vulnerabilidades o errores que puede llegar a presentar en un sistema, una red o equipo de cómputo. Este software puede lograr tener el control del sistema para así hurtar la data que está disponible en una red. Cuando se evidencia un error en un sistema los

---

[1] KASPERSKY. ¿Qué es un botnet?. [Sitio web]. [Consultado 13 de septiembre 2022]. Disponible en: https://www.kaspersky.es/blog/que-es-un-botnet/755/

[2] PROTECCIÓN DATOS. Cracker informático. ¿Es lo mismo que un hacker? [Sito web]. 2021. [Consultado 30 de agosto 2021]. Disponible en: https://protecciondatos-lopd.com/empresas/cracker-informatico/

[3] VALENCIA, Juliana. Legislación aplicable a las conductas delictivas en internet. [En línea]. 2020. [Consultado 31 de septiembre 2021]. Disponible en: http://bibliotecadigital.usbcali.edu.co/bitstream/10819/737/1/Legislacion_Aplicable_Conductas_Pena_2009.pdf

intrusos consiguen detectar las debilidades de un sistema con el objetivo de controlar e infectar la red y el sistema. [4]

Groming: Práctica utilizada actualmente donde una persona adulta logra obtener la confianza de un menor de edad con la finalidad de abusar y aprovechar la debilidad de ellos. Esta técnica se puede presentar principalmente a través de internet por medio de redes sociales, logrando una conexión emocional y lograr sacar provecho de la vulnerabilidad de los menores de edad. Esta modalidad de engaño logra obtener imágenes muy personales, es así, como el atacante utiliza esta conducta y logra convencer al menor de edad de acceder a sus peticiones impropias, para luego conseguir extorsionar a la víctima con el propósito de forzarlo a tener encuentros físicos. Esta modalidad de engaño está asociada a la pedofilia. [5]

Hacker: En la actualidad la tecnología ha tenido cambios grandes, uno de esos cambios puede ser positivos como negativos. La palabra hacker puede tener una connotación buena como mala, pero es importante tener en cuenta que depende del escenario como se tome la situación. En un "sentido Negativo", los hackers son grupos de personas que acceden de manera no autorizada a páginas web explorando las vulnerabilidades que existen en un sistema de información. Pero cuando hablamos de un "Sentido Positivo", los hackers es un grupo de profesionales en ciberseguridad que buscan detectar las vulnerabilidades de un sistema e identificar las débiles de las aplicaciones informáticas su finalidad es buscar soluciones a este tipo de situaciones para dar solución.[6]

Malware: Programa informático con intensiones malintesionadas de los cuales incluye virus, troyanos, ransomware, gusanos entre otros. Se utiliza como una herramienta de comunicación como el correo electrónico, dispositivos extraíbles y mensajes de texto, también se propaga en descargas engañosas, este software malicioso busca información confidencial, con el fin de acceder a ella para cometer delitos.[7]

Malware está diseña para ocasionar daños a los sistemas de información e infraestructura tecnológica, afectando en gran manera la seguridad de los dispositivos, aplicaciones,

---

[4] AVG. ¿Qué es un exploit en seguridad informática? [Sitio web]. 2022]. [Consultado 12 de septiembre 2022]. Disponible en: https://www.avg.com/es/signal/computer-security-exploits

[5] INCIBE. Grooming. [Sitio web]. 2022]. [Consultado 12 de septiembre 2022]. Disponible en: https://www.incibe.es/aprendeciberseguridad/grooming

[6] VIX. ¿Qué es un hacker? [Sito web]. 2021. Disponible en: https://www.vix.com/es/btg/tech/13182/que-es-un-hacker

[7] SIGNIFICADOS. Significado de Malware. [Sitio web]. 2019. [Consultado 31 de septiembre 2021] Disponible en: https://www.significados.com/malware/

software y equipos de cómputo de las compañías detectando las vulnerabilidades que existen en la infraestructura TI. [8]

Phishing: Método utilizado por los ciberatacantes su función es estafar o engañar a las víctimas para obtener información confidencial de manera fraudulenta, logran adquirir las contraseñas de las víctimas y así mismo acceden a las cuentas bancarias y tarjetas de crédito.[9]

Esta técnica ocurre cuando la víctima recibe mensajes de texto y correo electrónico, la victima procede a abrirlo, sin saber que el contenido es engañoso ya que se hace pasar por una persona u organización de confianza. Logrando que la víctima acceda se dirige al sitio web en el que se direcciona un sitio ilegitimo luego la victima ingresa las credenciales, contraseñas, información confidencial o datos personales, de esta manera el atacante obtiene la información privada. El objetivo del ciberdelincuente procede a acceder la información bancaria de la víctima. [10]

Ransomware: Software malicioso o malintencionado, su funcionalidad es restringir el acceso a determinadas rutas o archivos donde se encuentra información sensible de una organización. Esto con el fin de que los intrusos obtengan información para cobrar una recompensa económica a las víctimas y así realizar la recuperación de los datos.[11]

Esta es una de las técnicas más utilizadas para engañar a las victimas usando métodos, envió como correos electrónico y mensajes de textos de los cuales contienen enlaces y archivos engañoso y peligrosos. Cuando la víctima procede en acceder a la página web o descarga dicho archivo en el dispositivo o equipo de cómputo este se propaga en el sistema del equipo, archivos, imágenes, entre otros capturando y encriptando la información más relevante de la organización o víctima. Después de este proceso se arrojará un mensaje de alerta donde se indicará que la data ha sido secuestrada y para ello es necesario pagar un dinero y según el atacante cibernético devolverá la información

[8] HORNETSECURITY. ¿Qué es malware? ¿qué tipos de malware hay? [Sitio web]. 2022]. [Consultado 12 de septiembre 2022]. Disponible en: https://www.hornetsecurity.com/es/knowledge-base/malware/?_adin=02021864894

[9] MALWAREBYTES. ¿Qué es Phishing?. [Sitio web]. 2020. [Consultado 15 de septiembre 2022]. Disponible en: https://es.malwarebytes.com/phishing/

[10] MALWAREBYTES. Suplantación de identidad (phishing). [Sitio web]. 2020. [Consultado 15 de septiembre 2021]. Disponible en: https://es.malwarebytes.com/phishing/

[11] KASPERSKY. El ransomware: qué es, cómo se lo evita, cómo se elimina. [Sitio web]. 2021. [Consultado 15 de septiembre 2021]. Disponible en: https://latam.kaspersky.com/resource-center/threats/ransomware

de la víctima. Cabe aclarar, la mayoría de las veces la información no se logra recuperar a pesar de que la víctima realice el pago. [12]

Riesgo: En la actualidad existen acciones o actividades que realizan las personas que conllevan al uso de los servicios tecnológicos, herramientas, equipos de cómputo y con el acceso al internet y la conectividad de dispositivos. Esto abre una oportunidad para que se realicen actos negativos que afectan la funcionalidad de las organizaciones como el manejo de la información sensible, arquitectura TI y recursos tecnológicos. Todas estas situaciones que en el día a día se viven se presenta como un riesgo y crítico en cuanto al gremio de las compañías y la misma sociedad. Dado a esto, es importante identificar las vulnerabilidades existentes en los sistemas de información de las organizaciones y así mismo aplicar medidas de seguridad que logren mitigar los riesgos que se puedan presentar.[13]

Spyware: Denominado también como malware o programa malicioso espía, consiste en espiar los equipos de cómputo o red corporativa logrando tener acceso a información confidencial y personal. Se encarga de almacenar información el cual la víctima o usuario realiza con frecuencia, como por ejemplo el historial del navegador sobre las páginas web consultadas y eta información sea enviada por terceros sin que el usuario lo perciba. Un ejemplo las ventanas emergentes de los cuales se presentan algunas ofertas engañosas logrando así engañar a las víctimas y accedan a estos sitios web, logran capturar la información personal o privada del usuario.[14]

Vishing: Es un delito informático que consiste en engañar a las víctimas por medio de llamadas telefónicas, donde el atacante se hace pasar por una entidad confidencial o conocida, procede a solicitar los datos confidenciales de la víctima con el fin de infectar el dispositivo con un malware.[15] Esta modalidad de estafa consiste en usar números telefónicos fraudulentos, mensajes de texto y software de modificación de voz. Este tipo de ataque cibernético está relacionado con la ingeniería social en el que logra convencer a la víctima para que proporcione los datos personales.

---

[12] XATAKA. Qué es el Ransomware y cómo te puedes proteger de él. [Sitio web]. 2019. [Consultado 15 de septiembre 2022]. Disponible en: https://www.xataka.com/basics/que-ransomware-como-te-puedes-proteger

[13] GLOBALIMF. Riesgo, Amenazas y Vulnerabilidad conceptos claves de un ataque informático. [Sitio web]. 2021. [Consultado 06 de septiembre 2021]. Disponible en: https://globalimf.com.ec/openuide/blog/gestion-de-riesgos-informaticos/

[14] KASPERSKY. ¿Qué es el spyware? – Definición. [Sitio web]. 2022. [Consultado 15 de septiembre 2022]. Disponible en: https://latam.kaspersky.com/resource-center/threats/spyware

[15] WELIVESECURITY. Qué es el vishing: estafa a través de llamadas o mensajes de voz. [Sitio web]. 2021. Disponible en: https://www.welivesecurity.com/la-es/2021/05/03/que-es-vishing/

Vulnerabilidad: Es una debilidad dentro de un sistema de información, el cual permite al atacante exponer la integridad, confidencialidad y disponibilidad de la información o la infraestructura de una organización.[16] Existen varios tipos de vulnerabilidades de tipo de hardware, software, procedimentales o humanas.

WannaCry: Ataque cibernético que es usado por criptogusano este es dirigido al sistema operativo Windows se encarga de atacar los datos de la víctima y así logran ser cifrados, luego proceden a realizar el secuestro de la información. Después piden rescate de la información, y así obtiene un beneficio económico en el que debe ser pagado con la modalidad de criptomoneda Bitcoin. El objetivo es tomar de nuevo el acceso a los datos del dispositivo o equipo de cómputo.[17]

[16] INCIBE. Amenaza vs Vulnerabilidad [Sitio web]. 2020. [Consultado 16 de septiembre 2021]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarla s%20y%20eliminarlas%20lo

[17] WIKIPEDIA. Ataques ransomware WannaCry. [Sitio web]. 2021. [Consultado 16 de septiembre 2021] Disponible en: https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry

RESUMEN

La presente monografía se contextualiza el uso constante de la tecnología en todo el mundo. Y más aún con la situación presentada en el año 2020, con la llegada del covid19 desencadeno la identificación de ataques cibernéticos ransomware más peligrosos en el país que se convierten en una gran amenaza para las organizaciones colombianas. A raíz de esta situación se ha evidenciado ciertos aspectos importantes en las entidades colombianas que se vieron en la obligación de replantear y fortalecer mecanismos, procesos y disponer de infraestructuras tecnológicas adecuadas para cumplir con las necesidades de las compañías estatales y privadas con la finalidad de tener un buen uso de las tecnologías de la información. De acuerdo con lo anterior, se ha evidenciado por medio de investigaciones y noticias nacionales que se han informado el incremento de casos sobre los ataques cibernéticos que se presentaron desde el año de la pandemia hasta la fecha. Pero gracias a los avances tecnológicos se han hecho trasformaciones para el mejoramiento y detección de ataques cibernéticos. Es así, como las compañías colombianas protegen la data de acceso no autorizados y logren detectar intrusos en la red, aplicaciones, servicios e infraestructura de las compañías.

Existen ciertas situaciones en el mundo digital que vulneran y atacan las organizaciones con el fin de acceder a la información sensible de una entidad. Los ciberdelincuentes ejecutan algunos ataques cibernéticos para secuestrar u obtener datos importantes de las entidades colombianas con el objetivo de acceder a la información y la red corporativa logrando alterar todo el sistema ocasionando daños graves, poniendo en riesgo la confidencialidad, integridad y disponibilidad de la información. Estos atacantes cibernéticos utilizan herramientas especializadas como software malicioso, es decir ransomware o métodos de engaño que consiste en secuestrar información confidencial y sensible. Ransomware se propaga en el sistema luego detecta los archivos del sistema logrando acceder a ellos para bloquearlos y procede a solicitar un rescate para la recuperación de la data de las compañías colombianas. Por consiguiente, se pretende con esta presenta investigación realizar un análisis y estudio que permita identificar las falencias que tienen las organizaciones del gobierno colombiano y compañías privadas frente a este tipo de ataques cibernéticos que en la última década ha tomado bastante fuerza y se han identificado fallas en los procesos e implementaciones de cada compañía, logrando evitar fallas o secuestro de información.

Palabras claves: Ataque cibernético, Amenaza, Integridad, Ransomware, Secuestro de Información.

ABSTRACT

This monograph contextualizes the constant use of technology around the world. And even more so with the situation presented in 2020, with the arrival of covid19, it triggered the identification of the most dangerous ransomware cyber attacks in the country that become a great threat for Colombian organizations. As a result of this situation, certain important aspects have been evident in Colombian entities that were forced to rethink and strengthen mechanisms, processes and have adequate technological infrastructure to meet the needs of state and private companies in order to have good use of information technologies. In accordance with the above, it has been evidenced through investigations and national news that the increase in cases of cyber attacks that have occurred since the year of the pandemic to date has been reported. But thanks to technological advances, transformations have been made to improve and detect cyber attacks. This is how Colombian companies protect data from unauthorized access and manage to detect intruders in the company's network, applications, services and infrastructure.

There are certain situations in the digital world that violate and attack organizations in order to access the sensitive information of an entity. Cybercriminals carry out some cyberattacks to kidnap or obtain important data from Colombian entities with the aim of accessing information and the corporate network, managing to alter the entire system, causing serious damage, putting the confidentiality, integrity and availability of the information at risk. These cyber attackers use specialized tools such as malicious software, that is, ransomware, or deception methods that consist of hijacking confidential and sensitive information. Ransomware spreads in the system then detects the system files, gaining access to them to block them and proceeds to request a ransom to recover the data of the Colombian companies. Therefore, the aim of this research is to carry out an analysis and study that allows identifying the shortcomings that Colombian government organizations and private companies have in the face of this type of cyber attacks that in the last decade have gained considerable strength and failures have been identified. in the processes and implementations of each company, managing to avoid failures or information hijacking.

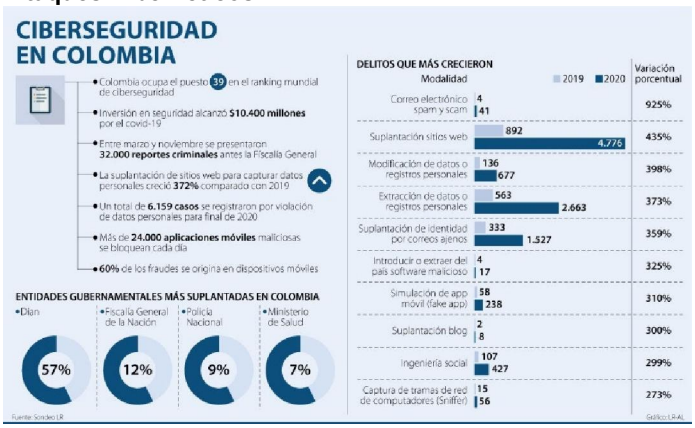
Keywords: Cyber attack, Threat, Integrity, Ransomware, Information Hijacking.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Durante los últimos cinco años y con la llegada de la pandemia las empresas colombianas se vieron obligadas a realizar grandes cambios, adaptándose a la transformación digital y el trabajo en casa. En el que se ha acelerado el crecimiento del uso de tecnologías de información y comunicación. Pero estos cambios han traído consecuencias negativas en el aumento de ciberataques. Teniendo en cuenta los últimos reportes proporcionados por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) se evidencio un incremento de ataques cibernéticos en Colombia de siete billones de denuncias. Este reporte tuvo una afectación de 8.355 casos. Según CCIT, Colombia ocupo el puesto 39 en el ranking de ciberseguridad. [18] Tomando en cuenta esta información, a continuación, se evidencia el incremento de ciberataques en relación a entidades públicas más suplantadas en Colombia y donde se describen otros delitos que también han tenido un incremento significativo en el país, como se evidencia en la ilustración 1.

Ilustración 1. Estadística Ataques Cibernéticos



Fuente: ASUNTOS LEGALES. Los ataques cibernéticos aumentaron 30% durante el primer semestre de este año según la Fiscalía. [Consultado 12 octubre 2023]. Disponible en: https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212

De acuerdo, con la anterior ilustración las estadísticas proporcionadas por CCIT permite determinar el incremento que ha tenido el país en cuanto a los ciberataques después de la pandemia.

[18] CCIT. Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno. [Sitio web]. 2022. [Consultado 12 de octubre 2023]. Disponible: https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

Ransomware siendo uno de los ataques cibernéticos más peligrosos que actualmente existe, es una de las causas principales en las que se posiciona como uno de los códigos maliciosos en los que se accede indebidamente a los sistemas de información y redes corporativas. Afectando en gran manera lo equipos de cómputo, sistemas de información e infraestructura tecnológica, logrando acceder sin autorización y teniendo un incremento de códigos maliciosos para lograr el objetivo de adquirir la data de las compañías. Y así mismo, los atacantes cibernéticos toman provecho de las nuevas condiciones de trabajo.

Durante la pandemia el comportamiento del cibercrimen la fiscalía General de la Nación, en su último reporte presentado desde el año 2021 tuvo un gran incrementado en el número de ataques cibernéticos en las compañías y entidades públicas de Colombia ya que han implementado estrategias y medidas de ciberseguridad para fortalecer la seguridad de la información, pero estos planes de trabajo no han sido idóneos ya que se ha disparado el número de casos en secuestro de la información a organizaciones mediante ransomware en el que han ocasionado pérdidas económicas importantes que han afectado pagos por las extorsiones ocasionados por los atacantes cibernéticos. [19]

Por ello, la ciberseguridad debe hacer parte fundamental para las estrategias organizacionales fomentar y reforzar la seguridad, realizar la actualización de los sistemas de información, hacer copias de seguridad e identificar las brechas de seguridad y las vulnerabilidades existentes en un sistema. De acuerdo a esto, es importante evaluar las amenazas que se puedan presentar en la seguridad de las empresas y entidades públicas tomando todas las medidas necesarias para controlar y evitar que la información confidencial y sensible sea tomada por los ciberdelincuentes. De esta manera, es importante que las empresas públicas y privadas puedan estar preparadas para afrontar los ataques cibernéticos ransomware. A continuación, se describe los sitios web de empresas en Colombia con mayor peligro de acceso a la red corporativa, ya que los usuarios cuando asignan las contraseñas en las credenciales de usuario no se especifica los parámetros que debe tener por política de seguridad, según la ilustración 2.

[19] CCIT. Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno. [Sitio web]. 2022. [Consultado 12 de octubre 2023]. Disponible: https://www.ccit.org.co/estudios/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno/

Ilustración 2. Dominios de empresas más expuestas por las credenciales de usuarios.

No.	Dominio.gov.co comprometido	Credenciales expuestas	No.	Dominio.gov.co comprometido	Credenciales expuestas
66	muisca.dian.gov.co	3,318	703	www.colpensiones.gov.co:8070	359
226	simo.cnsc.gov.co	1,122	744	jovenesenaccion.dps.gov.co	339
277	www2.icfesinteractivo.gov.co	933	813	www.positivaenlinea.gov.co	307
328	personas.serviciodeempleo.gov.co	766	837	web.sispro.gov.co	296
446	www.icetex.gov.co	555	893	visibles.migracioncolombia.gov.co	273
461	evaluarparaavanzar311.icfes.gov.co	539	910	www.fna.gov.co:8081	265
500	sede.colpensiones.gov.co	499	937	snrbotondepago.gov.co	254
512	oficinavirtual.shd.gov.co	489	943	webazure.dian.gov.co	252
573	community.secop.gov.co	434	1077	solicitudes.icetex.gov.co	213
605	servidorpublico.sigep.gov.co	414	1200	www.medellin.gov.co	192
629	miseguridadsocial.gov.co	404	1244	ecenso.dane.gov.co	182
682	epagos.registraduria.gov.co	373	1297	www.funcionpublica.gov.co	176

Fuente: CCIT. Estudio trimestral de ciberseguridad Ataques a entidades de gobierno. [Consultado 12 de octubre 2023] Disponible: https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf

Teniendo en cuenta, la estadística proporcionada por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), se evidencia que la mayoría de las compañías no tienen implementando políticas de seguridad. Por eso, es importante toda organización debe contar con estos procedimientos documentos, con la finalidad de proteger la data y todos los activos de las empresas en Colombia.

1.2 FORMULACIÓN DEL PROBLEMA

En los últimos años las entidades del gobierno colombiano han sido blanco de ciberataques en los cuales han ocasionado daño en los sistemas de información, suplantación de identidad y robo de información sensible. Sin embargo, es importante tomar medidas de prevención que permitan implementar técnicas que logren identificar intrusos en la red y software malintencionados. Por lo tanto, es necesario hacer recomendaciones al personal de las organizaciones colombianas para evitar ataques cibernéticos ransomware con el fin de evitar descargas de programas maliciosos o accesos a páginas engañosas.

De acuerdo a lo anterior, es posible consolidar la siguiente pregunta en el que se relaciona la presente monografía:

¿Qué impactos puede ocasionar los ataques cibernéticos ransomware en las entidades colombianas y como se puede evitar?

2 JUSTIFICACIÓN

El desarrollo de la presente monografía se enfoca en la identificación de los últimos diez años sobre la problemática que se ha estado presentando en las organizaciones colombianas. A medida que evoluciona el mundo de las tecnologías y con la implementación de nuevas transformaciones digitales e innovaciones, se ha detectado un incremento de amenazas cibernéticas que afectan notoriamente a las organizaciones. Es necesario que se tomen medidas para analizar esta problemática que afecta la confidencialidad, disponibilidad e integridad de la información. Por ello, es necesario tomar medidas de prevención y establecer estrategias que logren combatir la delincuencia cibernética.

Es importante identificar las implicaciones que se presentan con los ciberdelincentes que lograr acceder a los sistemas informáticos con el fin de tomar información de las organizaciones para obtener un lucro económico. Lo ideal es tomar decisiones importantes con el fin de implementar la solución para la prevención de los ataques cibernéticos y así mismo proteger la infraestructura tecnológicas de las compañías.

La finalidad de esta monografía es realizar un estudio sobre Ransomware con el fin de proteger las entidades estatales prevenirlas de este tipo de ataques y analizar el comportamiento de este virus informático para implementar estrategias de seguridad que permitan minimizar estos riesgos en las organizaciones y con el fin de capacitar al personal con el propósito que conozcan este tipo de ataques.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar los ataques de Ransomware más relevantes en los últimos cinco años que han afectado a las organizaciones colombianas, mediante consultas en fuentes especializadas con el fin de proponer recomendaciones y estrategias que permitan minimizar el impacto de los riesgos.

3.2 OBJETIVOS ESPECÍFICOS

- Detallar los ataques de Ransomware más relevantes en los últimos cinco años que han afectado a las organizaciones colombianas, presentados a través de fuentes oficiales con el fin de identificar las técnicas abordadas por los atacantes.

- Consultar las vulnerabilidades más recurrentes de las organizaciones que puedan ser aprovechadas por algún ransomware, para la identificación de los impactos que se genere dentro de la organización.

- Proponer una serie de recomendaciones de buenas prácticas a los usuarios y administradores del sistema con el fin de diseñar planes de trabajo que permitan identificar los ataques cibernéticos que se presenten en las organizaciones estatales.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La presente monografía se enfocará en el comportamiento y métodos utilizados en los ataques cibernéticos ransomware que han afectado en los últimos años a las empresas colombianas. De esta manera, vamos a retomar unos años atrás, exactamente en el año de 1989, cuando el estudiante de Harvard Joseph L. Popp creo el primer ransomware el cual lo llamo: “AIDS Trojan” en la que utilizo el método de criptografía simétrica, 20.000 discos estaban infectados de este virus y fueron distribuidos a una conferencia de salud a la OMS. Cuando se dio la utilización de estos discos automáticamente los equipos de cómputo fueron afectados propagándose en todos los archivos del sistema capturando la información para luego pedir rescate. Algo importante en este primer ransomware el impacto que tuvo en ese momento no fue tan efectivo ya que la distribución de este virus era limitada. [20]

Desde entonces, la evolución de ransomware ha venido cambiando y se han descubierto a través de los años la existencia de variantes en gran escala, propagándose de manera rápida, utilizando métodos de infección. Permitiendo a los ciberdelincuentes descubrir nuevas formas de acceder a un sistema de información o red corporativa, logrando identificar las vulnerabilidades de un sistema con el objetivo de quebrantar la seguridad de las compañías.

Los ataques ransomware también llamado malware de rescate, se basa en utilizar un código malicioso en el que cifra los archivos de un sistema o víctima. La finalidad de este ataque ransomware es impedir el acceso a los datos o información de un equipo de cómputo o dispositivo. Secuestrando la data y los mantiene bloqueados, piden dinero a la víctima para el rescate de la información. [21] Ransomware tiene comportamientos singulares en donde puede variar la dinámica de ataque, ya que cuenta con una variedad de familias de códigos maliciosos en las que no se podrán detener.

Con la primera aparición de Ransomware y haciendo una comparación en la actualidad, los atacantes han empleado un enfoque más inteligente y sofisticado, en el que inician el

[20] STORMSHIELD. Breve historia de los ransomware. 2012. [Sito web]. [Consultado 12 octubre 2023]. Disponible en: https://www.stormshield.com/es/noticias/breve-historia-de-los-ransomware/

[21] IBM. ¿Qué es Ransomware?. 2023. [Sitio web]. [Consultado 14 octubre 2023]. Disponible: https://www.ibm.com/mx-es/topics/ransomware

ataque por medio de un correo electrónico de suplantación adjuntando un enlace de una página web malintencionada. Cuando la víctima accede al sitio web ingresa todos los datos personales obteniendo de una manera fácil las credenciales de la víctima. Con esta información el delincuente cibernético acceder a la red de una organización, teniendo la libertad de visualizar las bases de datos, acceso al correo electrónico y demás accesos de la compañía. Su finalidad es estudiar la manera de atacar e identificar las vulnerabilidades del sistema de manera silenciosa sin que el administrador del sistema detecte alguna anomalía, para luego propagar el código malicioso, secuestrar la data y bloquear el sistema. [22]

Es importante que las organizaciones colombianas tomen conciencia y logren plantear capacitaciones en ciberseguridad a los empleados para que puedan tener bases sólidas que les permitan identificar si existe alguna actividad sospechosa como, por ejemplo: un correo electrónico malicioso o sitio web malicioso. Esto ayudara para que el atacante cibernético no pueda acceder al sistema o que pueda obtener las contraseñas de acceso aprovechándose del desconocimiento de las víctimas.

Una de las formas en la que se puede reconocer un código malicioso en el sistema, es por formatos o extensiones de los archivos. Ransomware cifra la información o los datos de manera simétrica o asimétrica, con el objetivo de restringir los accesos de los archivos ya contaminados por el malware. El delincuente cibernético procede a enviar una petición a la víctima por medio de un correo electrónico o mensaje de texto donde se le indica a la víctima una alerta de rescate donde saldrá afectado el sistema, aplicaciones del recurso tecnológico. La victima observara una ventana emergente en el que se le indica bloqueo total de la maquina o dispositivo. Esta es una de las maneras en las que engañan a las victimas obteniendo la información confidencial de una entidad o persona. [23]

Ransomware tiene diferentes variantes según la forma de engaño, en el que se logra agrupar en dos categorías: Crypto Ransomware (CR), Ransomware no criptográfico (NRC). [24]

---

[22] REVISTABYTE. El ransomware y su evolución. 2022. [Sitio web]. [Consultado 15 de octubre 2023]. Disponible: https://revistabyte.es/noticias/el-ransomware-y-su-evolucion/

[23] IBM. ¿Qué es el ransomware? 2022. [Consultado 15 octubre 2023]. Disponible: https://www.ibm.com/mx-es/topics/ransomware

[24] M. G. Moreno, Introducción a la Metodología de la investigación educativa 2, 2a reimpresión., vol. 2. México, D.F. Editorial Progreso, 2000.

4.1.1 Crypto Ransomware (CR). Este tipo de Ransomware es un malware que cifra la información o datos de un dispositivo en el que solicita un rescate para la recuperación de la información adquirida por el atacante cibernético. La manera en el que ransomware tiene dos maneras para acceder de manera ilícita es por medio del correo electrónico y sitios web. Los atacantes atacan a las empresas y personas, el modelo que utilizan los ciberdelincuentes es con el modelo de ransomware de servicio.

Teniendo en cuenta lo anterior, el comportamiento de Ransomare criptoransomware se desarrolla de tres maneras:

1. El delincuente cibernético envía un mensaje con el malware y este lo dirige al equipo de cómputo o dispositivo de la víctima mediante de un correo electrónico este medio contiene un enlace engañoso.
2. El segundo paso el malware cifra los archivos o la información de la víctima con la finalidad de encriptar los archivos del sistema.
3. El ransomware deja un mensaje en el que cobra un rescate para la recuperación de la información. Una de las maneras en las que los delincuentes es dejar una carpeta con los archivos encriptados o dejan un mensaje en el escritorio del equipo de cómputo indicando que la información está secuestrada. [25]

Ransomware cifrado tiene dos cifrados:

- **Simétrico**: En el cifrado de algoritmo simétrico se utiliza: AES, DES, 3DES o RC4. El cifrado simétrico solo utiliza una sola contraseña para cifrar los datos, el proceso de cifrado es rápido y transfiere grandes cantidades de información, fácil de usar.

- **Asimétrico**: En el cifrado de algoritmo asimétrico para este caso se utiliza DSA o RSA. Para este algoritmo es necesario la utilización de dos contraseñas para que pueda funcionar, debe ser una clave pública y privada. En la publica la contraseña debe publicarse para poder cifrar la información y en la privada sirve para descifrar los datos. [26]

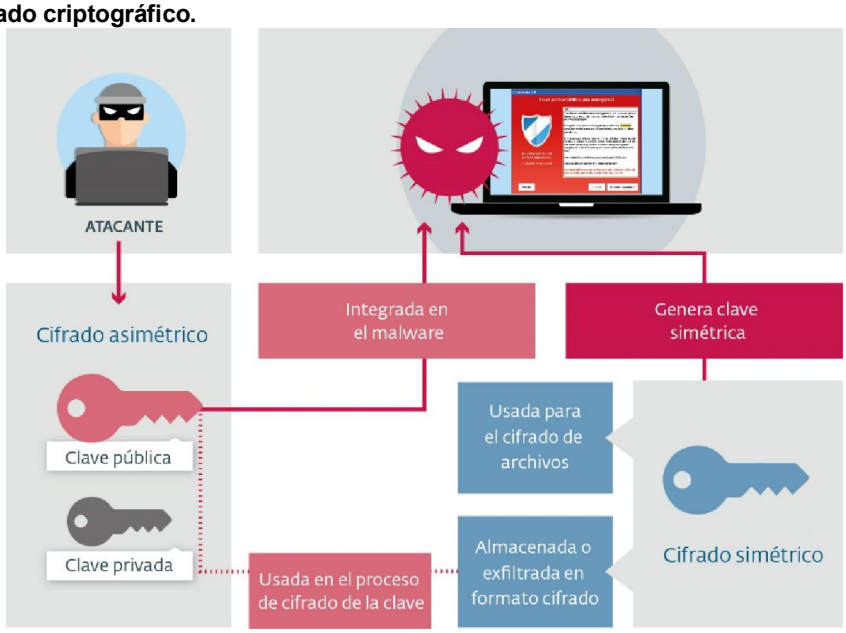
[25] PANDASECURITY. CryptoLocker: Qué es y cómo evitarlo. 2020. [Sitio web]. [Consultado 16 octubre 2023]. Disponible: https://www.pandasecurity.com/es/mediacenter/malware/cryptolocker/

[26] INNOVACIONDIGITAL360. Cifrado simétrico y asimétrico: Definición y diferencias.2023. [Sitio Web]. [Consultado 16 octubre 2023]. Disponible:https://www.innovaciondigital360.com/blockchain/cifrado-simetrico-y-asimetrico-definicion-y-diferencias/

4.1.2 Locker Ransomware o Ransomware no criptográfico (NCR). Este tipo de ransomware rechaza el acceso a los dispositivos, ya que su funcionalidad es bloquear las funciones principales del equipo de cómputo. Es decir, no permite que la víctima pueda tomar el control del equipo ya que bloquea el teclado y el mouse, y esta acción inhabilita poder acceder al dispositivo. Cuando la víctima no puede tener el control del equipo le arroja un mensaje que el ciberdelincuente le envía en el que le informa para obtener la recuperación del dispositivo deber pagar un dinero. En este tipo de ransomware tiene una parte positiva y es que no logra acceder a los archivos del dueño de la información, esto sucede cuando la víctima logra recuperar el control del equipo cuando hace el pago sobre el rescate solicitado, la información no la tocara el atacante cibernético. [27]

En la siguiente imagen se puede evidenciar el modus operandi del atacante cibernético al implementar el algoritmo cifrado asimétrico y simétrico. Ilustración 3.

Ilustración 3. Cifrado criptográfico.



Fuente: WELIVESECURITY. Cómo y por qué el cifrado moldeó al ransomware criptográfico. 2016. [Sitio web]. [Consultado 11 de octubre 2023]. Disponible: https://www.welivesecurity.com/la-es/2016/09/13/cifrado-ransomware-criptografico/

El uso de este tipo de cifrado criptográfico se puede utilizar para fines para proteger los datos ante un acceso no autorizado, se puede emplear en organizaciones privadas y públicas.

[27] KASPERSKY. Identificación de ransomware: en qué se diferencian los troyanos de cifrado. [Sitio web]. 2022. [Consultado 29 de abril 2022]. Disponible en: https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Según un informe por ESET existen dos vectores de propagación más comunes sobre los ataques cibernéticos ransomware Crypto y Loker: [28]

- Envió de correo electrónico con contenido engañoso.
- Acceso a páginas web engañosas y descargar de archivos en redes peer to peer (P2P).

Los vectores de propagación indicados anteriormente tienen algo en común. El atacante cibernético a través de estos dos métodos necesita de la intervención de las personas o usuarios para que realicen la acción de descargar los archivos o acceder a los sitios web maliciosos.

El riesgo que puede ocasionar los ataques ransomware en las empresas al obtener la data, es comprometer la disponibilidad de la información. Este activo es muy importante para todas las organizaciones ya que esto afectaría e impactaría la reputación y la economía de las empresas, al ser afectados por un ataque cibernético ransomware. De igual manera las compañías trabajan con redes compartidas en donde tiene el riesgo de compartir y acceder a redes compartidas. Uno de los riesgos definidos es la perdida financiera, perdida de información confidencial como datos confidenciales y privados de clientes, indisponibilidad de los servicios y aplicaciones corporativas, daños críticos en la infraestructura tecnológica.

Esto evidencia una problemática importante en las compañías privadas y públicas que afectan la infraestructura IT y la data. Lo ideal es asegurar toda la data, la red corporativa para que pueda ser protegida y evitar los ataques cibernéticos. Se puede concluir que toda información de cualquier persona u organización se ha convertido en un material muy importante para la sociedad en general y para los ciberdelincuentes. Los atacantes cibernéticos han mejorado los métodos de ataque para acceder de manera sospechosa a las organizaciones.[29]

---

[28] ASSETS ESETSTATIC. 2022. [Sitio web]. [Consultado 15 octubre 2023]. Disponible: https://web-assets.esetstatic.com/wls/2017/11/guia-ransomware.pdf

[29] QUANTI. Los riesgos del ransomware que representa para la empresa y lo que todos los administradores de sistemas deberían considerar al momento de asegurar sus datos. [Sitio web]. 2023. [Consultado 15 de octubre 2023] Disponible: https://quanti.com.mx/articulos/los-riesgos-del-ransomware-que-representa-para-la-empresa-y-lo-que-todos-los-administradores-de-sistemas-deberian-considerar-al-momento-de-asegurar-sus-datos/

Los problemas de seguridad en los sistemas de información en las organizaciones colombianas, se detectó las falencias y las vulnerabilidades que tiene estos sistemas y recursos tecnológicos. Los delincuentes informáticos utilizan técnicas y herramientas especializadas logran acceder y afectar la infraestructura tecnológica. Los ciberdelincuentes toman las medidas necesarias para no ser detectados y así poderse infiltrar. La mayoría de las veces logran no ser descubiertos ya que logran borrar cualquier evidencia para así no ser identificados.

Los atacantes cibernéticos cada vez encuentran métodos avanzados para acceder a la información y tomar los datos personales, en la mayoría de los casos cobran dinero para que sea recuperada la data. Estos tipos de ataques contienen diferentes actividades ilegales. Por lo tanto, existen siguientes infracciones como las que se describen a continuación:[30]

- **Delitos que atentan contra la integridad, confidencialidad y disponibilidad de la data:** Estos delitos consisten en acceder de manera no autorizada y proceden a realizar cambios en los datos, hurtan la información. Su finalidad es obtener la información para realizar actos o actividades ilícitas, esto con fines económicos y espionaje a las organizaciones públicas y privadas.

- **Delitos informáticos:** Consiste en realizar fraudes, falsificación, acceden a los recursos tecnológicos sin autorización, suplantando la identidad de la víctima u organización.

- **Delitos según el contenido:** Estos delitos tienen contenido explico que afectan la integridad de las personas como por ejemplo el racismo, religión, juegos ilegales, entre otros.

- **Delitos según su infracción:** Estos delitos hacen referencia a los derechos de autor o la información es propiedad intelectual.

Los ataques cibernéticos están al acecho y tienen a direccionarse a las entidades públicas de Colombia ya que no invierten en infraestructura y son las más afectadas porque no invierten en la seguridad o no realizan inversiones en innovación tecnológica. No fortalecen la seguridad en la red corporativa. Los intrusos logran acceder de una

[30] GONZÁLEZ SOLARTE, Nancy. Casos de estudio de cibercrimen en Colombia. Riohacha. Universidad Nacional Abierta y a Distancia. 2020. 23-24 p. [Consultado 25 agosto 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36606/nagonzalezso.pdf?sequence=1&isAllowed=y

manera fácil, obteniendo contraseñas y credenciales para llegar a la información confidencial de una compañía, también logran afectar los recursos tecnológicos ya que realicen estudiar para detectar las vulnerabilidades del sistema o la red.

Las cifras más recientes que se han presentado por los ciberdelincuentes según el Centro Cibernético de la Policía Nacional pretende minimizar estos ataques de suplantación de tarjetas SIM, Vishing, fraude de criptomonedas, ransomware y afectación de correos corporativos. Estos ataques cibernéticos obligan a las organizaciones invertir mucho dinero para mejorar la infraestructura y la red corporativa evitar este tipo de daños en los sistemas de información y los recursos tecnológicos, pero la inversión es necesaria para la protección de la compañía, la integridad, disponibilidad y confidencialidad de la información.[31]

Una de las falencias que se ha detectado en las organizaciones es cuando se requiere de muchas mejoras en el recurso tecnológico, plantear estrategias de mejorar e implementar políticas de seguridad para evitar las brechas de seguridad, capacitando a los empleados para que se fortalezcan en el conocimiento en temas de ciberseguridad. Para que no estén expuestas a hacer blanco de ataques cibernéticos, ya que lo ciberdelincuentes se aprovechan del desconocimiento de los empleados. Las entidades públicas no están lo suficientemente capacitados sobre los riesgos que se lleguen a presentar. Los empleados de una compañía acceden a las peticiones que se realicen por correo electrónico y no lo ven como una sospecha y proceden a realizar descargas de archivos no confiables o abrir archivos con procedencia no segura. Estas acciones no son seguras ya que el administrador del sistema no detecta a los intrusos y no existe un monitoreo constante a la red corporativa para que pueda bloquear la descarga de software malicioso, esto dan paso a que los intrusos accedan al sistema y proceden a propagar el virus logran contaminar los equipos de cómputo e infiltrarse para tomar información sensible o confidencial de las entidades públicas y privadas. En ese orden de ideas, la mayor vulnerabilidad para todas las organizaciones son los usuarios o colaboradores de las compañías.[32]

Los ataques cibernéticos en Colombia tuvieron un crecimiento de número de incidentes reportados a las autoridades de la Policía Nacional. Se registró un total de casos

---

[31] EL TIEMPO. Los distintos ataques afectan principalmente a empresas y agencias gubernamentales del país. [Sitio web]. [Consultado 25 de agosto 2021]. 2019. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesos-al-ano-380830

[32] GARCÍA FORERO, Luis Felipe Guillermo, et al. Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. 2020.

registrados de 23.000 incidentes cibernéticos del 2021 con una gran diferencia del año 2020 que tuvo un reporte de 18.290 casos reportados. Pero para el año 2023, se ha evidenciado el crecimiento de denuncias de crímenes cibernéticos. [33]

- Para el 2023, se ha reportado en el sector de la salud, superando un 78%, en cuanto al año 2022.[34]
- Se registraron en el 2022 54.121 denuncias sobre delitos cibernéticos, superando un incremento del 30% más que el año 2021.[35]
- En el 2021 se generó un reporte de 23.000 delitos informáticos, con un incremento del 30% del año 2020.
- En el 2020 se generó un reporte de 18.290 delitos informáticos, con un incremento del 30% del año 2019.
- En el 2019 se generó un reporte de 15.948 delitos informáticos, con un incremento del 20% del año 2018.
- En el 2018 se generó un reporte de 21.687 delitos informáticos, con un incremento del 36% más que año 2017.

De acuerdo a estas cifras, se ha evidenciado un incremento bastante notorio durante los años transcurridos, por día se reportan denuncias con más de 60 casos de ataques cibernéticos. Colombia es uno de los países con más aumento de ataques cibernéticos con el 133% en todas las instituciones afectadas por ransomware a diferencia del año 2021. Con estas cifras son de gran preocupación ya que está en riesgo la información sensible de las organizaciones que ponen el riesgo el acceso de la información confidencial y logran afectar los recursos tecnológicos de las compañías.[36]

---

[33] ASUNTOS LEGALES. Los ataques cibernéticos aumentaron 30% durante el primer semestre de este año según la Fiscalía. [Sitio web]. [Consultado 25 de agosto 2021]. 2021. Disponible en: https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212

[34] AMERICA-RETAIL. Security Report 2023 anticipa un aumento de los ciberataques. [Sitio web]. 2023. [Consultado 25 de febrero 2023]. Disponible en: https://www.america-retail.com/ciberseguridad/security-report-2023-anticipa-un-aumento-de-los-ciberataques/

[35] LA REPUBLICA. Ataques cibernéticos han crecido 30% y EPM y Sanitas son dos de miles. [Sitio web]. [Consultado 24 de febrero 2023]. 2022. Disponible en: https://www.larepublica.co/empresas/ataques-ciberneticos-en-colombia-han-crecido-30-epm-y-sanitas-son-dos-de-miles-3508452

[36] BLOOMBERGLINEA. ¿Por qué hay una ola de ciberataques en Colombia y el país está tan vulnerable? [Sitio web]. 2023. [Consultado 26 de febrero 2023]. Disponible en: https://www.bloomberglinea.com/2023/01/25/por-que-hay-una-ola-de-ciberataques-en-colombia-y-el-pais-aun-es-tan-vulnerable/

4.2 MARCO CONCEPTUAL

4.2.1 Amenaza Informática, consiste en causar daño a un sistema informático con el objetivo de lograr acceder a la información confidencial, su finalidad es divulgarla la data secuestrada los atacantes la publican en la web oscura. También los intrusos modifican y destruyen la información para ocasionar grandes datos en las compañías. Estos eventos son muy utilizados para generar mala reputación a las empresas. Otra amenaza informática es vulnerar un sistema con la finalidad de aplicar la ingeniera social; manipulando a las victimas ya que no cuentan con el conocimiento en temas de ciberseguridad o no existe una capacitación adecuada a los empleados.[37] Los ciberdelincuentes sacan provecho de la infraestructura de las compañías cuando existen vulnerabilidades en un sistema en el que les permitirá acceder a la red corporativa de manera ilegal con el objetivo de interrumpir el funcionamiento de un sistema de información o recurso tecnológico logrando acceder a la data para secuestrarla o dañarla. [38]

Teniendo en cuenta la definición de las amenazas informáticas se evidencia dos tipos de amenazas:

- Amenazas intencionales, se producen a razón de tomar información no autorizada con la finalidad de implementar técnicas de ingeniera social y divulgar código malicioso en un sistema de información.

- Amenazas no intencionales, toda acción tomada dentro de una organización y este es divulgada, expone una vulnerabilidad en un sistema de información el cual pone en riesgo todo tipo de información.

[37] HOSTDIME. ¿Qué es una amenaza informática? ¿Cómo contenerla? [Sitio web]. 2020. [Consultado 10 septiembre 2021] Disponible en: https://www.hostdime.la/blog/que-es-una-amenaza-informatica-como-contenerla/

[38] SEGURIDAD INFORMÁTICA. Amenazas a la Seguridad de la Información. [Sitio web]. [Consultado 11 de septiembre 2022]. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

4.2.2 Ataque Informático, cualquier manipulación ofensiva de explotación intencional tiene como finalidad tomar el control de destruir un sistema informático. Aprovechando las vulnerabilidades para acceder a exponer o alterar la información y la infraestructura tecnológica. Por lo general esto es provocado por los atacantes cibernéticos que acechan la forma de acceder a un sistema de manera no autorizada con el objetivo de suplantar identidades y realizar espionaje. Las técnicas más utilizadas es recurrir a vulnerabilidades que existen en un sistema o las fallas que se puedan presentar en la infraestructura (software y Hardware) para tener el control.[39]

4.2.3 Delito Informático, corresponden actividades ilícitas, ya que estas acciones se ejecutan por medio de entornos tecnológicos y digitales, redes corporativas, sistemas informáticos y equipos de cómputo o dispositivos, su finalidad es causar daños, provocan impedir el uso de los sistemas informáticos. Estos delitos abarcan acciones ilegales, cuando una persona realiza delitos cibernéticos logra dañar la infraestructura IT y la reputación de las compañías, estos delincuentes cibernéticos son expertos porque tienen conocimientos en ciberseguridad, tienen muchas modalidades de engañar a las víctimas, realizar la captura de la data, daños en la infraestructura TI. Por lo general, los delitos informáticos son muy difíciles de detectarlos ya que las compañías en algunas ocasiones no lo reportan por el temor de perder prestigio en la sociedad.[40]

4.2.4 Denegación del servicio, también es conocido como ataque DoS, el propósito es generar saturación en los puertos, con la finalidad de enviar información consecutiva, y logra saturar o sobrecargar el servidor de un sistema. Con esta acción logra que el servidor se sobrecargue y no pueda sostener, ni seguir prestando los servicios de un sistema de información, afectando en gran manera las páginas web de la compañía. De esta manera, logra que todos los servicios se bloqueen y así mismo impedir que los usuarios no puedan acceder. La finalidad de este ataque es saturar el flujo de información e imposibilitar el servidor no pueda prestar los servicios de manera correcta. [41]

[39] CASER. Ataque Informático. [Sitio web]. 2022]. [Consultado 11 de septiembre 2022]. Disponible en: https://www.caser.es/glosario-seguros/comercio/ataque-informatico

[40] SIGNIFICADOS. Qué es Delitos informáticos. [Sito web]. 2021. [Consultado 30 de agosto 2021]. Disponible en: https://www.significados.com/delitos-informaticos/

[41] F5. Denegación del servicio. [Sitio web]. 2022]. [Consultado 12 de septiembre 2022]. Disponible en: https://www.f5.com/es_es/services/resources/glossary/denial-of-service

4.2.5 Ingeniera Social, es una técnica de manipulación que son empleadas por los atacantes cibernéticos o cibercriminales con el propósito de engañar a las víctimas, utilizan métodos de persuasión o suplantación de identidad. Logrando obtener la información personal, confidencial y bancaria de las víctimas con el objetivo de ejecutar actividades ilícitas o ilegales, sobre un sistema logrando acceder a la red o dispositivo, tomando el control de acceso requerido. Es importante tener en cuenta que existe varios tipos de ingeniera social que aplican de acuerdo a la población vulnerable, como por ejemplo: Phishing, Spear phishing, Vishing, Quid Pro Quo, entre otros.[42]

4.2.6 Ransomware, hace referencia a un software malintencionado, es decir Malware consiste en impedir el acceso a la información, equipos de cómputo o dispositivos, ya que su finalidad es obtener la data sin autorización del dueño de la información para secuestrar la información para luego pedir cobrar recompensa para que la víctima la pueda recuperar y así evitar que el atacante cibernético la destruya. Los atacantes cibernéticos indican un tiempo determinado para se realice el pago y así se pueda devolver la información de la víctima. Ransomware se propaga por múltiples mecanismos, por medio de publicidad engañosa, envío de mensajes falsos por medio de correos electrónicos, campañas de spam, por malas configuraciones de software, por la descargar de herramientas no oficiales de la compañía y por no realizar actualizaciones constantes en los aplicativos, sistemas operativos y equipos de cómputo.

El propósito de los delincuentes cibernéticos es engañar a las victimas logrando que la víctima realice la descarga del software infectado por el virus en la que fue enviada por un correo electrónico, al realizar la descarga es depositado en los equipos de cómputo o dispositivos telefónicos. En la actualidad estos métodos de ataque cibernético realizan el bloqueo de la data y del dispositivo. La habilidad de los ciberdelincuentes amenaza a las víctimas con realizar fugas de información confidencial, para publicar la información en páginas de web oscura, es decir publicarla en internet. Para las victimas es una situación compleja ya que puede ocasionar daños económicos, dañar la reputación de las organizaciones o víctima. En efecto se convierte en una extorsión critica. [43]

[42] KASPERSKY. Ingeniería Social. ? [Sitio web]. 2022]. [Consultado 14 de septiembre 2022]. Disponible en:https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

[43] TRENDMICRO. Qué ocurre durante un ataque de ransomware?. [Sitio Web]. 2021. [Consultado 28 de agosto 2021]. Disponible en: https://www.trendmicro.com/es_es/what-is/ransomware/ransomware-attack.html

4.2.7 Smishing, es un tipo de delito informático que emplea mensajes de textos al celular o dispositivo, con la finalidad de que la víctima logre comunicarse a través de un link de una página web maliciosa, el atacante informático logra suplantar el número telefónico de la entidad bancaria para generar confianza a la víctima, esto permitirá tener el acceso total de la información personal, el delincuente accede a las paginas bancarias haciéndose pasar por la víctima y procede a extraer el dinero. [44]

4.2.8 Software Malicioso, es conocido como Malware, está diseñado para entorpecer un sistema de información o recurso tecnológico causando daño, con la intención destruir o perder la información. El software malicioso hace acciones indebidas donde procede a instalarse con la aprobación de las víctimas, sin que ellos tengan el conocimiento de que corresponde a programas informáticos malicioso, en algunas ocasiones se instalan sin la detección del mismo accediendo a toda la infraestructura TI. Esta acción ocasiona el bloqueo de los equipos de cómputo y el hurto de información. Existen otros tipos de software malicioso como: spyware, virus, registrador de pulsaciones, ransomware o todo tipo de código malicioso que pueda acceder a los dispositivos o equipos de cómputo.[45]

4.2.9 Virus Informático, la intención de los virus informáticos es modificar la operatividad en los equipos de cómputo o dispositivos. Logran que la víctima o el administrador del sistema no pueda identificarlos o ser detectados. Estos virus pueden acceder sin la autorización de la víctima ya que no existe un control o software de detección de software maliciosos. Este código malicioso se puede ejecutar por sí mismo, logra instalar una ruta especifica con la intención de dañar el sistema, con esta acción logra hacer la ejecución en los equipos de cómputo. Los archivos del sistema son reemplazados por archivos ejecutables generando una copia del archivo infectado. [46]. Los virus informáticos se propagan a través de software maliciosos tienen el poder de duplicarse de manera automática y logran modificarlos para ser destruirlos. De este modo, su intención es ocasionar daño al sistema.

Existen muchos virus, la evolución que ha tenido constante y demasiado rápida. Estos virus se propagan rápidamente y peligrosa afectan los recursos tecnológicos de compañías públicas y privadas o gente del común. La manera de poderlos identificar estos virus:

---

[44] OSI. ¿Qué es el smishing? [En línea]. 2022. [Consultado 24 de noviembre 202]. Disponible en: https://www.osi.es/es/actualidad/blog/2021/11/17/que-es-el-smishing

[45] VMWARE. Programas maliciosos. [Sitio web]. 2021. [Consultado 06 de septiembre 2021]. Disponible en: https://www.vmware.com/latam/topics/glossary/content/malware.html

[46] WIKIPEDIA. Virus informático. [Sitio web]. 2021. [Consultados 15 de septiembre 2021]. Disponible en: https://es.wikipedia.org/wiki/Virus_inform%C3%A1tico

- **Macro Virus:** Su manera de proceder es adjuntar los archivos que están creados por un programa. Se ejecutan un clic o digitando una tecla. Se ha identificado en este tipo de virus se descubren en archivos de paquetes office como: Word o Excel, se propagando a medida que la víctima abre los archivos, luego se van duplicando, porque toma los documentos y los infecta, luego se propaga en el sistema o dispositivo. Para el caso de los correos electrónicos su función es enviar una copia exacta del archivo origen, hace una lista de distribución de los contactos de la víctima. Cuando la víctima envía el correo con el archivo afectado lo envía a sus contactos. Los receptores abren el correo descargan en el equipo de cómputo o dispositivo móvil y este se descarga los archivos de formato: (.xls o .docx) para luego alterar el contenido. [47]

- **Virus de archivo:** Para este virus el objetivo principal, es situar código malicioso y poner en riesgo todos los archivos, la data del sistema. De esta manera, se crea botnets interconectados que su función es deshabilitan la seguridad y el software que tienen los equipos de cómputos, pero solo actúan cuando los dispositivos están encendidos. Para este tupo de virus es reescriben los archivos ejecutables del sistema, para luego activarse cuando el equipo esta encendido, su acción es tomar el control del dispositivo de manera inmediata.[48]

- **Virus de Secuencia de Comandos (Scripting):** La función de este virus Scripting es atacar las páginas de navegación que la víctima acceder de manera constante o más accedida. Este virus reemplaza el código o lenguaje de programación de los sitios o páginas web con el objetivo de insertar enlaces o links en el que el contenido es un software malicioso para que se pueda propagar o extenderse en el equipo de cómputo. Por supuesto, las víctimas no detectan este acceso indebido, ya que tiene contenido se evidencia de manera confiable, pero realmente no es así, ya que el sitio web es malicioso y las publicaciones o anuncios que realizan falsos, logrando que la víctima acceda sin tener la precaución de que es un virus y este infectar los dispositivos o el equipo de cómputo. [49]

---

[47] LATAM KASPERSKY. ¿Qué es un virus de macro? 2022. [Consultado 22 de noviembre 2022]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/macro-virus

[48] SEGU-INFO. Archivos Ejecutables. [En línea]. 2022. [Consultado 22 de noviembre 2022]. Disponible en: https://www.segu-info.com.ar/virus/tipos_virus

[49] AVAST. ¿Qué son las secuencias de comandos en sitios cruzados (XSS)? [En línea]. 2022. [Consultado 22 de noviembre 2022]. Disponible en: https://www.avast.com/es-es/c-xss

- **Virus del sector de arranque:** Este tipo de virus consiste en infectar las particiones del disco duro y estos proceden a ejecutarse en el arranque del ordenador. Su propagación es a través de los dispositivos físicos como por ejemplos; las memorias USB y discos extraíbles. [50]

[50] SOFTWARELAB. ¿Qué es un virus informático? [En línea]. 2022. [Consultado 23 de noviembre 2022]. Disponible en: https://softwarelab.org/es/que-es-un-virus-informatico/

4.3 MARCO HISTÓRICO

En el año 2015, la compañía Trustwave generó un informe a nivel global de seguridad donde se evidencia que los ciberdelincuentes obtiene un 1,425% de inversión por la implementación de la infección malware a los equipos de cómputo e infraestructuras TI de las organizaciones. Por ende, el secuestro de información ha tomado un impacto bastante importante en los últimos años que ha afectado a usuarios y organizaciones se han visto afectadas por códigos maliciosos como el Ransomware que perjudica los entornos corporativos.

En el año de 1989, se reportó el primer caso de los ataques cibernéticos Ransomware en el que fue identificado con el nombre de Troyano PC Cyborg, ya que la funcionalidad de este ataque era reemplazar los todos los archivos existentes en el equipo de cómputo y tomaba el nombre de: "autoexec.bat". De esta manera el código malicioso ocultaba los directorios, también los cifraba con otros nombres, sobre todo en los archivos que estaba en la ruta de la unidad C. Este ransomware lo que realizaba era dejar todos los archivos inutilizables. Luego solicitar a la víctima cobrar un pago para la renovación de la licencia o la devolución de los archivos, en ese entonces pedían un valor de 189 dólares a PC Cyborg Corporation.[51]

Durante siguientes años, se alertó que existían evidencias nuevas versiones y que estaban relacionadas con el ataque cibernético Ransomware. Su objetivo primordial era extorsionar a las víctimas y compañías.

En el año 2005, se identificó una nueva referencia u otro tipo de Ransomware llamada PGPVCoder. Este ataque consistía en infectar equipos de cómputo mediante un archivo llamado: "anketa.doc", consistía en el envió de un archivo adjuntado, en el que el contenido era un código malicioso y este era enviado a correos electrónicos. La victima al descargar el archivo infectado se propagaba e identificaba todas las extensiones: .xls, .doc, .pdf, .ppt, entre otros, con el fin de contaminar los archivos del equipo de cómputo. [52]

[51] WELIVESECURITY. La evolución del ransomware: del ochentero PC Cyborg a un servicio en venta. [Sitio web]. 2015. [Consultado 6 de octubre 2021]. Disponible en:https://www.welivesecurity.com/la-es/2015/08/21/evolucion-del-ransomware/

[52] OSORIO SIERRA, Andrés Felipe. Esquema metodológico apoyado en una herramienta (software) para la detección y prevención de Crypto Ransomware en una estación de trabajo. 2019. [Consultado 6 de octubre 2021]. Disponible en: https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/1391/OsorioSierraAndresFelipe2019.pdf?sequence=1&isAllowed=y

Se conoció el caso de Winlock, que se trata de un software malicioso que su función era bloquear las pantallas del equipo de cómputo. Este ransomware fue identificado en el año 2010. Cuando este ataque cibernético accedía en el equipo realizaba el bloqueo en la pantalla, luego arrojaba un mensaje donde se solicitaba, la recuperación de la data, pero esta tenía una condición y era el pago inmediato. Y así, el atacante cibernético devolvería la funcionalidad del equipo a la víctima. El valor que le solicitaba el atacante cibernético era de 10 dólares. Si la víctima no realizaba el pago el ciberdelincuente le afectaría los archivos del dispositivo tecnológico. [53]

En el año 2006, se detectó un nuevo ransomware llamado: “Archiveus”. Fue uno de los primeros ransomware con cifrado asimétrico y este contenía un algoritmo RSA. Su función era bloquear todos los accesos de los archivos en el equipo de cómputo logrando afectar la ruta de la carpeta “Mis Documentos”, los delincuentes cobraban por el rescate de la data. [54]

Sobre el año 2008 surge una nueva aparición de Ransomware, el trabajo de los ciberdelincuentes era engañar a los usuarios para descargar software falso, para luego acceder al sistema, para luego realizar una copia del programa malicioso en el equipo de cómputo, capturar la información de la víctima y después indicarle al usuario cobrar dinero hacer la recuperación de la data o que el dispositivo no infectarlo del virus.

En el año 2012, se conoció otro ataque cibernético llamado “Reventon” consistía en bloquear el acceso al sistema. A las víctimas el delincuente cibernético era mostrar un falso mensaje, donde se le informaba de un supuestamente mensaje que su procedencia era de la policía nacional. El mensaje se le informaba que la víctima había infringido la ley, y por esta razón debía pagar una multa. De este modo, el sistema se restauraría. [55]

En el transcurrir de los años los ataques cibernéticos han tenía una evolución bastante amplia ya que cada aparición de estos virus llega con más fuerza y son más difíciles de detectar. Teniendo en cuenta que las organizacionales, en ese entonces no actualizaban

---

[53] CODIGOGEEK. WinLock te permite bloquear ventanas en Windows utilizando una contraseña. [Sitio web]. 2022. [Consultado 11 octubre 2023]. Disponible: https://www.codigogeek.com/2012/11/21/winlock-te-permite-bloquear-ventanas-en-windows-utilizando-una-contrasena/

[54] SENA, Matías Ezequiel; HECHT, Pedro. Carrera de Especialización en Seguridad Informática.

[55] QUANTI. La historia del ransomware: Historia, tipos de ransomware y futuros impactos. 2023. [Sitio web]. [Consultado 10 octubre 2023]. Disponible: https://quanti.com.mx/articulos/la-historia-del-ransomware-historia-tipos-de-ransomware-y-futuros-impactos/

los sistemas operativos, no tenían implementadas políticas de seguridad y planes de contingencia para evitar este tipo de ataques cibernéticos.

En el año 2014, se tomaron medidas en contra de los ataques cibernéticos Ransomware. Luego, surgieron nuevas apariciones y variantes de este tipo de ransomware. Una de ellas llamada: "CryptoWall" consistía en afectar masivamente los equipos de cómputo de las organizaciones. Debido a esta situación los ciberdelincuentes tuvieran ingresos de 325 millones de dólares.[56]

Entre los años 2015 y 2016, aparecieron nuevos ataques cibernéticos, pero ya estaban direccionados para dispositivos móviles llamados "LockerPin" consistía en cambiar el PIN y este no les permitía el acceso a los teléfonos móviles. Estos afectaban son sistemas operativos Android.[57]

En el año 2017, se revelo una nueva aparición de un ciberataque llamado "WannaCry", infectando a más de 250.000 dispositivos realizaron la implementación de una técnica de hacking llamada "EternalBlue", consistió en vulnerar los protocolos SMB de Windows. Con este ataque cibernético los ciberdelincuentes lograron obtener mucho dinero debido a la gran cantidad de dispositivos infectados, razón por la cual las victimas procedían a pagar según los mensajes enviados a los dispositivos.[58]

En el año 2018 en el que aparece otra evolución de Ransomware llamada "SynAck", este contenía mecanismos que permitían contrarrestar las tecnologías de protección. Se identificaron las siguientes medidas:

- Anular los procesos y servicios sobre el acceso de los archivos importantes y confidenciales.
- Trastornar el código ejecutable antes de realizar alguna compilación.
- Limpiar los registros del evento, la finalidad es obstaculizar el análisis del incidente.

---

[56] ALFA-INFORMATICA. Virus Cryptowall – ¿Qué es? 2016. [Sitio web]. [Consultado 12 octubre 2023]. Disponible: https://www.alfa-informatica.com/virus-cryptowall-que-es/

[57] BBC. Lockerpin, el peligroso virus que cambia la contraseña de bloqueo de tu celular. [Sitio web]. 2015. [Consultado 10 octubre 2023]. Disponible: https://www.bbc.com/mundo/noticias/2015/09/150915_tecnologia_lockerpin_virus_cambia_contrasena_bloqueo_lv

[58] KASPERSKY. La evolución del ransomware y las herramientas para combatirlo. [Sitio web].2018. [Consultado 6 de octubre 2021]. Disponible en: https://www.kaspersky.es/blog/evolution-of-ransomware/16275/

- Rastrear con la finalidad de no ser identificados.
- Emplear mecanismos de duplicación en los procesos con el fin de acceder como un proceso malicioso a un proceso legítimo. [59]

Debemos tener en cuenta la importancia de implementar esquemas de seguridad con el fin de minimizar este tipo de ataques, ya que a medida que pasan los años Ransomware ha tenido una evolución bastante amplia y así es más difícil identificarlos.

En el año 2019, a partir del primer semestre se reportó el 2.94% tuvo en su momento una disminución de victimas ransomware a comparación de los dos años anteriores. Es así, que la compañía Kaspersky registro entre 900.000 y 1,2 millones de víctimas de ransomware durante el primer periodo del año afectando notoriamente parte del territorio Colombia el cual sufrieron organizaciones con una escala de ataques ransomware afectando las redes informáticas. Utilizando métodos de ingeniera social y detección de vulnerabilidades en los sistemas de información, equipos de cómputo y aplicaciones desactualizadas.[60]

Una de las técnicas utilizadas para este ransomware es llamado Ryuk que es un tipo de malware que infecta los sistemas y cifra archivos para secuestrar la información de las víctimas para así solicitar el rescate de los datos de los usuarios dueños de la información. [61]

Para el año 2020, fue el año más duro para Colombia dado a que tuvo más ataques cibernéticos debido a la pandemia ya que los hackers y organizaciones criminales aprovecharon este nuevo cambio de transformación digital, donde muchas compañías implementaron el trabajo en casa. En el país se registró más de 7 millones de intentos para acceder a la infraestructura TI y sistemas de información. Uno de los informes entregados por la compañía Fortinet reporto 1,6 millones de intentos de accesos no autorizados en todo el territorio colombiano. Dentro de este reporte se identificó técnicas de ataque como phishing método utilizado con el fin de engañar a las victimas mediante

---

[59] SECURELIST. Panorama de las ciberamenazas en el segundo trimestre de 2018. [Sitio web]. 2018. [Consultado 10 octubre 2023]. Disponible: https://securelist.lat/it-threat-evolution-q2-2018/87394/

[60] SECURELIST. La historia de 2019: Ciudades sitiadas por ransomware. [Sitio web]. 2019. [Consultado 9 octubre 2023]. Disponible: https://securelist.lat/story-of-the-year-2019-cities-under-ransomware-siege/89947/

[61] SECURELIST.LAT. La historia de 2019: Ciudades sitiadas por ransomware. [Sitio web]. 2019. [Consultado 26 de febrero 2023]. Disponible en: https://securelist.lat/story-of-the-year-2019-cities-under-ransomware-siege/89947/

correos electrónicos con archivos HTML del cual tenían archivos adjuntos con software malicioso y este logra acceder a los datos de la víctima con la finalidad de direccionarlo a una página web maliciosa y así obtener los datos personales y proceder a realizar la estafa correspondiente. [62]

Para los años 2021 y 2022, el incremento de amenazas cibernéticos y cibercrimen ha sido aún más alto dado que muchas organizaciones han sido estudiadas y vulneradas dado al incremento del trabajo en casa y la transformación digital. Se han reportado las ciudades más afectadas en cuanto este tipo de ataques ransomware son Bogotá con un reporte de 8.355 casos, Medellín 1.664 ataques cibernéticos y Cali con un total de 1.569. Estudios identificaron modalidades de ciberataques de las cuales se indicaron; suplantación de identidad con un incremento del 108% registradas durante el año 2020.Otra modalidad más usada con un reporte del 29% siendo así un valor alto con la suplantación de páginas web con la finalidad de capturar los datos personales de las víctimas. La fiscalía General de la Nación indico que tuvo un alto incremento con modalidades como Phishing, smishing y pharming con un incremento de 638 casos reportados.[63]

Para el 2023, se ha identificado que el cibercrimen aun será peor dado que el incremento del malware no ha dejado de aumentarse, el sector de salud y financiera es uno de los atractivos para los delincuentes cibernéticos dado que logran obtener información sensible de los usuarios, así como las claves de acceso a las cuentas bancarias, acceso a los dispositivos móviles logrando acceder y proceder a realizar el fraude.

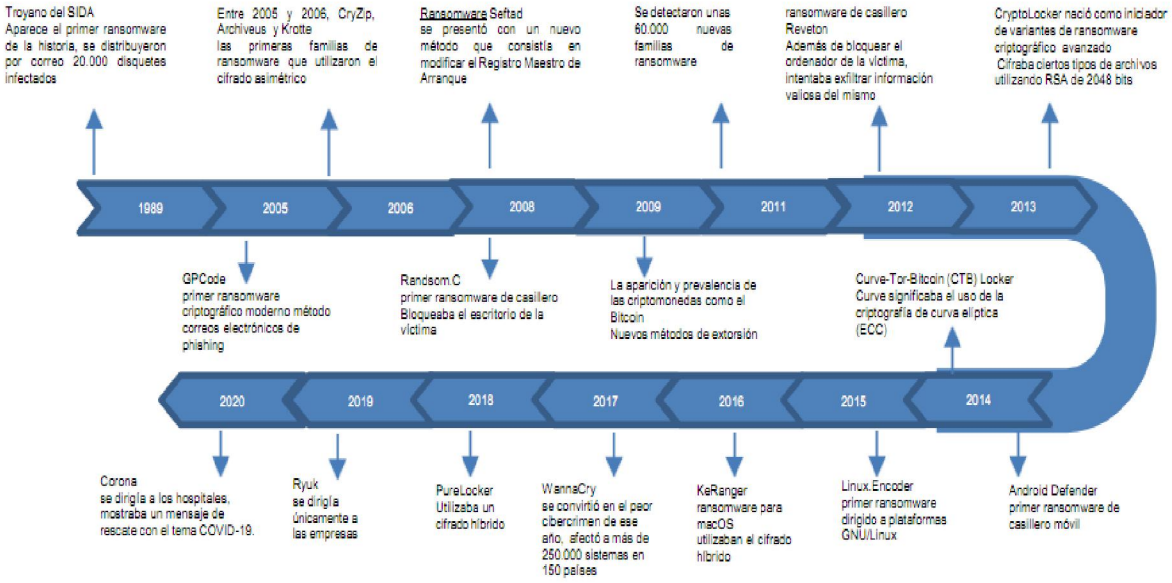
A continuación, se evidencia durante los últimos años la evolución que ha tenido Ransomware. Ilustración 1.

---

[62] INFOBAE. 2020 fue el año en que Colombia tuvo más ciberataques. [Sitio web]. 2021. [Consultado 27 febrero 2023]. Disponible en: https://www.infobae.com/america/colombia/2021/02/25/2020-fue-el-ano-que-colombia-tuvo-mas-ciberataques/

[63] SEMANA. El año de los ciberataques en Colombia, estas son las alarmantes cifras. [Sitio web]. 2021. [Consultado 27 de febrero 2023]. Disponible en: https://www.semana.com/economia/empresas/articulo/el-ano-de-los-ciberataques-en-colombia-estas-son-las-alarmantes-cifras/202125/

Ilustración 4. Evolución de Ransomware.



Fuente: PINZÓN RUIZ, Jhon Jairo. 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. 2021. P. 26. [Consultado 27 febrero 2023]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/50093/jjpinzonru.pdf?sequence=3&isAllowed=y

Haciendo un análisis del diagramada representado en la ilustración anterior se puede observar se ha representado algunos nombres de virus y troyanos durante los años en que la variante correspondiente se amplió rápidamente en Internet, es así que evidenciando la evolución de Ransomware ha tenido un crecimiento y mejoras en las técnicas implementadas por los atacantes cibernéticos. Se identificó que los ciberdelincuentes no necesitan exploits para la escalada de privilegios y la propagación de malware.

Desde el año 1989, ransomware es una amenaza que ha existido desde hace más de 30 años de historia donde las organizaciones han sufrido este tipo de ataques cibernéticos ransomware donde han tenido un impacto significativo en los negocios, ya que esto arroja resultados como pérdida de ingresos e información confidencial y prestigio de la compañía. En la actualidad uno de los de los ataques cibernéticos más relevantes es el Ransomware ya que es una de las amenazas más existentes en la seguridad de la información dentro de las organizaciones colombianas, esto con lleva a que las

compañías deben implementar estrategias para mitigar estos ataques cibernéticos y así asegurar la disponibilidad e integridad de la información.[64]

Teniendo en cuenta la evolución que ha tenido Ransonware durante los últimos años. Es así como se describe los cambios evidenciados para este ataque cibernético.

- **Año 1989 (PC Cyborg),** se evidencio un troyano que consistía en reemplazar archivos con formato AUTOEXEC.BAT realizaba el ocultamiento de directorios o archivos, ya que eran cifrados de la unidad C, produciendo un daño en el sistema lograban dañar el sistema operativo dejando inutilizable. Adicionalmente, os atacantes cibernéticos le solicitaba a la víctima la renovación de la licencia para luego exigir un pago que oscilaba un valor de 189 dólares los delincuentes cibernéticos lo direccionaban a un correo de nombre de PC Cyborg Corporation.[65]

- **Año 2005 (GPCoder)**, consistía en cifrar archivos con ciertas extensiones específicas, luego de esta acción, dejaba un archivo de texto en el escritorio del equipo de cómputo y proporcionaba unas instrucciones a la víctima para cobrar el rescate de la información.[66]

- **Año 2010 (WinLock)**, consistía en bloquear el equipo de cómputo y este arroja un mensaje de advertencia donde se le indicaba a la víctima realizar un pago a cambio de hacer la recuperación del sistema que este caso era desbloquear el equipo.

- **Año 2012 (Reveton)**, consistía en engañar a la víctima haciéndola creer que era un "virus de la policía"[67] este realizaba el bloqueo del equipo de cómputo, es decir, se realizaba un bloqueo de la pantalla y arrojaba un mensaje falso indicando que era la Policía Nacional o FBI, su descripción decía el equipo es bloqueado ya que contenía material ilegal como software pirata o contenido con derechos de autor, y este le indicaba que debía pagar una multa y así este le restauraría el sistema.

---

[64] CCIT. Informe tendencias del Cibercrimen primer trimestre del año 2020. [Sitio web]. 2020. [Consultado 6 de noviembre 2022]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-abril-2020-final.pdf

[65] WELIVESECURITY. La evolución del ransomware: del ochentero PC Cyborg a un servicio en venta. [Sitio web].2015. [Consultado 08 octubre 2023]. Disponible: https://www.welivesecurity.com/la-es/2015/08/21/evolucion-del-ransomware/

[66] INFORTEC. Historia del ransomware: los 15 casos más curiosos. 2018. [Sitio web]. [Disponible 01 octubre 2023]. Disponible: https://www.infortec.co/historia-del-ransomware-los-15-casos-mas-curiosos/

[67] Ibid., p, 10.

- **Año 2013 (CryptoLocker y CryptoWall),** este tipo de Ransomware se describe en realizar cifrados asimétricos con clave pública RSA de 2048 bits quiere decir que solo cifra archivos con extensiones .doc y jpg, este medio de amenaza solicita al usuario realizar un pago por medio de bitcoins.[68]

- **Año 2015 (CTB Locker),** consiste en realizar la propagación de un virus troyano, cuando la víctima realiza la descarga por medio de engaños este se ejecuta descargando un código malicioso y procede a realizar el cifrado de la información de la víctima. Su modalidad es indicarle a la víctima que deberá realizar un pago para hacer rescatar la información capturada.

- **Año 2017 (CTB Locker),** consiste en cifrar los archivos del equipo de cómputo que está infectado modalidad de algoritmos AES-128 y RSA-2048, donde es imposible hacer la recuperación ya que se propaga de manera rápida infectando a todos los equipos que están en la red, esta modalidad de ataque busca detectar las vulnerabilidades del sistema, para atacar e infectar archivos y todo lo que contenga el recurso tecnológico. [69]

- **Año 2018 (Ryuk)**: Se desarrolló para deshabilitarla las características de recuperación del cual tiene por defecto los sistemas operativos, este ataque realiza el cifrado del disco duro mientras está conectado a la red, es así como ingresa al sistema y no permite el acceso de la víctima. Por lo tanto, pide un pago para la recuperación de la información y el dispositivo afectado.[70]

- **Año 2020 (Jokero):** Es un malware que funciona como un ransomware su objetivo principal es propagarse a nivel mundial afectando diferentes sistemas de información. [71]

---

[68] WELIVESECURITY. Guía de Ransomware. [Sitio web].2022. p. 9 - 10. [Consultado 01 de mayo 2022. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/11/guia-ransomware.pdf

[69] Ibid., p, 10.

[70] WIKIPEDIA. Ryuk (ransomware). [Sitio web]. 2021. [Consultado 9 septiembre 2021]. Disponible en: https://es.wikipedia.org/wiki/Ryuk_(ransomware)

[71] ESEDSL. Nuevos virus informáticos surgidos en 2020 que deberías mantener alejados de tu empresa. [Sitio web]. 2020. [Consultado 26 de febrero 2023]. Disponible en: https://www.esedsl.com/blog/nuevos-virus-informaticos-surgidos-en-2020#:~:text=Jokeroo,vez%20y%20de%20forma%20internacional.

- **Año 2021 (Babuk):** Es un malware creado por rusos, consiste en cifrar archivos existentes en un sistema logrando afectar el sistema y así lograr pedir el rescate por la información cifrada.[72]

[72] UNAALDIA HISPASEC. REvil Ransomware da un paso más en su extorsión. [Sitio web]. 2022. [Consultado 26 febrero 2023]. Disponible en: https://unaaldia.hispasec.com/2019/12/revil-ransomware-da-un-paso-mas-en-su-extorsion.html

4.4 ANTECEDENTES

Para el desarrollo de este documento investigativo se tomaron varias referencias de proyectos relacionados con los ataques cibernéticos ransomware, documentos, noticias y revistas científicas.

Tomando como referencia la investigación el documento "Tendencias Cibercrimen Colombia 2019 - 2020", documento realizado por Adriana Ceballos, Lorena Mesa; Carlos Argáez y Fredy Bautista por la entidad la Cámara Colombiana de Informática y Telecomunicaciones del año 2019 donde se evidencio un análisis previo que permitió conocer el impacto que tiene actualmente el cibercrimen. Muchas empresas han sido blanco de ataques cibernéticos ransomware, y se describe las nuevas modalidades de engaño. La presente monografía permitió tomar información relevante e importante para continuar con la investigación y análisis sobre el comportamiento, técnicas de ataque y explorar información sobre las organizaciones criminales que utilizan el ransomware como método de engaño.[73]

Monografía "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", desarrollado por Jhon Jairo Pinzón Ruiz de la Universidad Nacional Abierta y a Distancia en este documento se plasmó información sobre los impactos de Ransomware que han afectado notablemente las entidades de Colombia donde se centraliza todos los vectores de ataque, el crecimiento que ha tenido los ataques cibernéticos durante los últimos años en Colombia. [74]

Proyecto "Ciberseguridad en Colombia, avances y retos" desarrollado por Laura Daniela Bueno Munar de la universidad Militar Nueva Granada en este documento se argumentó la dificultad y consecuencias que ha tenido Colombia en cuanto al cambio tecnología y la nueva transformación digital dado que durante el año 2021 y 2022 se registraron más de 45.000 denuncias por fraudes y delitos cibernéticos. Los atacantes cibernéticos están mejorando las técnicas de ataque logrando secuestrar la información y afectar de gran manera los sistemas de información y portales web de las organizaciones colombianas

[73] CCIT. Tendencias cibercrimen Colombia 2019-2020. [Sitio web]. 2020. [1 de octubre 2021] Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[74] PINZÓN RUIZ, Jhon Jairo, et al. 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. 2021. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/50093/jjpinzonru.pdf?sequence=3&isAllowed=y

denegando el acceso a los servicios y afectando la operatividad de los recursos tecnológicos de las compañías. Se evidencio durante la investigación de este documento que las entidades colombianas han sido muy afectadas por estos grupos de cibercrimen dado que la infraestructura TI en algunas situaciones son obsoletas, la falta de actualizaciones en las aplicaciones, servicios y recursos tecnológicos. Las organizaciones no invierten en la infraestructura tecnológica y esto es una puerta abierta para que los intrusos accedan e identifiquen las vulnerabilidades, los delincuentes cibernéticos pueden acceder más fácil. [75]

Proyecto “Importancia de la seguridad informática y ciberseguridad en el mundo actual”, desarrollado por José Luis Gamboa Suárez de la Universidad Piloto de Colombia. En este documento se analizó el auge que tiene los delitos informáticos durante los últimos años, debido a la falta de conocimiento de temas de seguridad informática y ciberseguridad, es una vulnerabilidad que aprovechan los delincuentes cibernéticos para acceder a la red corporativa, dispositivos móviles en el que implementan nuevas técnicas de engaño para así lograr acceder a la información sensible y datos personales. [76]

[75] BUENO MUNAR, Laura Daniela, et al. Ciberseguridad en Colombia, avances y retos. 2022. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/41303/BuenoMunarLauraDaniela2022.pdf.pdf?sequence=2&isAllowed=y

[76] GAMBOA SUAREZ, José Luis. Importancia de la seguridad informática y ciberseguridad en el mundo actual. 2020. [Consultado 24 de febrero 2023]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

4.5 MARCO LEGAL

Con el fin de determinar un marco legal en relación al presente trabajo investigativo se mencionan las siguientes leyes de los cuales se han reglamentado los esquemas de ciberseguridad en Colombia.

4.5.1 CONPES 3701 de 2011, Lineamientos de Política para Ciberseguridad. Este lineamiento de ciberseguridad o ciberdefensa buscar plantear una estrategia a nivel nacional que permita mejorar la capacidad de asumir retos en cuanto a la seguridad informática y estos sean asumidos de manera oportuna frente a riesgos que se puedan presentar, teniendo en cuenta el compromiso que tiene con el estado colombiano. Se analizan las debilidades que están presentes, ya que se hacen revisiones de antecedentes tanto nacional e internacional. Por lo anterior, se identificaron los siguientes problemas:

- Implementar iniciativas que permitan prevenir y controlar todas las operaciones y emergencias cibernéticas con la finalidad de proteger la infraestructura tecnológica a nivel nacional.

- Diseñar y plantear capacitaciones especializadas que abarquen temas de ciberseguridad.

- Fortalecer y dar cumplimiento a la legislación en la protección de los datos.

El estado colombiano debe emitir el documento CONPES (Consejo Nacional de Política Económica y Social) 3701, lineamientos indispensables de políticas de seguridad y ciberdefensa para fortalecer la protección de los datos.[77]

[77] MARTÍNEZ RODRÍGUEZ, William. Análisis de la evolución del aseguramiento informático en entidades del sector gobierno colombiano. Universidad Nacional Abierta y a Distancia. 32 p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/37623/whmartinezr.pdf?sequence=1

4.5.2 CONPES 3854 de 2016, Policía Nacional de Seguridad Digital. Es un lineamiento que plantea una estrategia nacional, teniendo en cuenta ciertas consideraciones de la seguridad digital. Esto implica la gestión de riesgos en la seguridad digital cuya finalidad es que las entidades públicas y privadas logren establecer e identificar los riesgos y amenazas en las que están expuestas ante cualquier ataque cibernético. Este un documento publicado por MinTIC, MinDefensa, Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación. Para el año 2020 se estimó una implementación de políticas de seguridad que permita impactar de manera positiva la economía del país. [78]

4.5.3 Ley 1581 de 2012, Protección de datos personales, esta ley expone el desarrollo y el derecho constitucional a toda la ciudadanía. En el que permite conocer la actualización de los datos que estén almacenado en las bases de datos. La ley 1581 determina todos los datos sensibles y confidenciales, expone la privacidad del titular en el cual se puntualizan los procedimientos y condiciones que existe en la legalidad para el tratamiento de los datos personales. En resumen, se incorporan los mecanismos de control o sanciones que incumplan la ley.[79]

4.5.4 Ley 1273 de 2009, Protección de la información y los datos, esta ley se ajusta en detalle los delitos informáticos y penalidades que conllevan el territorio colombiano, con el uso indebido a los datos personales, para las organizaciones se debe tener en cuenta esta ley que las protege, donde los intrusos atentan contra los datos sensibles y causan daño.

Este delito se clasifica en dos grupos:

- Delitos contra la integridad, disponibilidad e integridad de los datos en los sistemas de información.
- Delitos informáticos y otras infracciones.

[78] DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3854. 2016. [Consultado el 17 de septiembre 2022. Bogotá, Colombia. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[79] AGUILAR CASTAÑEDA, Miguel. La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados. Universidad Católica. Colombia. 2018. 12 p. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/23060/1/La%20Ley%20De%20Protecci%C3%B3n%20De%20Datos%20En%20Colombia.pdf

Esta ley proporciona el reconocimiento de conductas criminales y engañosos relacionados en los entornos informáticos, junto con aquellas situaciones que acarrean medidas punitivas a este tipo de delitos. [80]

4.5.5 LEY 1928 de 2018, Aprobación convenio sobre ciberdelincuencia, se acoge esta ley interna para el estado colombiano el contenido del convenio sobre ciberdelincuencia, el cual fue adoptada el 23 de noviembre del año 2001 en Budapest. Este convenio de ciberseguridad fue el primer tratado internacional requiere elaborar una estrategia que requiere minimizar los delitos informáticos a través de un acuerdo de leyes precisas entre todas las naciones. Se trata de tener un trato especial en cuanto a los delitos informáticos relacionados a violación de seguridad en redes, derechos de autor, delitos de odio.[81]

4.5.6 Decreto 1008 de 2018, Política de gobierno digital, este decreto detalla los lineamientos generales en relación a la política de gobierno digital. De acuerdo a esto, las estrategias de gobierno buscan, mediante el aprovechamiento de tecnologías de la información y las comunicaciones producir un estado competitivo para el sector empresarial en el que genere un entorno de confianza y un valor público. La política de gobierno digital relaciona normas y leyes que referencias a la investigación realizada y así mismo suministrando una visión más clara en cuanto a la seguridad informática. Esto con el fin de regular el estado colombiano removiendo y reconociendo las estrategias implementadas en ciberseguridad y análisis de las entidades competentes.[82]

---

[80] CHAVARRO, Camila. Casos de estudio de cybercrimen para el mejoramiento de la seguridad informática en pymes y medianas empresas. 2019. Universidad Nacional Abierta y a Distancia. 31 p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/30220/ctrujilloch.pdf?sequence=1&isAllowed=y

[81] CONGRESO DE COLOMBIA. Ley Estatutaria 1928 de 2018. Colombia. 2018. 5-22 p. [Consultado el 17 de septiembre 2022]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

[82] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1008 de 2018. Colombia. 2018. [Consultado el 17 de septiembre 2022]. Disponible en: https://www.crcom.gov.co/es/noticias/comunicado-prensa/gobierno-en-linea-se-renovo-y-ahora-sera-gobierno-digital

4.5.7 MSPI, modelo de seguridad y privacidad de la información. El modelo de Seguridad y Privacidad de la información establece las necesidades y requisitos sobre los procesos, la seguridad y la estructura organizacional. La finalidad de este modelo es salvaguardar la integridad, confidencialidad y disponibilidad manteniendo los tres pilares de la seguridad de la información. Todos los activos de las organizaciones colombianas, deben ser protegidas y que estén respaldadas legalmente. Este modelo es importante para que se de uso a la privacidad de la data y asegurar la protección de la misma. El estado colombiano busca aportar e incrementar la transparencia en la gestión pública, generando una conciencia sobre las buenas practicas relacionadas a la seguridad de la información como apoyo de la seguridad digital. [83]

[83] GOBIERNO DIGITAL. Documento de seguridad y privacidad de la información. 2021. [Consultado el 19 de septiembre 2022]. Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237872_maestro_mspi.pdf

5 ATAQUES RANSOMWARE MÁS RELEVANTES EN LAS ENTIDADES COLOMBIANAS DURANTE LOS ÚLTIMOS CINCO AÑOS

Los ataques cibernéticos Ransomware es una problemática a nivel mundial el cual es identificada por compañías importantes de ciberseguridad, antimalware y la ley de responsables que van en contra del cibercrimen como Europa y la Interpol. Es así que las investigaciones realizadas por estas entidades internacionales detectaron nuevas familias de Ransomware que llegaron a nuevas modalidades de amenazas o ataques cibernéticos con la capacidad de encontrar claves y mecanismos de acceso que logran vulnerar la infraestructura TI en las entidades públicas y privadas.

Los vectores de propagación que son utilizados por los ciberdelincuentes que logran él envió de correos electrónicos y estos son llamativos para las víctimas, dado que contiene información y publicidad engañosa logrando que las victimas accedan a páginas web o realizan descargas de archivos o software con procedencia sospechosa y estas no sean detectadas por los usuarios o víctimas.

La propagación del Ransomware es de tipo Lockscreen, este método consiste en bloquear la pantalla del computador impidiendo el acceso al equipo de cómputo, para lograr esta acción el atacante cibernético realiza él envió de un correo electrónico con la intensión de engañar a la víctima y este accede al contenido del correo y este es direccionado a un servidor para realizar la descargar del malware. Después de ser ejecutada esta acción, el archivo infectado es descargado en el equipo de cómputo y este procede a cifrar toda la información que contenga el recurso tecnológico y el software malicioso evita que cualquier sistema de seguridad como los antivirus, firewall, entre otros logren bloquear o reestablecer el sistema.[84]

Cualquier medio de envió de código malicioso ya sea por correo electrónico o páginas web de dudosa procedencia su finalidad es descargar software malicioso y este infecta, comprometen el equipo de cómputo y aplicaciones del sistema.

Teniendo en cuenta lo anterior, se tomó a consideración la investigación realizada por la Interpol que en Colombia se han detectado cinco clases de Ransomware más utilizadas:

[84] WELIVESECURITY. Guía de Ransomware. [Sitio web].2022. [Consultado 01 de abril 2022]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/11/guia-ransomware.pdf

- **Ransomware de cifrado:** Consiste en cifrar archivos, fotos, documentos importantes de las víctimas, entre otros.

- **Lock Screen Ransomware WinLocker:** Consiste en bloquear la pantalla del equipo de cómputo, evitando realizar cualquier acción que requiera la víctima.

- **Master Boot Record (MBR) Ransomwarealware:** Consiste en posicionarse en el disco duro y esta toma la acción de reiniciar el sistema operativo y modificar los registros del sistema o dañarlos.

- **Ransomware de cifrado de servidores web:** Consiste en acceder a los servidores web y proceden a cifrar los archivos que este contenga.

- **Ransomware de dispositivos móviles:** Consiste en infectar dispositivos móviles con sistema operativo Android y estos realizan descargar no autorizadas. [85]

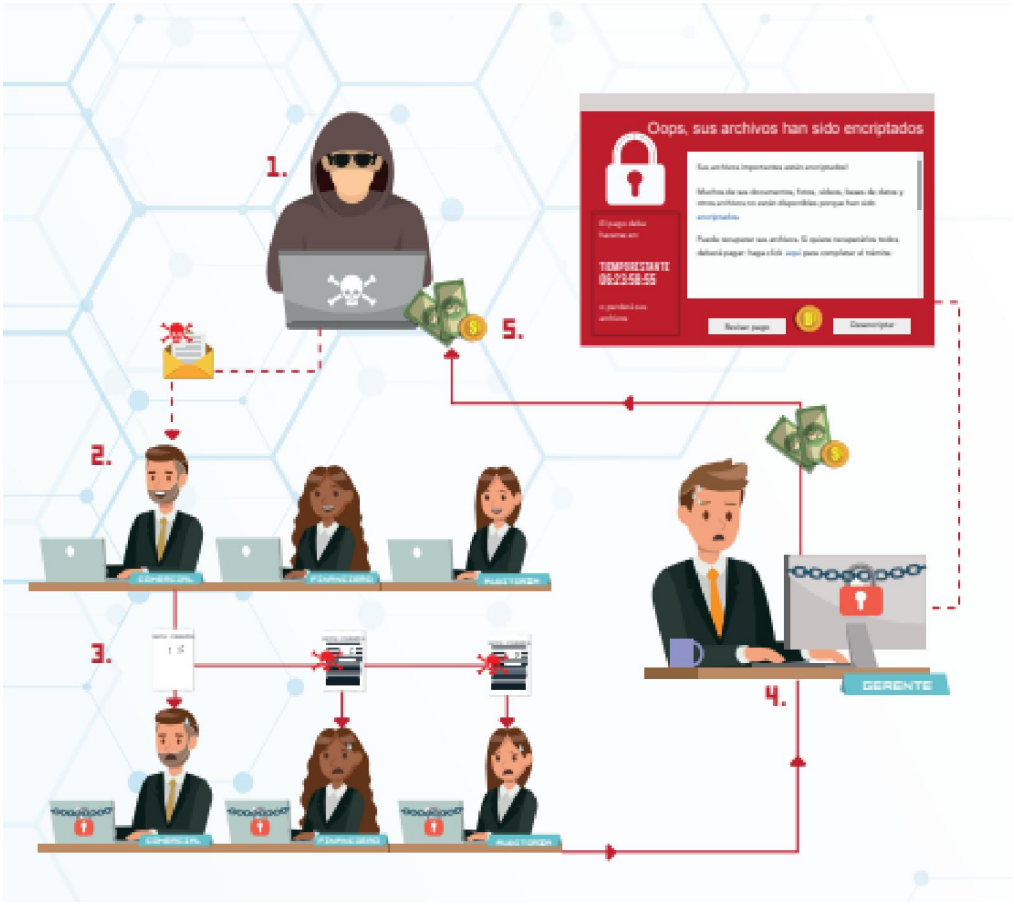
En relación a las investigaciones realizadas por la Interpol también se observó en los laboratorios forenses se identificaron variaciones de Ransomware como: Darma, Wannacry, Crysis, estas infecciones consisten en interrumpir, modificar y encriptar el flujo de información de las organizaciones afectadas por este medio de ataque. [86]

Su manera de atacar es por medio de enlaces o sitios web maliciosos que consiste en la modalidad de que la víctima logre acceder al link y realice el descargue con la finalidad de infectar el sistema y captura la información sensible de las entidades. A continuación, se visualizará la estructura o método de acceso de los atacantes cibernéticos el cual se puede evidenciar en la ilustración 2.

[85] GARCÍA FORERO, Luis Felipe Guillermo, et al. Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. [Sitio web]. 2020. [Consultado 30 de abril 2022]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[86] INTERPOL. na operación mundial conjunta contra el ransomware se salda con detenciones y el desmantelamiento de una red delictiva. [Sitio web]. 2021. [Consultado 8 octubre 2023]. Disponible: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2021/Una-operacion-mundial-conjunta-contra-el-ransomware-se-salda-con-detenciones-y-el-desmantelamiento-de-una-red-delictiva

Ilustración 5. Estructura de ataque.



Fuente: GARCÍA FORERO, Luis Felipe Guillermo, et al. Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. [Sitio web]. 2020. [Consultado 30 de abril 2022]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

La estructura de un ataque cibernético consiste en que el delincuente cibernético envía peticiones adquiriendo distintas modalidades de engaño, como, por ejemplo: método phishing, vishing, ingeniera social, correo electrónico instantáneo y este contiene software malicioso, fraude por mensajes falso en whatsapp, entre otros. Logrando engañar a las víctimas y estas accedan a las técnicas utilizadas por los delincuentes cibernéticos, logrando acceder a los dispositivos móviles y equipos de cómputo para así obtener la información personal y sensible.

En la actualidad las organizaciones colombianas han estado en constante riesgos debido a los constantes cambios que ha tenido la tecnología. Los ciberdelicuentes

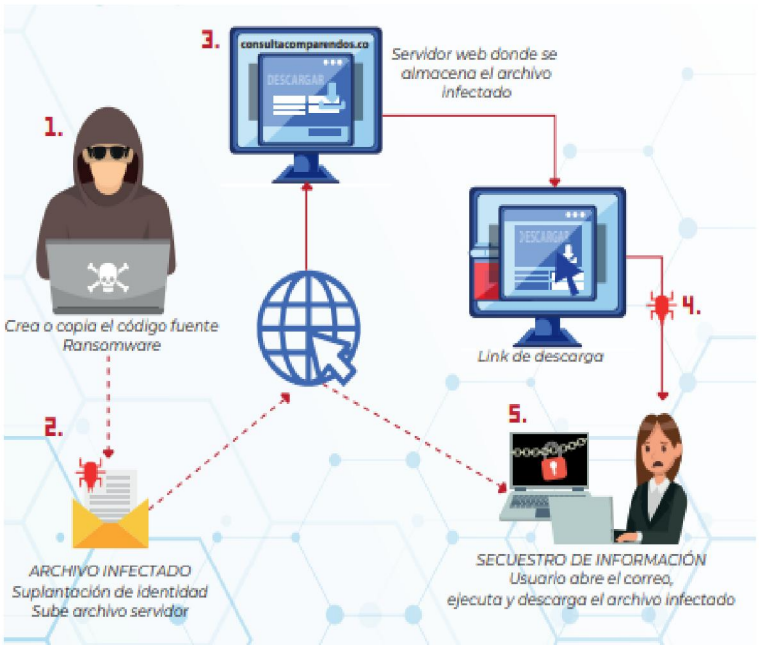
constantemente han estado implementando herramientas maliciosas con el fin de vulnerar los sistemas de información de las entidades públicas y privadas. Los ataques cibernéticos ransomware siempre estarán al asecho y las victimas serán las organizaciones, ya que los delincuentes cibernéticos tomarán como método de secuestrar la data, y pedirán rescate de la información. La finalidad es ganar un lucro económico. Y esta situación han impactado de gran manera en las organizaciones colombianas

Durante el 2020 año de la pandemia se ha detectado e identificado en Colombia hubo un alto volumen de denuncias donde se reportó el incremento de robo de información, ya que las empresas colombianas fueron blanco de ataques cibernéticos. Debido a los cambios que se ha tenido que implementar en las entidades de Gobierno y compañías privadas. Por el cambio de trabajo en casa fue necesario transformar y cambiar los procesos e implementar la transformación digital: Este fue un cambio importante que ayudo a estar en las nuevas tendencias e innovaciones tecnológicas, pero no tuvieron en cuenta algo importante; delincuentes cibernéticos quienes mejoraron las técnicas de ataque con la finalidad de afectar los sistemas informáticos y los recursos tecnológicos logrando el incremento de cinco tipos de Ransomware. Ocasionando daños importantes en las organizaciones y perdidas económicas. [87]

La modalidad o estrategias que usan los ciberdelincuentes mantienen una estructura precisa, mejorando los mecanismos que les permitiría acceder a la red corporativa, recursos tecnológicos y dispositivos móviles. Utilizando técnicas nuevas como: la ingeniera social, phishing, logrando acceder a la información y ocasionando daño en la infraestructura tecnológica. A continuación, se utilizando y proceden acceder de la siguiente manera como se muestra en la ilustración 3.

[87] CCIT. Tendencias cibercrimen Colombia 2019-2020. [Sitio web]. 2020. [1 de octubre 2021] Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Ilustración 6. Modalidad de ataque Ransomware.



Fuente: CEBALLOS LÓPEZ, Adriana. Tendencias Cibercrimen Colombia 2019-2020. [En Línea]. Consultado 14 de noviembre de 2021. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

En la actualidad la tecnología ha tenido grandes cambios importantes, una de ella es la innovación que se ha implementado en los sistemas informáticos y la infraestructura TI. De acuerdo a esto, en el presente año 2021 el esquema de ciberseguridad ha sido afectado por la llegada e incremento de ataques cibernéticos que han afectado a todas las organizaciones. Debido a la pandemia en la que actualmente se vive a causa del virus Covid-19, situación que ha ocasionado grandes pérdidas de información, estafas cibernéticas, accesos a servidores causando daño y secuestro de información.

A causa de la pandemia y debido a esta problemática las compañías públicas y privadas han tenido que replantear nuevas formas y modelos de trabajo, llevando todas las operaciones a plataformas de teletrabajo. Con la transformación digital y la incorporación del trabajo en caso por medio de accesos remotos y la descentralización de la información de las organizaciones. Razón por la cual se ha incrementado el número de uso de conexiones personales por temas laborales y estudiantiles. Lamentablemente con este nuevo cambio tecnológico y el incremento de canales virtuales genero un impacto bastante amplio sobre los ataques cibernéticos.

Muchas empresas han sido afectadas por los ciberdelicuentes, esto con lleva un incremento durante en el primer trimestre del 2020, con este aumento las compañías tuvieron que invertir en la infraestructura en el esquema de seguridad informática con un total de 10.400 millones de dólares.[88]

Durante el año 2021 la compañía británica Sophos los ataques cibernéticos en Ransomware son los más maliciosos debido a las evoluciones que ha tenido este software malintencionado realizando el método de cifrado de archivos por medio de los malware llamados "NotPetya y WannaCry" ya que su finalidad es el secuestro de la información importante de las organizaciones ocasionando grandes pérdidas económicas. Es así, como en los últimos años se ha incrementado este tipo de ataques cibernéticos. Ilustración 4.

Ilustración 7. Prevalencia de Ransomware.

Fuente: TECNOZERO. Sophos publica su estudio: El estado del ransomware en 2021. [Sitio web].2021. [Consultado 17 de noviembre 2021]. Disponible en: https://www.tecnozero.com/antivirus-y-anti-ransomware/sophos-publica-su-estudio-el-estado-del-ransomware-en-2021/

En relación a la encuesta realizada por la compañía Sophos sobre los últimos años donde partimos desde el año 2017 al 2021.

[88] NOTA ECONÓMICA. Aumentan cifras de ataques cibernéticos en Colombia al cierre de 2020. [Sitio web]. 2020. [Consultado 17 de noviembre 2021]. Disponible en: https://lanotaeconomica.com.co/movidas-empresarial/aumentan-cifras-de-ataques-ciberneticos-en-colombia-al-cierre-de-2020/

Según el informe SOPHOS se evidencio una disminución de ataques cibernéticos donde los ciberdelincuentes logaron cifrar los datos con un 73% en el 2020 en comparación del año 2021 con un 54%. Algunas de las organizaciones lograron recuperar la información. Con estos sucesos, las empresas se vieron obligadas a mejorar la seguridad de los recursos tecnológicos, implementando políticas de seguridad con la finalidad de proteger la integridad de la información y la infraestructura TI.[89]

Es importante que las organizaciones colombianas establezcan un esquema de seguridad que permita que los profesionales en seguridad informática se fortalezcan en los conocimientos en hacking, con la finalidad de implementar estrategias y planes de acción con el propósito de atender las necesidades de las entidades. Sin embargo, los ataques más relevantes que han afectado a las entidades en Colombia, se evidencio nuevos cambios en el mundo de la tecnología, de esta manera en la actualmente la humanidad ha tenido que adaptarse a los nuevos cambios en el mundo de la tecnología, el cual ha permitido a realizar cambios importantes en la plataforma y optimizar procesos y recursos tecnológicos. Pues bien es así como la tecnología ha tenido otro inconveniente y es la aparición de los ciberdelincuentes de los cuales han implementado estrategas y herramientas maliciosas con la finalidad de dañar los recursos tecnológicos y lograr obtener un lucro económico con el acceso no autorizado para obtener información sensible y confidencial tanto a la sociedad como a las organizaciones.

Las organizaciones actualmente se han visto muy afectadas con estos ataques cibernéticos, debido a la sistematización de los datos, la optimización de procesos y la mejora de los sistemas de información. Dado a estos cambios tecnológicos dentro de las entidades es importante implementar políticas de seguridad para mitigar ataques cibernéticos ya que esto ocasionaría una desestabilización económica a las entidades en Colombia. [90]

Una de las afectaciones que Colombia ha sufrido fue el año de la pandemia donde los ciberdelincuentes se aprovecharon para mejorar los métodos de ataques y buscar las vulnerabilidades de los sistemas información y con la implementación de la

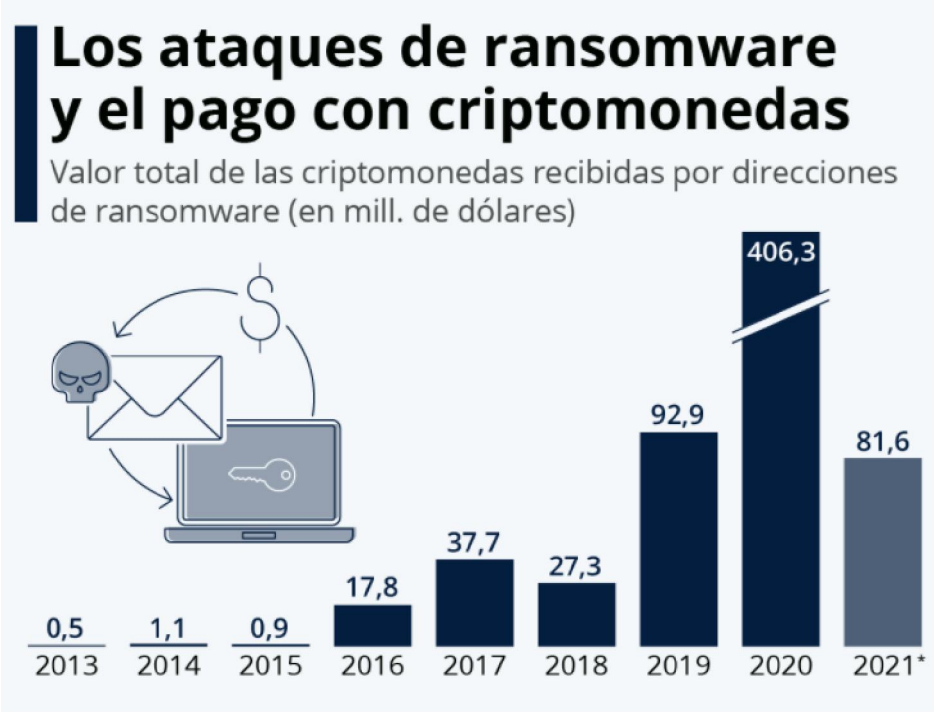
[89] TECNOZERO. SOPHOS pública su estudio: El estado del ransomware en 2021. [En línea].2021. [Consultado 17 de noviembre 2021]. Disponible en: https://www.tecnozero.com/antivirus-y-anti-ransomware/sophos-publica-su-estudio-el-estado-del-ransomware-en-2021/

[90] GUTIÉRREZ TORO, Dayro. Amenazas cibernéticas y su impacto en las organizaciones del sector industrial y servicios de Colombia en la última década. 2017 Universidad Nacional Abierta y a Distancia. Riohacha. 2020. 28-32 p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31937/dlgutierrezt.pdf?sequence=1&isAllowed=y

transformación digital fue un punto mucho más alto para que los delincuentes afectaran las organizaciones colombianas.

A continuación, se dará una de las estadísticas más relevantes sobre los ataques cibernéticos en Ransomware de los cuales se han presentado en los últimos años. Ilustración 5.

Ilustración 8. Estadística últimos años ataques cibernéticos Ransomware.



Fuente: STATISTA. Los pagos de rescate con criptomonedas por ataques ransomware se dispararon en 2020. [Sitio web]. 2021. [Consultado 17 de noviembre 2021]. Disponible en: https://es.statista.com/grafico/25240/valor-total-de-las-criptomonedas-recibidas-por-direcciones-de-ransomware--en-mill-de-dolares-%252A/

En el año 2020, fue el año más difícil de Colombia ya que se presentó este inconveniente sobre la pandemia se incrementaron los ataques cibernéticos en Ransomware debido a la transformación digital implementada actualmente, grandes cambios que se hicieron en los procesos en cuanto al manejo de trabajo remoto, ya que muchas compañías se vieron obligados a implementar métodos y estrategias para el trabajo en casa, esto disparo aún más los ciberataques.

La dirección de Investigación Criminal Interpol de la Policía Nacional identifico los servicios tecnológicos del Gobierno Electrónico fue un vector de ataque para distribuir el Ransomware. Con el nuevo enfoque que se ha dado en la transformación digital el Gobierno Colombiano desarrollo las plataformas con la finalidad de ser un estado más eficiente es así como presta los servicios en línea a los ciudadanos. Pero desafortunadamente los ciberdelincuentes examinaron estas plataformas para realizar actos delictivos, es decir, difundir malware con el propósito de secuestrar la información mediante la utilización de estos servicios que presta el gobierno.

Los mecanismos utilizados por los cibercriminales es el uso de correos institucionales con procedencia engañosa utilizando el nombre de entidades del gobierno como: La Fiscalía General de la Nación, el SIMIT y la DIAN su intención es Lamar la atención de los ciudadanos y colaboradores de las mismas entidades, logrando acceder a estos links de procedencia dudosa y enviando mensajes como, por ejemplo: “Invitación a pagar de manera urgente sus Obligaciones.zip”. Este tipo de mensajes logran engañar a los usuarios y proceden a descargar los archivos adjuntos y estos contienen el malware de nombre: “TrojanWin32Xtratmzc” con esta acción el atacante logra acceder al dispositivo y equipo de cómputo en el cual podrá visualizar la información o lo que sucede con el ordenador. [91]

Con este tipo de modalidad de engaño durante el año 2016 se evidencio un incremento del 114.4% en ataques de este tipo en todo el territorio colombiano en comparación al año 2016 con 238 de incidentes reportados. En el año 2017 uno de los primeros análisis que se realizó en materia de cibercrimen en Colombia, donde la Cámara Colombia de Informática y Telecomunicaciones, CCTI, se reportaron falsas ofertas publicitarias en páginas web falsas y correos electrónicos estas eran enviadas a las víctimas con la finalidad que el usuario accediera a ellas y en ese momento el atacante accedía de manera ilícita con la finalidad de hacer hurto de la información y así mismo cobrar una recompensa para ser recuperada dentro de un tiempo limitado. [92]

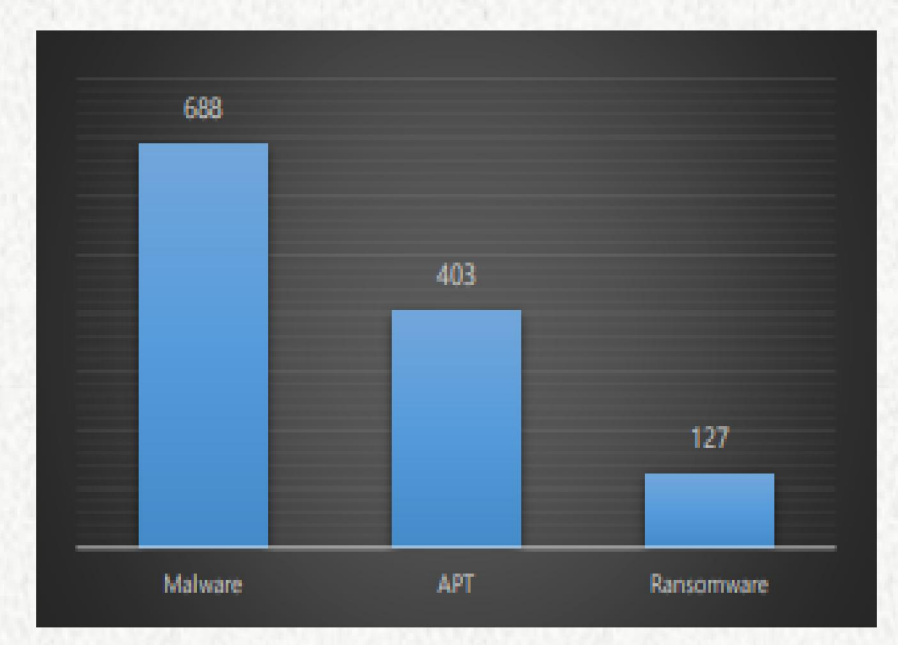
[91] STATISTA. Los pagos de rescate con criptomonedas por ataques ransomware se dispararon en 2020. [Sitio web]. 2021. [Consultado 17 de noviembre 2021]. Disponible en: https://es.statista.com/grafico/25240/valor-total-de-las-criptomonedas-recibidas-por-direcciones-de-ransomware--en-mill-de-dolares-%252A/

[92] EL NUEVO SIGLO. Se disparan denuncias de estafa en plataformas digitales. [Sitio web]. 2017. [Consultado 17 de octubre 2021]. Disponible en: https://www.elnuevosiglo.com.co/articulos/04-2017-se-disparan-denuncias-de-estafa-en-plataformas-digitales

Unos de los atacantes también relevantes en Colombia es el ataque cibernético APT (Amenazas Persistentes Avanzadas), [93] esta modalidad permite al atacante realiza un análisis sobre el objetivo el cual va a hacer atacado utilizando un software malicioso con la finalidad de examinar las vulnerabilidades de los sistemas informáticos. En el año 2015 se reportaron 48 incidentes en relación al año 2016 con 286 incidentes reportados.

En cuando al ataque cibernético Ransomware este tuvo un aumento de ataques del 500% en relación en los años 2016 y 2015 siendo una de las modalidades más utilizadas en cuanto al cibercrimen durante el año 2017, se evidencia un 76% de las infecciones ransomware mediante el engaño de correos electrónicos y spam. Ilustración 6.

Ilustración 9. Ataques más relevantes en Colombia.



Fuente: POLICÍA NACIONAL – Dirección de Investigación Criminal e Interpol Pág. 5. [Consultado el 17 de noviembre 2021]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Teniendo en cuenta la gráfica anterior, los estudios realizados por el Centro Cibernético Policial, se identificó en un incremento del 114.4% relacionados a los ataques Malware en Colombia. De los cuales se reportaron 153 incidentes entre los años de 2015 y 2016

[93] POLICÍA NACIONAL - Dirección Investigación Criminal e Interpol. 2016. Pág.5. 2016. [Consultado el 17 de septiembre 2022]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

un aumento bastante alto a comparación de otros años donde no se evidenciaba este tipo de ataques cibernéticos.

En cuanto a las amenazas APT logra que el delincuente cibernético pueda lograr determinar los objetivos empleando código malicioso para identificar las vulnerabilidades de un sistema donde se reportaron 48 a 286 incidentes en los años del 2015 al 2016. Finalmente, en Ransomware tuvo un incremento del 500% a comparaciones de los años 2015 al 2016, siendo una de las modalidades principales en cuanto a las tendencias de cibercrimen donde se evidencia la modalidad de engaños por medio de correos electrónicos y spam.

5.1 ATAQUE CIBERNÉTICO EN LA ALCALDÍA DE SANTA FE DE ANTIOQUIA.

En 19 de agosto del año 2021, se reportó por la alcaldía de Santa fe de Antioquia se vio afectada por el secuestro de información y el bloqueo de las aplicaciones o servicios de la entidad ocasionado por un ataque cibernético ransomware. esta información fue dada por el director de la unidad de sistemas de información de ese municipio. adicionalmente, se indicó que los atacantes cibernéticos tuvieron el control de la plataforma digital por seis días. esto afecto la suspensión de los servicios a la ciudadanía de forma digital. de acuerdo, a la informado por el alcalde de la ciudad indico que los atacantes cibernéticos exigieron el pago por bitcoins a cambio de recuperarla, debido a que la información correspondía a datos financieros fue necesario congelar las cuentas bancarias del municipio. [94]

Vector de Ataque: La alcaldía de Santa Fe de Antioquia sufrió un ataque llamado BlackCat que corresponde a un ransomware el cual pide rescate para retomar el control de las plataformas. Posible técnica de acceso phishing, el modelo de trabajo de estos ciberdelincuentes se llama ransomware bajo servicio, esto quiere decir, secuestro de información ya que al realizar el ataque cibernético cobro a la víctima un pago, ya que la información encriptada seria devuelta al dueño de la información y esta no sea publicada o revelada a medios electrónicos, porque como se sabe al capturar la información esta corresponde a datos sensibles o datos privados.

Los atacantes cibernéticos logran acceder a la información tomando como primera instancia extorsionar para que la víctima. Ya que el delincuente cibernético realizaría la

[94] INFOBAE. Ciberdelincuentes secuestraron los datos de la alcaldía de Santa Fe de Antioquia. [Sitio web]. 2021. [Consultado 27 de febrero 2023]. Disponible en: https://www.infobae.com/america/colombia/2021/08/19/ciberdelincuentes-secuestraron-los-datos-de-la-alcaldia-de-santa-fe-de-antioquia/

liberación de los equipos de cómputo y la data. El segundo paso que indican los delincuentes cibernéticos es solicitar el pago para liberar la información sensible el cual fue hurtada para así evitar multas a la entidad para que la información no sea difundida públicamente. El tercer paso de los criminales es descubrir la información sensible de terceros para solicitar el rescate de la información ya que ellos amenazan con publicar o filtrar la información identificada en una web oscura.

Los criminales informáticos relacionan el ataque a la Alcaldía Santa Fe de Antioquia a la fecha se desconoce el modus operandi, ya que se desconoce el origen y la manera de como accedieron al sistema y red corporativa. La información dada a los medios de comunicación fue la siguiente, se recibieron correos electrónicos donde les indicaban que debían pagar en criptomonedas y así liberarían la data que estaba encriptada por los delincuentes cibernéticos. [95]

Tipo de afectación: La afectación presentada del ciberataque a la Alcaldía Santa Fe de Antioquia, se identificó que los atacantes cibernéticos lograron mantener el control de las plataformas digitales por seis días, afectando el ingreso de la ciudadanía a la página web. Una de las afectaciones que tuvo este ciberataque fue una de las secretarias de Hacienda, no pudieron expedir copias de las facturas de los impuestos y esto ocasiono que no se lograra realizar de manera digital. Una de las afectaciones que tuvo la entidad fue la inscripción de diferentes procesos como los certificados comerciales. Esto afecto notablemente ya que se tuvieron que expedir las copias de las facturas de los impuestos de manera manual. Ya no tenían la disponibilidad de los servicios y no se podían hacer pagos por pse.[96]

Técnicas utilizadas por los atacantes: Las técnicas utilizadas por los ciberdelincuentes llamados BlackCat quienes son los responsables de acceder a la plataforma y servicios de la Alcaldía Santa Fe de Antioquia, cifrado de información y datos sensibles este grupo de cibercrimen tienen como medida de seguridad, dificultar el descifrado de archivos si están cifrados. El uso de dos algoritmos de cifrado de diferentes y garantía para que la clave de descifrado nunca sea almacenada en la unidad de los archivos cifrados.

---

[95] BLUERADIO. Denuncian que hackers secuestraron información de Alcaldía de Santa Fe; exigen pago con bitcoin. [Sitio web]. 2021. [Consultado 27 de febrero 2023]. Disponible en: https://www.bluradio.com/blu360/antioquia/denuncian-que-hackers-secuestraron-informacion-de-la-alcaldia-de-santa-fe-de-antioquia

[96] EL COLOMBIANO. Hackers secuestraron datos de la Alcaldía de Santa Fe de Antioquia. [Sitio web]. 2021. [Consultado 17 de noviembre 2021]. Disponible en: https://www.elcolombiano.com/antioquia/seguridad/hackers-secuestran-datos-de-alcaldia-de-santa-fe-de-antioquia-EC15421126

Otra técnica utilizada por BlackCat es enviar un correo electrónico a través de un sitio web el cual ha sido una página fraudulenta, luego el malware encripta todos los archivos de la víctima mostrando una alerta indicando que el usuario ha quebrantado las leyes federales produciendo un bloqueo en el equipo de cómputo o dispositivo móvil. Luego de esta notificación, el atacante procede a informarle a la víctima para desbloquear el recurso tecnológico debe pagar el rescate a través de bitcoin o criptomoneda. [97]

Vulnerabilidades: El ataque cibernético que tuvo la Alcaldía Santa Fe de Antioquia se detectó que muchas de las organizaciones en Colombia son blanco atractivo para los criminales cibernéticos dado que no invierten en la seguridad digital y esto lo aprovechan los delincuentes para acceder a la red corporativo y realizar la captura de información de manera no autorizada.

- **Software obsoleto:** Los equipos de cómputo y sistemas de información no cuentan con actualizaciones vigentes, permitiendo brechas de seguridad que logran permitir el acceso no autorizado a datos informáticos, redes corporativas, aplicaciones o dispositivos. La finalidad del intruso es acceder y burlar los mecanismos de seguridad implementados en la entidad.

- **Error humano:** Los errores humanos son los más comunes dado que el personal de una compañía desconoce temas relacionados con ciberseguridad, esto los hace más vulnerables ya que no desconocen los métodos o técnicas utilizadas por los ciberdelincuentes permitiendo el acceso indebido a correos electrónicos o descargar inusuales. Es importante que las organizaciones realicen constantemente capacitaciones relacionadas con ciberataques para proteger los dispositivos, servicios, sistemas de información.

- **Malas prácticas:** Una de las vulnerabilidades más atractivas para los ciberdelincuentes corresponde a la debilidad de las contraseñas utilizadas por los usuarios y esto abre una gran oportunidad para los delincuentes puedan acceder a los sistemas de información. La aceptación de correos electrónicos con proceden delictiva, descargas de software maliciosos y acceso a página no seguras de procedencia maliciosa.[98]

---

[97] PICUSSECURITY. Pandilla de ransomware BlackCat. [Sitio web] 2022. [Consultado 27 de febrero 2023]. Disponible en: https://www.picussecurity.com/resource/black-cat-ransomware-gang

[98] LA NACION. Malas prácticas que ponen en riesgo la seguridad de las cuentas digitales [Sitio web]. 2023. [Consultado 01 octubre 2023]. Disponible: https://www.lanacion.com.ar/tecnologia/dia-de-la-contrasena-tres-malas-practicas-que-ponen-en-riesgo-la-seguridad-de-las-cuentas-digitales-nid04052023/

- **Falta de fortalecimiento en la red corporativa**: Esta vulnerabilidad es atractiva para los delincuentes cibernéticos dado que se evidencia brechas de seguridad en cuanto a la falta auditorías internas y externas, estas deben ser periódicas, falta de implementación de políticas de seguridad, administrar los permisos de los usuarios.[99]

5.2 ATAQUE CIBERNÉTICO EPS SALUD TOTAL.

El pasado domingo 1 de mayo del año 2022, se reportó un ataque cibernético a la entidad de salud total teniendo una afectación en los servicios de la página web afectando en gran manera los servicios de la página web de la oficina virtual, punto de atención desde casa, la aplicación móvil, la entrega de medicamentos. la afectación presentada a la entidad se deshabilito las conexiones de los servidores físicos y virtuales, con el fin de evitar hurto de información, se tomó este protocolo de seguridad logrando asegurar la información de la entidad de salud. según las investigaciones realizadas se identificó el responsable de este ataque quienes se denominan vicesociety. [100]

Vector ataque: El grupo criminal ViceSociety usa el vector de ataque es utilizando métodos como el phishing (envió de correo malicioso), logrando engañar a las víctimas con esta técnica el malware se propaga a la red corporativa. Según la investigación realizada una de los vectores utilizados por estos cibercriminales es la explotación de vulnerabilidades permitiendo realizar la ejecución de código malicioso de forma remota sobre los equipos de cómputo. Realizan la utilización de campañas masivas con el envío de correos malspam o malware spam (utilización de ingeniera social que es engañar a las victimas) estos contienen archivos con software malicioso logrando que las victimas accedan a este de correos y descarguen el archivo con código malicioso.

Tipo de afectación: La afectación presentada a la EPS Salud Total produjo la falla de la plataforma web de la entidad generando la rehabilitación de los servicios negando el acceso a la oficina virtual, la solicitud de medicamentos, realizar la atención inmediata de urgencias, atenciones desde casa y afecto el acceso a la aplicación móvil. La falla presentada fue por muy poco tiempo debido a que los administradores del sistema

[99] NAPIT. Consejos para su empresa evitar problemas con la red corporativa. [Sitio web]. 2023. [Consultado 28 de febrero 2023]. Disponible en: https://www.napit.com.br/es/5-consejos-para-su-empresa-evitar-problemas-con-la-red-corporativa/

[100] INFOBAE. EPS Salud Total suspende servicios virtuales por un ataque informático extremo. [Sitio web]. 2022. [Consultado 4 marzo de 2023]. Disponible en: https://www.infobae.com/america/colombia/2022/05/04/eps-salud-total-suspende-servicios-virtuales-por-un-ataque-informatico-extremo/

detectaron algo inusual en el sistema el cual activaron el protocolo de seguridad logrando deshabilitar la conexión de los servidores de la entidad. [101]

Técnicas utilizadas por los atacantes: Las técnicas utilizadas por los ciberdelincuentes llamados ViceSociety es una de las técnicas utilizadas para lograr acceder a la red, en donde la entidad de Salud Total es vulnerable ya que utilizan el método de la ingeniería social el cual logran persuadir a las victimas logrando engañarlas para tomar datos personales. Otra técnica utilizada es el phishing método por el cual el atacante cibernético realiza un envío de correos electrónicos masivos en el que tiene archivos maliciosos, esta campaña de correos por lo general, se descripción es la extorción a las victimas quienes por temor a represarías acceden a descargar los archivos maliciosos y estos se propagan en el sistema y red corporativa logrando encriptar información sensible y así mismo tomar el control de las aplicaciones y servicios de la entidad.

Vulnerabilidades: La investigación arroja algunas de las vulnerabilidades presentadas en al EPS Salud Total logrando acceder al sistema y es así como lograron atacar los servicios de la entidad.[102]

- **Errores humanos:** Esta vulnerabilidad es muy recurrente en las entidades ya que por lo general es ocasionado por los usuarios quienes por desconocimientos y concientización no toman las medidas preventivas de revisar los accesos a sitios web que están accediendo y la descarga de software sospechoso.

- **Administración y control de permisos:** Esta vulnerabilidad si no es trabaja por los administradores del sistema, sin tener en cuenta que es importante controlar y administrar los permisos y privilegios de los usuarios según su función. Esto impide que los usuarios accedan a sitios con procedencia maliciosa o que realicen descargas de archivos y estos contienen software malicioso, los administradores del sistema no podrían controlar estas acciones ya que no utilizan herramienta que detecten intrusos o anomalías en la red corporativa.

---

[101] SALUDTOTAL. Salud Total EPS-S está siendo objeto de ataque informático externo. [Sitio web]. 2022. [Consultado 4 marzo 2023]. Disponible en: https://saludtotal.com.co/plan-de-beneficios-en-salud/salud-total-eps-s-esta-siendo-objeto-de-ataque-informatico-externo/

[102] INFOBAE. EPS Salud Total suspende servicios virtuales por un ataque informático extremo. [Sitio web]. 2022. [Consultado 4 marzo de 2023]. Disponible en: https://www.infobae.com/america/colombia/2022/05/04/eps-salud-total-suspende-servicios-virtuales-por-un-ataque-informatico-extremo/

- **Falsificación de solicitudes entre sitios:** Esta vulnerabilidad engaña a las víctimas donde se muestra como un usuario autentico con la finalidad de acceder al sitio web ya el usuario desconoce las intenciones maliciosas del intruso. Este método de ingeniera social logra que el usuario proporcione todos los datos personales como contraseñas y credenciales, luego envía una petición a una aplicación web vulnerable.

5.3 ATAQUE CIBERNÉTICO EN LA ENTIDAD DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA (DANE).

El 9 de noviembre del año 2021, la entidad el departamento administrativo nacional de estadística (DANE) la página web fue blanco de un ataque cibernético, donde afecto uno de los servidores de la entidad, este ciberataque afecto varias máquinas donde se identificó la no disponibilidad, generando la denegación del servicio, adicionalmente eliminaron los servidores y las máquinas virtuales de la entidad. al detectar esta situación el personal del área de tecnología realizó la desactivación de la data store, pero lamentablemente el atacante ya había borrado la información, que corresponde a 230 teras de datos de la entidad, la afectación fue bastante critica dado que lograron acceder al correo institucional, se afectaron 420 servidores, daños en la infraestructura tecnológica y la eliminación de backup de información o copias de seguridad. esta situación presentada afecta en gran manera la confidencialidad de la data de la entidad. [103]

Según información dada por los medios de comunicación se notificó que los ciberdelincuentes solicitaron al DANE 25.000 dólares para retornar la información y el restablecimiento de la página web, la información capturada tenia datos relevantes como datos sensibles sobre índices de pobreza, educación, salud, también obtuvieron los datos personales de la población de diferentes territorios del país, entre otros. Adicional a esto, los hackers especializados comenzaron a enviar correos electrónicos a la ciudadanía haciéndose pasar por la entidad, esto género que muchos de los ciudadanos accedieran y proporcionaran información personal, es así, como la entidad realizo un comunicado indicando que los delincuentes cibernéticos se estaban haciendo pasar por la entidad. [104]

---

[103] EL TIEMPO. Así tumbaron la plataforma digital del Dane y exigieron rescate. [Sitio web].2021. [Consultado 17 de noviembre 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/dane-asi-fue-el-hackeo-a-la-plataforma-digital-de-la-entidad-631818

[104] PORTAFOLIO. El DANE fue blanco de un ataque cibernético. [Sitio web]. 2021. [Consultado 25 de febrero 2023]. Disponible en: https://www.portafolio.co/economia/gobierno/dane-fue-blanco-de-hackeo-o-ataque-cibernetico-558379

Estos ataques cibernéticos se incrementaron dado a la nueva modalidad del teletrabajo dado que las aplicaciones y acceso remoto, es una puerta gigante para que los atacantes cibernéticos aprovechan de estas situaciones para que puedan acceder a las plataformas e incluso los accesos a las VPN.

Vector ataque: Una de las hipótesis y previa investigación por parte del DANE, Respuesta ante Emergencias Informáticas, el Centro Cibernético de la Policía Nacional y La Fiscalía General de la Nación informaron la técnica utilizada por los delincuentes cibernéticos fue por ataques denegación de servicio o Ataques DDoS el objetivo de este ataque es bloquear o saturar los servicios de la página web y otra técnica es por phishing (correo electrónico), el cual contenía un enlace malicioso o una segunda teoría fue por un dispositivo extraíble, es decir, una memoria USB. Según la investigación realizada se tiene como certeza que identifico un usuario llamado "Vcenter" y se detectó que tenía permisos de administrador logrando acceder de manera autorizada y sin que fuera detectado comenzó la tarea de copiar la información, para luego realizar la eliminación del sistema. Según el experto en ciberseguridad Andrés Velásquez investigador de seguridad digital y privacidad de la organización Karisma comunico que el ciberdelincuente debió estar varias horas en el sistema ya que logro tomar gran parte de la información a un nivel demasiado alto y que logro vulnerar el sistema sin ser detectado de manera inmediata. [105]

Tipo de afectación: La afectación presentada al Departamento Administrativo Nacional de Estadística presento una falla en la página oficial de la entidad con un tiempo estimado por 10 días, también tuvo una afectación de un servidor de la compañía ocasionando una pérdida de 230 teras de información confidencial. Esta información fue secuestrada y eliminada por los atacantes cibernéticos. Esta situación se dio a conocer un informe más detallado el ex director del Daniel Oviedo indico que los archivos hackeados era gran parte de información de estadística y comandos web que funcionaba en ese entonces 88 servicios de los 275 que presta el DANE no fueron recuperados en su totalidad. [106]

---

[105] ELCOLOMBIANO. El cibersecuestro de datos que tiene en jaque al DANE. [Sitio web]. 2021. [Consultado 25 febrero 2023]. Disponible en: https://www.elcolombiano.com/colombia/secuestro-a-informacion-del-dane-en-colombia-IE16031966

[106] BLURADIO. Denuncia del Dane ante Fiscalía por ataque cibernético: borraron información sensible y confidencial. [Sitio web]. 2021. [Consultado 27 de febrero 2023]. Disponible en: https://www.bluradio.com/nacion/denuncia-del-dane-ante-fiscalia-por-ataque-cibernetico-borraron-informacion-sensible-y-confidencial

Técnicas utilizadas por los atacantes: Las técnicas utilizadas por los ciberdelincuentes que no se ha logrado identificar el nombre de la organización, pero lo que se llevó a cabo la investigación los hackers utilizaron ataques DDos cuyo objetivo es saturar los servicios logrando inhabilitar la página logrando que ningún usuario pueda acceder a ella. Adicional a ello, el DANE advirtió a la ciudadanía hicieran caso omiso a una serie de correos electrónicos y mensajes de texto de los cuales se estaba haciendo pasar por funcionarios de la entidad, cometiendo delito de suplantación de identidad. Este crimen informático es sancionable según el artículo 269G de la Ley 1273 del 2009. Para el DANE se deja un temor colectivo por el robo de información ya que está en manos de delincuentes cibernéticos que pueden utilizar estos datos para realizar ingeniería social, estafas, suplantación de identidad, entre otros delitos.[107]

Vulnerabilidades: El Departamento Administrativo Nacional de Estadística al detectar las vulnerabilidades detectadas en el ataque que sufrió la entidad, debilidad en los sistemas de información y la infraestructura TI.[108]

- **Sistemas débiles:** Los ciberdelincientes aprovechan los sistemas y aplicaciones no actualizados o parcheados siendo un atractivo para tomar esta vulnerabilidad y aprovechar la oportunidad para acceder de manera no autorizada.

- **Tecnología obsoleta:** Todos los recursos tecnológicos y sistema de información como aplicaciones, sistemas operativos y demás recurso deben mantenerse actualizada periódicamente y estar al día con la nueva tecnología que esté vigente en el momento.

- **Fortalecer la seguridad en la red corporativa**: Los atacantes evidencia una red vulnerable ya que no cuenta con políticas establecidas que aseguren el fortalecimiento de la red, ausencia de contraseñas de fácil detección, debilidad en auditorias periódicas y falta de control en los permisos adquiridos a los usuarios.[109]

---

[107] BLURADIO. Denuncia del Dane ante Fiscalía por ataque cibernético: borraron información sensible y confidencial. [Sitio web]. 2021. [Consultado 27 de febrero 2023]. Disponible en: https://www.bluradio.com/nacion/denuncia-del-dane-ante-fiscalia-por-ataque-cibernetico-borraron-informacion-sensible-y-confidencial

[108] BUENO MUNAR, Laura Daniela. Ciberseguridad en Colombia, avances y retos. p.13. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/41303/BuenoMunarLauraDaniela2022.pdf.pdf?sequence=2&isAllowed=y

[109] ITECHSAS. Cómo mejorar la seguridad de la red empresarial. [Sitio web]. 2019. [Consultado 2 octubre 2023] Disponible: https://www.itechsas.com/blog/ciberseguridad/mejorar-la-seguridad-de-la-red-empresarial/

- **Cross Site Scripting:** Los atacantes ingresan scripts en las páginas web legitimas afectadas y estas son navegadas por los usuarios quienes por desconocimiento ingresan las credenciales y contraseñas al sitio web no legitimo logrando hurtar los datos ingresados por las víctimas.

- **Puertos de red abiertos:** Los delincuentes realizan un escaneo a la red corporativa en el que logran detectar la existencia de puertos abiertos y estos no tienen ningún control por parte del administrador del sistema y tampoco existe una administración del mismos. Los permisos o privilegios se deben establecer por la entidad.

- **Contraseñas de fácil acceso:** Por lo general, los atacantes lo primero que empiezan a indagar son las contraseñas, logrando así acceder a una de ellos ya que las contraseñas tienen parámetros muy básicos y de fácil acceso para acceder a la red corporativo, aplicaciones, servidores, entre otros.

5.4 ATAQUE CIBERNÉTICO A LA UNIVERSIDAD JAVERIANA

El pasado miércoles 23 de noviembre del 2021 indicaron que fueron víctimas de un ataque cibernético por el grupo criminal vicesociety. la universidad javeriana al detectar anomalías en la página oficial procedió a suspender los servicios que se prestan en este sitio web. según lo indicado por la universidad los sucesos presentados fueron en medio de los exámenes finales generando inconvenientes en la prestación de servicios. es así, que la universidad procedió a tomar los protocolos de seguridad para este tipo de ataques cibernéticos que se realizan de forma rápida y oportuna, deshabilitando los servicios para no tener afectaciones en los servicios tecnológicos para proteger la información de la universidad y la operación del sistema. según los medios de comunicación y ente investigativo informaron que las sedes de Cali y Bogotá fueron las que tuvieron afectación debido al ataque cibernético.[110]

Gracias al sistema core implementado por la universidad los ciberdelincuentes no lograron afectar la información sensible como el registro académico, información financiera y gestión administrativa ya que están protegidos por el sistema de seguridad diseñado por la universidad.

[110] INFOBAE. Universidad Javeriana confirmó que fue víctima de un ataque cibernético. [Sitio web]. 2021. [Consultado 4 marzo 2023]. Disponible en: https://www.infobae.com/america/colombia/2021/11/23/universidad-javeriana-confirmo-que-fue-victima-de-un-ataque-cibernetico/

Vector ataque: Según las investigaciones realizadas por la fiscalía y expertos de ciberseguridad de la universidad Javeriana identificaron el vector de ataque de la organización criminal ViceSociety hacen la utilización de ransomware as a service (RaaS) quienes desarrollan software malicioso para encriptar información robusta y llegar al punto de denegar los accesos a las diferentes plataformas y servicios. Esta técnica la utilizan con la finalidad de poner en venta la información capturada y de esta manera cualquier usuario pueda realizar la comprar de la información para obtenerla y hacer delitos en contra de la organización que en este caso es la universidad. Estos grupos delincuenciales tienen como estrategia enviar correos electrónicos a las víctimas a través de técnicas como phishing logrando infectar el equipo o dispositivo de la víctima, con el fin que se propague el malware por toda la red corporativa realizando la encriptación de los archivos de la compañía. Esa es la manera en como los atacantes utilizan este tipo de vulnerabilidades aprovechándose del desconocimiento de las víctimas en cuando a ciberseguridad. [111]

Tipo de afectación: El ataque cibernético sufrió las afectaciones de los servicios utilizados en la página web de la universidad se identificaron fallas en las sedes de Cali y Bogotá. Los servicios más afectados fueron el ingreso del registro académico, la visualización de la información financiera y administrativa no había disponibilidad de estos servicios ya que hubo una indisponibilidad para acceder a lo indicado anteriormente.

Técnicas utilizadas por los atacantes: La investigación realizada por los expertos de ciberseguridad de la universidad es que los atacantes utilizaron técnicas de ingeniera social utilizando el método de phishing (envió de correo electrónico para estudiantes, personal administrativo o docentes), donde se adjunta el software malicioso y este tiene contenido engañoso logrando que las victimas logren ingresar al link o realizar la descarga de los archivos malicioso, con la finalidad que el malware se propague por toda la red corporativa y este realice una búsqueda de información sensible y proceda a encriptarla y así mismo lograr deshabilitar los servicios o página web de la universidad para denegar los servicios obstaculizando el acceso a los usuarios y administradores del sistema para que logren perder el control de los mismos. [112]

---

[111] SEMANA. La Universidad Javeriana confirma que sufrió ataque informático en Bogotá y Cali. [Sitio web]. 2021. [Consultado 4 marzo 2023]. Disponible en: https://www.semana.com/nacion/articulo/la-universidad-javeriana-confirma-que-sufrio-ataque-informatico-en-bogota-y-cali/202153/

[112] PROTECCIONDATOS. [Sitio web]. 2021. [Consultado 4 marzo de 2023]. Disponible en: https://protecciondatos-lopd.com/empresas/ransomware-as-a-service-raas/

Vulnerabilidades: La investigación realizada a la universidad javeriana se identificó los factores que lograron los hackers el lograr acceder a la red corporativa de la universidad, el desconocimiento de temas relacionados en ciberseguridad, muchos de los usuarios se limitan a la utilización de los recursos sin tener en cuenta que están en constante peligro ya que existen muchas organizaciones criminales que están al acecho y así mismo aprovechas cualquier vulnerabilidad que se presente. Es por esta razón que se detectó estas vulnerabilidades en la red corporativa de la universidad.

- **Inadecuada gestión y protección de contraseñas:** Se ha evidencia que los usuarios no utilizan contraseñas más seguras, la universidad debe implementar políticas de seguridad para el acceso al sistema y estas deben cumplir ciertos parámetros específicos para que sea más difícil la detección de contraseñas según las técnicas implementadas por los hackers.[113]

- **Falta de controles de seguridad:** Al no tener políticas de seguridad establecidas por la universidad, esto abre una brecha de seguridad en la red permitiendo el acceso a intrusos en la red, accediendo de manera no autorizadas y esto les permitirá acceder a la información y tomar control de la infraestructura de la compañía. Esta vulnerabilidad es altamente accesible para los ciberdelincuentes.

- **Falta de formación a los usuarios en temas relacionados con ciberseguridad:** La falta de conocimiento en cuanto a ciberseguridad es muy importante para que los usuarios estén enterados sobre los métodos utilizados por los delincuentes cibernéticos, esto evitaría en gran manera sean persuadidos por los atacantes ya que tendrán los conocimientos necesarios, y esto evitaría que ingresen al sistema de manera no autorizada.

- **Ausencia de sistemas de identificación y autenticación:** La falta de fortalecer los métodos de acceso a los sistemas de información y los recursos tecnológicos hace que la identificación y autenticación de credenciales se vena débiles y vulnerables para los atacantes. De esta manera, se implementaría políticas de seguridad más robustas que logren proteger los accesos indebidos y sean más difíciles de detectar por los ciberdelincuentes.

[113] INFOBAE. Hackeo al Senado: el grupo de ciberdelincuentes Vice Society filtró 30 mil archivos. [Sitio web]. 2022. [Consultado 4 marzo 2023]. Disponible en: https://www.infobae.com/tecno/2022/03/14/hackeo-al-senado-el-grupo-de-ciberdelincuentes-vice-society-filtro-30-mil-archivos/

- **Descargas o accesos de internet no controladas**: Se evidencia la falta de controles y la administración de permisos, el cual se debe tener en cuenta la gestión, cargo o funciones de los usuarios. Ya que al establecer herramientas y antivirus que controlen el tráfico de red, permite el fortalecimiento de red corporativo. Esto evitaría accesos indebidos, también es importante realizar escaneo de red e implementar herramientas que permitan detectar las vulnerabilidades del sistema.

5.5 ATAQUE CIBERNÉTICO A LA PÁGINA WEB DEL INVIMA.

El 3 de octubre del año 2022, el instituto nacional de vigilancia de medicamentos y alimentos (INVIMA). se reportó un ataque cibernético en la entidad en la página web de la entidad en el que se afectó la disponibilidad de información, también afecto las aplicaciones externas de la entidad. la amenaza provocada deshabilitó la plataforma del instituto, se afectaron también los servidores físicos y virtuales.

Este es el segundo ataque que presentó esta entidad dado que en el mes de febrero se evidencio la misma afectación a los servicios indicadores anteriormente. Estas situaciones presentadas son alarmantes para la entidad es así, que es importante implementas estrategias y fortalecer los recursos tecnológicos para mitigar este tipo de ataques. [114]

Vector ataque: El grupo delincuencial cibernético logro vulnerar la red corporativo del INVIMA accediendo sin autorización cuyo objetivo es hurtar información y cifrar dispositivos. Una de las técnicas asociadas es ofrecer ransomware “as a Service (RaaS)”, cifrando los archivos y comprometiendo maquinas con Windows, afectando servidores físicos y virtuales. Utilización del método de Phisihing (campaña de envió de correos desde el dominio oficial de la entidad). Debido que en el primer ataque cibernético que sufrió la entidad para lograr el restablecimiento de los servicios tardo 30 días. El método que estaba utilizando los atacantes es la extorción a funcionarios de la entidad y de otras entidades gubernamentales. Todo el personal estaba vinculado por la entidad y que tienen relaciones en el exterior también fueron extorsionados. [115]

---

[114] INFOBAE. Ataque cibernético a página web del INVIMA tiene en vilo información y aplicativos internos del instituto. [Sitio web]. 2020. [Consultado 1 de noviembre 2022]. Disponible en: https://www.infobae.com/america/colombia/2022/10/04/ataque-cibernetico-a-pagina-web-del-invima-tiene-en-vilo-informacion-y-aplicativos-internos-del-instituto/

[115] CONSULTORSALUD. El INVIMA es objeto de nuevo ataque cibernético. [Sitio Web]. 2022. [Consultado 1 de marzo 2023]. Disponible en: https://consultorsalud.com/invima-objeto-ataque-cibernetico/

Tipo de afectación: La afectación presentada al Instituto Nacional de Vigilancia de Medicamentos y Alimentos presento fallas en el portal web del INVIMA, los servidores virtuales y físicos fueron deshabilitados, dado al ataque cibernético presentado a la entidad, como también se vieron afectados los certificados de exportación e importación y ventanilla única de comercio exterior, los servicios la importación de medicamentos vitales y la liberación de los lotes. Adicional a esta situación presentada el gremio de la salud como los laboratorios farmacéuticos, la Asociación Nacional de Exportadores, la Cámara de Comercio Colombo Americana fueron afectados debido a la situación que se presentó en el INVIMA ya que genero entregas importantes para las entidades anteriormente nombradas. [116]

Técnicas utilizadas por los atacantes: Las técnicas utilizadas por los ciberdelincuentes llamados BlackBye quienes generaron un virus informático llamado ransomware blackbyte capturando la información el cual pidieron un rescate por la recuperación de dicha información. Los hackers se aprovechan de las debilidades y vulnerabilidades de las páginas web en cuanto a la seguridad que deben implementar utilizando a las herramientas de detección de vulnerabilidades para tener acceso a la infraestructura tecnológica, debilitar y bloquear los servicios, acceder a la información sensible de la entidad, para así lograr su objetivo.

Blackbyte es un método que se presenta como un servicio legítimo, pero en realidad es un tercero que realiza solicitudes para hacer el secuestro de la infraestructura corporativa para solicitar una recompensa y realizar el pago.

Vulnerabilidades: Para el Instituto Nacional de Vigilancia de Medicamentos y Alimentos (INVIMA), los atacantes cibernéticos rastrean debilidades en el sistema o red corporativo, es donde se aprovechan de acceder a la infraestructura TI.

- **Falencias de parchado:** Los atacantes se aprovechan de cada situación que esté sucediendo en la infraestructura TI, cuando se detecta que faltan actualizaciones en las aplicaciones o sistemas de información, equipos de cómputo, u otros dispositivos, abre una brecha de seguridad dejando vulnerable la red corporativa y este es un atractivo para los delincuentes cibernéticos.

[116] RCNRADIO. Con virus informático Blackbyte fue atacada la página del INVIMA. [sitio web]. 2022. [consultado 28 de febrero 2023]. disponible en: https://www.rcnradio.com/tecnologia/con-virus-informatico-blackbyte-fue-atacada-la-pagina-del-invima

- **Detección de fallas o errores en el software o servicios:** Se detecta algún componente de la red está funcionando de forma incorrecta, este tipo de vulnerabilidades son detectadas por los ciberdelincuentes de esta manera logran acceder usan técnicas de DDoS denegando el servicio o la red corporativa colapsando el trafico malintencionado para que su funcionamiento arroje errores y no logre funcionar.

- **Malas prácticas con el manejo del recurso tecnológico:** Se pueden generar vulnerabilidades con estas prácticas cuando los usuarios realizan la apertura de archivos o link de procedencia malintencionada, publicidad engañosa con estas técnicas de las cuales las denominadas ataques phishing logran suplantar compañías haciendo creer a las víctimas que son verídicas, se debe tener más control sobre estas prácticas para evitar ser detectadas con personal malicioso.

5.6 ATAQUE CIBERNÉTICO EPM MEDELLÍN.

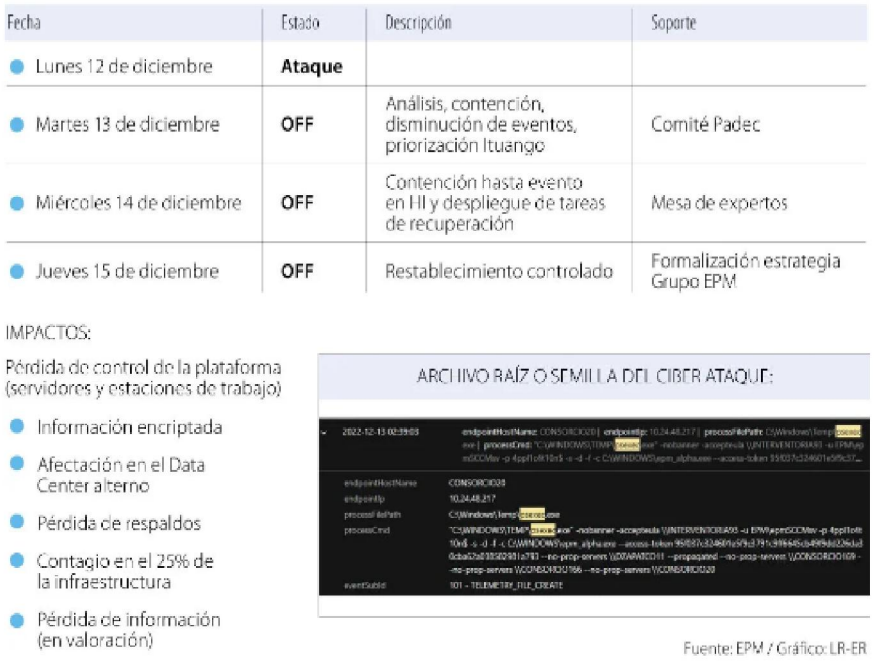
El 13 de diciembre del 2022 la compañía empresas públicas de Medellín EPM, anunció que se vio afectado por un ataque cibernético el cual fue víctima. EMP anuncio la afectación de los servicios las oficinas y los canales virtuales del servicio al cliente no estaban disponibles el cual no permitió el acceso y la prestación de los servicios públicos. la organización cibercriminal llamada blackcat realizo un ataque cibernético afectando los servicios de EMP el cual publico información confidencial de la compañía, información referente a los usuarios de la compañía. en su momento la entidad pública indico la labor que estaba realizando para lograr establecer todos los servicios públicos, iniciando una contención para lograr la estabilidad y recuperación de la plataforma tecnológica. sobre este hecho empezó a circular una información de cuatro archivos donde se evidencio información hurtada y que le corresponde a EMP, esta información comenzó a circular por un sitio web llamado “Deep Web”. [117]

Alrededor de 35.000 clientes de energía prepago fueron los más afectados por este ciberataque, ya que no lograban acceder a la plataforma con el fin de realizar pagos de facturas, realizar recargas de energía prepago o revisar información requerida de la compañía.

[117] ELTIEMPO. Medellín este es el grupo que se adjudicó el ataque cibernético EPM. [Sitio Web]. 2022. [Consultado 27 febrero 2023]. Disponible en: https://www.eltiempo.com/colombia/medellin/blackcat-el-grupo-que-se-adjudico-el-ataque-cibernetico-a-epm-729363

Según la investigación realizada por expertos en ciberseguridad la compañía perdió el control de la plataforma, se detectó que se desencriptó la información de la compañía que tuvo una afectación en el Data Center alterno y se analizó un contagio del 25% de la infraestructura. EPM se apoyó para la realización de la evaluación de los hechos presentado del ciberataque en colaboración de empresas como IBM, Indra, Microsoft y con el apoyo de la Fiscalía General de la Nación. Se identificó las pruebas recopiladas se lograron establecer que el ataque se difundió en las instalaciones de la empresa EPM de la nueva sede Central Ituango.[118] La investigación realizada detecto que el ataque se dio a servidores que se llama consorcio que puso en peligro la entrega de la energía prepago, el objetivo de este ataque era evitar la puesta en marcha de la central. A continuación, se describe la línea de ataque que se presentó en la entidad pública EPM. Ilustración 7.

Ilustración 10. Línea de taque EPM.



Fuente: LA REPUBLICA. Ataque cibernético que EPM sufrió esta semana se dio desde la Central de Ituango. 2022. [Consultado 27 de febrero 2023]. Disponible en: https://www.larepublica.co/empresas/ataque-cibernetico-que-epm-sufrio-esta-semana-se-dio-desde-la-central-de-ituango-3510139

[118] INFOBAE. EPM anunció que está bajo ataque cibernético. [Sitio web]. 2022. [Consultado 1 octubre 2023]. Disponible: https://www.infobae.com/america/colombia/2022/12/13/epm-anuncio-que-esta-bajo-ataque-cibernetico/

Con el análisis e investigación en el que se vio afectada EPM Medellín por el ataque cibernético que sufrió se puede evidenciar tuvo una gran afectación bastante alta en su infraestructura perdiendo el control de la plataforma como equipos de cómputo y servidores. Afectando en gran manera el Data Center Alterno los delincuentes realizaron un contagio del 25% de la infraestructura TI sufriendo una pérdida de información sensible y confidencial de la entidad. Adicional a esto se evidencio perdida de respaldos siendo uno de los golpes más fuertes que tuvo esta organización, poniendo en riesgo los clientes a quienes actualmente se presta servicios públicos vitales para la sociedad.[119]

Vector ataque: El grupo delincuencial cibernético su método de ataque es generar caos y disrupción en todas las operaciones de la entidad al mismo tiempo al momento de acceder a la red corporativa de la entidad ejecutando diversos malware en simultaneo. [120]

En este caso, se afectó el sistema con cuatro tipos de malware. Según la investigación se identificaron los siguientes malware Crypters que consiste descargar malware y este procede a ocultarse para que el antivirus no lo detecte, también logra encriptar los archivos. El malware Infostealers tomo la información sensible y confidencial en el que comercializo en plataformas públicas y foros desde la DeepWeb, logrando extorsionar a las víctimas o terceros de la entidad indicando que la información será publicada.

También se detectó malware llamado Criptominers es utilizado para tomar uno de los equipos de cómputo que este afectado por el malware y proceden a realizar el minado de criptomonedas. Y, por último, se identificó Wipers software malicioso que procede a realizar el borrado de la información o bloquea el acceso a la información de la organización logrando así la afectación de las operaciones de la entidad. [121]

Tipo de afectación: La investigación dada por los medios de comunicación sobre el ciberataque de la EPM de Medellín presentó una afectación se identificó un ransomware en uno de los servidores internos de la entidad con el nombre “Consorcio20”, teniendo un impacto de sobre la pérdida de control de la página web de la compañía el cual fue

[119] LA REPUBLICA. Ataque cibernético que EPM sufrió esta semana se dio desde la Central de Ituango. 2022. [Consultado 27 de febrero 2023]. Disponible en: https://www.larepublica.co/empresas/ataque-cibernetico-que-epm-sufrio-esta-semana-se-dio-desde-la-central-de-ituango-3510139

[120] ELTIEMPO. Medellín: Este es el grupo que se adjudicó el ataque cibernético a EPM. [Sitio web]. 2022. [Consultado 01 marzo 2023]. Disponible en: https://muchohacker.lol/2022/12/grupo-blackcat-alphv-publica-pruebas-de-ataque-ransomware-a-epm/

[121] TELEANTIOQUIA. Avanza investigación por hackeo a EPM. [Sitio web].2022. [Consultado 04 marzo 2023]. Disponible en: https://www.teleantioquia.co/noticias/avanza-investigacion-por-hackeo-a-epm/

encriptada, afectando el Data Center Alterna, propagándose el virus con el 25% de la infraestructura y perdida de información, dejando por completo inhabilitada la página web de la entidad. [122]

Técnicas utilizadas por los atacantes: Las técnicas utilizadas por los ciberdelincuentes llamados BlackCat logran acceder al sistema, los atacantes cibernéticos enviaron un mensaje en el que indicaba que todos los archivos importantes de la entidad fueron encriptados y tendrían una extensión llamada: "8upt97g". Luego de esta acción indicaron que la data podría ser recuperada, pero tendrías que seguir ciertas instrucciones. El hurto de la información confidencial de la compañía, tenía datos personales de los funcionarios de la entidad. Indicaron que se tomaron datos como: reportes anules, pagos, clientes, estados financieros y bancarios, entre otros. El modus operandi de BlackCat es acceder al sistema y propagar el ransomware su técnica es hurtar la información de las organizaciones. Luego se sube a un servidor controlado por los delincuentes, después de alojar la información comienzan a encriptar, según la investigación dada por la compañía de ciberseguridad CronUp informo que los atacantes operan en Chile ya que según el rastreo que realizaron, el servidor está alojado en ese lugar. El 10 de diciembre se identificó que los delincuentes cibernéticos copiaron la información en ese momento, luego de varios días después que se conociera la noticia del ataque, la información ya estaba traslada a ese servidor. Toda la información que se tomó con cada una de las maquinas que lograron tener acceso de EPM, las máquinas tenían el nombre de: "EMP-att100", ellos lograron acceder a la carpeta que visualizaron toda la información de la compañía. [123]

Vulnerabilidades: Según las investigaciones y seguimientos que se ha realizado durante el ataque cibernético que tuvo la entidad se evidencia una de las posibles fallas en el sistema, logrando que los delincuentes accedieran al sistema de esa manera.

---

[122] INFOBAE. EPM anunció que está bajo ataque cibernético. [Sitio web]. 2022. [Consultado 28 febrero 2023]. Disponible en: https://www.infobae.com/america/colombia/2022/12/13/epm-anuncio-que-esta-bajo-ataque-cibernetico/

[123] INFOBAE. Grupo de ciberdelincuentes "BlackCat" reconoce el ataque a EPM y comienza a filtrar información. [Sitio web]. 2023. [Consultado 14 octubre 2023]. Disponible: https://www.infobae.com/america/colombia/2022/12/27/grupo-de-ciberdelincuentes-blackcat-reconoce-el-ataque-a-epm-y-comienza-a-filtrar-informacion/

- **Falta de protección en la red (Firewall):** Se evidencio en la investigación realizada y según lo indicado por los expertos en seguridad, lo hacker detectaron el firewall no estaba con las condiciones, políticas de seguridad establecidas, al parecer no tenía la seguridad correspondiente el cual impediría el ciberataque y esta fue la oportunidad perfecta para acceder a la red sin que fueran detectados. [124]

- **Falta de expertos en ciberseguridad:** Es importante reforzar la seguridad informática y la infraestructura, es decir, mantenerse actualizados en cuanto al campo de la seguridad informática. Al no contar con personal especializado sería más frecuentes los ataques cibernéticos ya que no se implementaría técnicas de protección y realizar seguimiento contante fortaleciendo las reglas en el firewall, escaneo de vulnerabilidades y auditorias periódicas para identificar las debilidades de la infraestructura. [125]

- **Deficiencias en las configuraciones de red y seguridad:** Las configuraciones realizadas sobre las tecnológicas que están disponibles en la entidad no se configuran adecuadamente esto puede crear brechas de seguridad, permitiendo el acceso a cualquier usuario que este navegando en la red. Por ello, es importante que la entidad establezca y defina políticas de seguridad objetivas y especificar las reglas para cada configuración de los dispositivos, servidores, equipos de cómputo, entre otros, estas deben ser consultadas periódicamente.[126]

[124] ELTIEMPO. Expertos hablan sobre la gravedad y riesgos del ciberataque que sufrió EPM. [Sitio web]. 2022. [Consultado 3 marzo 2023]. Disponible en: https://www.eltiempo.com/colombia/medellin/medellin-la-gravedad-y-riesgos-del-ciberataque-que-sufrio-epm-729517

[125] CYREBRO. Cómo evitar que la falta de expertos en ciberseguridad le frene. [Sitio web]. 2023. [Consulta 10 mayo 2023]. Disponible: https://www.cyrebro.io/es/blog/como-evitar-que-la-falta-de-expertos-en-ciberseguridad-le-frene/

[126] Blockbit. ¿Cuáles son los principales problemas de seguridad de red hoy? [Sitio web]. 2023. [Consultado 5 mayo 2023]. Disponible; https://www.blockbit.com/es/blog/cuales-son-los-principales-problemas-de-seguridad-de-red-hoy/

5.7 ATAQUE CIBERNÉTICO EPS SANITAS "KERALTY".

El pasado 28 de noviembre del 2022, se reportó a los medios de comunicación sobre la afectación que sufrió la EPS Sanitas "keralty" según lo informado se indicó que la organización criminal llamada ransomhouse procedieron a hurtar información sensible de la compañía, obteniendo de manera no autorizada los datos que corresponden a historias clínicas, los datos personales de pacientes y empleados de la compañía, los estados financieros fue otra información tomada por los delincuentes cibernéticos, también afectaron la asignación de medicamentos. tuvieron un total de información de 0,7 teras de información institucional de Keralty. en su momento esta organización criminal publico la data de la compañía como: presupuestos, balances, estados financieros e información sensible y personal. esta situación, afecto en gran manera la compañía el acceso a la salud se vio afectada en más de cinco millones de pacientes, la atención oportuna a los pacientes ya que no podían acceder a la historia clínica de los pacientes y afecto en gran manera la asignación de medicamentos.[127]

Vector ataque: El grupo cibernético RansomHouse tomo como técnica enviar correos donde se utilizó un código malicioso y según las investigaciones se identificó que fue enviado por medio de un acceso vulnerable, es decir, la identificación de una contraseña débil suministrada por un usuario que accedió a la VPN. La organización criminal logro acceder a la red corporativa sin ser detectada y procedió a tomar el control de los servicios, servidores y el hurto de la información confidencial generan un gran impacto en el sistema de la organización. Este ataque lo podemos llamar DDos generando la denegación del servicio, enviando solicitudes simultaneas al recurso web logrando desbordar la capacidad de la página web administrar varias solicitudes y evitar que funcione el sistema correctamente. [128]

Tipo de afectación: Para compañía Keralty tuvo una afectación debido al ciberataque en los sitios web y las operaciones de la EPS como los servicios de medicina prepagada, Colsanitas. El ataque proporcionado afecta a gran parte de la línea medica como la red internacional de doce hospitales y un total de 371 centros médicos donde se operaban varios países de Latino América, Asia, Estados Unidos y España interrumpiendo la

[127] BLOOMBERGLINEA. ¿Por qué hay una ola de ciberataques en Colombia y el país está tan vulnerable? [Sitio web]. 2023. [Consultado 4 marzo 2023]. Disponible en: https://www.bloomberglinea.com/2023/01/25/por-que-hay-una-ola-de-ciberataques-en-colombia-y-el-pais-aun-es-tan-vulnerable/

[128] CIBERTIP. Los hackers atacan al sistema de salud de Colombia con Ransomware. [Sitio web]. 2022.[Consultado 4 marzo 2023]. Disponible en: https://www.cibertip.com/hacking-incidentes/los-hackers-atacan-al-sistema-de-salud-de-colombia-con-ransomware/

atención prioritaria médica. Se evidencio en gran manera el hurto de la información de la compañía, personal de la empresa, información de proveedores. [129]

Técnicas utilizadas por los atacantes: Las técnicas utilizadas por los ciberdelincuentes llamados RansomHouse detectaron las vulnerabilidades presentadas en el sistema de la EPS según las investigaciones proporcionadas se detectó una contraseña débil donde el ciberdelincuente logra descubrirla, situación en la cual le permite acceder a la red sin ser detectado teniendo en cuenta que era el acceso de la víctima que tenía la clave de fácil detección, procede con la propagación del malware filtrándose en los dispositivos y recursos de la organización, logrando debilitar la red y ejerciendo el control de la red y demás servicios de la EPS. Realizaron un rastreo de la información sensible de la compañía procediendo a encriptar para solicitar los directores y personal importante de la empresa realizando un envío de mensajes de correo donde el contenido indico la extorción y amenaza de publicar la información obtenida por el hacker, con la finalidad de obtener una remuneración económica y lograr el objetivo de obtener dinero a cambio de realizar el desbloqueo del sitio web y la devolución de la información sensible. [130]

Vulnerabilidades: Con la identificación de las vulnerabilidades presentadas en la red corporativa de la EPS Sanitas, fortalecimiento en la red e implementación de herramientas que permitan reforzar la seguridad de la red y los servicios de la compañía. Adicional a ello, se identificó contraseñas débiles por parte de los usuarios, vulnerabilidad altamente atractiva para los ciberdelincuentes.

- **Contraseñas débiles:** Al utilizar contraseñas cortas donde no se implementen parámetros definidos por la organización o donde no este establecido una política d seguridad. Esto abre una brecha de seguridad que permitirá la identificación y acceso a la red. Los atacantes cibernéticos escanean e implementan técnicas de detección de contraseñas logrado tomar la información privada por las víctimas y logran acceder a los servicios y red corporativa de la compañía.

[129] LA FM. Keralty aseguró que se ha visto afectada la confidencialidad de datos de algunas personas tras ciberataque. [Sitio web]. 2022. [Consultado 04 marzo 2022]. Disponible en: https://www.lafm.com.co/colombia/keralty-aseguro-que-se-ha-visto-afectada-la-confidencialidad-de-datos-de-algunas-personas

[130] VIRTUAL UNIMINUTO. ¿Qué tipo de profesionales podían evitar el ciberataque a Keralty? [Sitio web]. 2022. [Consultado 4 marzo 2023]. Disponible en: https://virtual.uniminuto.edu/blog/que-tipo-de-profesionales-podian-evitar-el-ciberataque-a-keralty/?cn-reloaded=1

- **Accesos indebidos en la VPN:** Los servidores VPN permiten el tráfico de red en el cual permitirá los envíos de datos sensibles y confidenciales de las organizaciones. Es así, como se debe implementar el cifrado de datos el cual permitirá tener la conectividad con el equipo de cómputo personal a la red corporativa de la organización a través de un servidor remoto, crear reglas de políticas de seguridad desde el firewall. Estos accesos son atractivos para los ciberdelincuentes si evidencia alguna falla en la red. [131]

- **Vulnerabilidad servidores:** Se identifica la debilidad que tiene la red dado que no se implementaron políticas de seguridad ni herramientas para el fortalecimiento de la red. Como la detección de inclusos en la red corporativa ya que se debe controlar, administrar los permisos, privilegios y control de accesos.

- **Errores en la gestión de recursos:** Se evidencio esta vulnerabilidad en cuanto al parchado de aplicaciones y servicios, no se mantienen de manera periódica las actualizaciones correspondientes en los dispositivos, equipos de cómputo, sistemas operativos, servidores, aplicaciones y servicios utilizados por la entidad.

5.8 ATAQUE CIBERNÉTICO A LA ALCALDÍA DE MEDELLÍN.

La entidad estatal reporto a los medios de comunicación que el pasado miércoles 1 de febrero del 2023 fueron víctimas de un ciberataque y fue identificado por la organización criminal llamada lockbit quienes accedieron al sistema integrado de emergencias y seguridad (SIESM). durante la investigación realizada en donde se informó que se presentaron fallas en los servidores afectando los servicios, sobre la recepción llamadas de emergencia de la línea 123, estas no se lograron registrar en el sistema. durante el ataque cibernético se identificó que los hackers lograron acceder a la información personal, también accedieron a 11 agencias del sistema de emergencias del distrito. por supuesto fue una situación crítica ya que solicitaron el rescate de la información hurtada. los ciberdelincuentes tomaron pantallazos de la información y estos fueron difundidos por el sitio web: “Deep Web”. el ataque realizado a la alcaldía de Medellín se reportó que fue instalado el ransomware lockbit en el que se ingresó al sistema y red corporativa.[132]

---

[131] PORTAL CCI ENTEL. El Ransomware Ransomhouse compromete el sistema de Salud Keralty de Colombia. [Sitio web]. 2022. [Consultado 4 marzo 2023]. Disponible en: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1436/

[132] ELCOLOMBIANO. Filtran información del ciberataque a línea de emergencias de Medellín: hackers estarían pidiendo rescate a la Alcaldía. [Sitio web]. 2023. [Consultado 6 febrero 2023]. Disponible en: https://www.elcolombiano.com/antioquia/filtran-informacion-del-ataque-al-123-de-medellin-KJ20293595

Vector ataque: El grupo cibernético Lockbit utilizo como técnicas de ataque para la alcaldía de Medellín ingreso al sistema con el método phishing enviando por correo electrónico un sitio web al momento en que la víctima accede al link lo direcciona a una página web fraudulenta y este procede a descarga el archivo con el código malicioso, se utilizó otra técnica realizan campañas de spam donde se incluye herramientas de activación de software instalándose en el sistema y así procede a propagar archivos infecciosos para lograr apoderarse del sistema. [133]

Tipo de afectación: La afectación presentada a la Alcaldía de Medellín se presentó fallas en los servidores de Sistema Integrado de Emergencias y Seguridad de Medellín (SIESM), los hackers lograron tomar pantallazos de la información de la entidad como información personal y 11 agencias del sistema integrado del distrito sobre este hecho los delincuentes cibernéticos pidieron un rescate por la información tomada por ellos sea recuperada y esta no se haga publica en el portal Deep Web. Durante este ataque los servicios de la Alcaldía en este caso las agencias de seguridad y emergencias no se logró ingresar los casos presentados en el momento a través de la 123. [134]

Técnicas utilizadas por los atacantes: Las técnicas utilizadas por los ciberdelincuentes llamados Lockbit su objetivo es operar bajo el modelo de negocio RaaS, su finalidad es hacer uso de técnicas que logren comprometer y deshabilitar los esquemas de seguridad en un sistema o recurso tecnológico dejándolo vulnerable ante cualquier ataque cibernético. Utilizan técnicas de extorsión logrando cifrar grandes cantidades de información para luego pedir el rescate por la información cifrada.

Vulnerabilidades: Basándonos en la investigación realizada para la alcaldía de Medellín se evidencia unos de los factores más importantes es el desconocimiento sobre tenas relacionados con ciberseguridad para los usuarios de la entidad dado que acceden a correos, descargan archivos sospechosos o simplemente acceden a link con procedencia delictiva, pero por desconocimiento no identificad la amenaza que se está presentando.

- **Debilidad en la red corporativo:** Esta vulnerabilidad se presentó en la alcaldía de Medellín dado a que no se mantienen los equipos de cómputo actualizados con

---

[133] ELTIEMPO. Peligrosa banda de ciberdelincuentes se atribuyó ataque a seguridad de Medellín. [Sitio web]. 2023. [Consultado 4 marzo 2023]. Disponible en: https://www.eltiempo.com/colombia/medellin/lockbit-banda-se-atribuye-ataque-a-seguridad-de-medellin-739779

[134] INFOBAE. Ciberataque a la Alcaldía de Medellín. [Sitio web]. 2023. [Consultado 4 marzo 2023]. Disponible en: https://www.infobae.com/colombia/2023/02/02/ciberataque-a-la-alcaldia-de-medellin/

la última versión, los parchados correspondientes al sistema, es importante que el administrador del sistema realice e implemente políticas de seguridad para que estas se establezcan a la red corporativa. Fortaleciendo la red con la finalidad de mitigar el riesgo de amenaza.[135]

- **Falencia de parchado:** El administrador del sistema debe establecer actualizaciones periódicas para todo el sistema debido al riesgo constantes debido a la alta concentración que tiene las entidades del gobierno.

- **Fortalecimiento en la red:** Es importante implementa herramientas sofisticadas que permitan tener una doble protección de la red, el administrador del sistema debe monitorear constantemente la red para detectar intrusos en la red.

- **Falta de capacitación a los usuarios:** Es importante que los usuarios estén actualización en cuanto a temas de ciberseguridad, para que logren identificar las posibles amenazas que se puedan presentar. Así mismo, concientizar a los usuarios para que apliquen las medidas de seguridad y tengan claro las políticas de seguridad que tiene la entidad.

De acuerdo a lo anterior, se identificó ocho entidades del estado Colombia quienes sufrieron ataques cibernéticos de diferentes grupos delincuenciales y se describe la manera como fueron vulnerados los recursos tecnológicos, aplicaciones, servicios e infraestructura TI. Podemos observar, desde el 2020 se han incrementado el ciberdelito. Hubo un incremento del 133% instituciones hackeadas y vulneradas en relación al ataque cibernético ransomware este software que se encarga de secuestrar información sensible y confidencial, datos personales como credenciales de accesos a cuentas bancarias e ingresos a aplicaciones de las entidades colombianas a través de malware logrando pedir la recuperación y rescate de la información. [136]

[135] PIRANIRISK. Vulnerabilidades que afectan la seguridad de la información. [Sitio web]. 2022. [Consultado 4 marzo 2023]. Disponible en: https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

[136] NSIT. 10 reconocidas instituciones de Colombia hackeadas en el 2022. [Sitio web]. 2022. [Consultado 5 marzo 2023]. Disponible en: https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/

6 VULNERABILIDADES E IDENTIFICACIÓN DE LOS IMPACTOS GENERADOS EN LAS ENTIDADES

Las vulnerabilidades en un sistema se relacionan directamente a una falla en la seguridad de un sistema de información o infraestructura tecnológica, en el que los atacantes cibernéticos toman estos medios para acceder a ellos, de manera que puede exponer la disponibilidad, integridad y confidencialidad de la información. Los accesos no autorizados identificando las vulnerabilidades existentes de un sistema informático se convierto en una amenaza, y esto puede afectar el sistema interno y externo generando grandes pérdidas de información convirtiéndose en un riesgo altísimo para las organizaciones.

Posteriormente, se pueden identificar las siguientes vulnerabilidades más recurrentes en un sistema informático:[137]

- **Vulnerabilidades de un sistema:** Se presenta cuando se identifica un error en su diseño o código en las aplicaciones del sistema generando así una amenaza, dando acceso para admitir ataques externos e internos.

- **Vulnerabilidades de implementación:** Se presenta cuando se evidencian errores en la codificación del fabricante.

- **Vulnerabilidades factor humano:** Las causas principales de los ataques cibernéticos se ha evidenciado por el mal uso de los recursos tecnológicos por parte de los usuarios. Muchas veces se ha presentado la asignación de permisos a los usuarios sin tener en cuenta que no corresponde a un usuario administrador. Falta de capacitaciones y malas prácticas de los usuarios esto puede ocasionar un alto riesgo.

- **Vulnerabilidades secuencias de comandos sitios cruzados:** Consiste en inyectar código malicioso al navegador de la víctima mediante la página web donde se está intentando conectar, por ende, pone en riesgo la información

[137] AMBIT-BST. Tipos de Vulnerabilidades y Amenazas informáticas. [En línea]. 2020. [Consultado 20 de noviembre 2022]. Disponible en: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

confidencial y datos personales estas páginas web son controladas por los ciberdelicuentes ya que capturan los datos ingresados por las víctimas. [138]

- **Vulnerabilidades de falsificación de solicitudes entre sitio:** Esta vulnerabilidad se encarga de engañar a la víctima logrando autenticar el usuario realizando alguna acción en el que no tiene conocimiento que está accediendo o que información está ingresando a las páginas web de procedencia engañosa de esta manera toma todos los datos personales.

- **Vulnerabilidad de configuraciones incorrectas**: Consiste en la utilización de un componente de seguridad, donde los atacantes aprovechan de estas configuraciones que no son robustas, con valores predeterminados y la seguridad no se define como segura y no forzan el cambio de contraseñas como bases de datos, servidores web o aplicaciones de la entidad. Y es así como este ataque fuerza al navegador web de la víctima validando un servicio o algún acceso financiero y este lo direcciona a un sitio web vulnerable. Y es la manera en como los atacantes cibernéticos vulneran los sistemas hasta lograr acceder a la infraestructura TI.[139]

- **Vulnerabilidades autenticaciones débiles:** Cuando las credenciales de autenticación son débiles, las sesiones de usuarios pueden ser secuestradas por los atacantes cibernéticos con la finalidad de suplantar la identidad del usuario original, pueden lograr acceder al usuario administrador y pueden cambiar los permisos y el perfil de usuario. [140]

- **Vulnerabilidades Lógicas**: Estas vulnerabilidades hacen referencia a los ataques que directamente afectan la infraestructura y el desarrollo de cada operación, es decir, como la configuración, actualización y desarrollo de la infraestructura.

---

[138] AVAST. ¿Qué son las secuencias de comandos en sitios cruzados (XSS)? [Sitio web] 2022. [Consultado 5 mayo 2023]. Disponible: https://www.avast.com/es-es/c-xss

[139] KEEPCODING. ¿Qué es la configuración de seguridad incorrecta? [Sitio web]. 2021. [Consultado 5 mayo 2023]. Disponible: https://keepcoding.io/blog/que-es-la-configuracion-de-seguridad-incorrecta/

[140] COMPUTERWEEKLY. os puntos débiles de sistemas de autenticación para combatir a los hackers. [Sitio web]. 2005. [Consultado 05 mayo 2023]. Disponible: https://www.computerweekly.com/es/consejo/Los-puntos-debiles-de-sistemas-de-autenticacion-para-combatir-a-los-hackers

- **Vulnerabilidades Físicas**: Estas vulnerabilidades afectan la infraestructura es decir de manera física, los atacantes pueden acceder a la red o sistema de la compañía y tomar el control de los equipos de cómputo. Otra de las situaciones que se pueden presentar en cuanto a la detección de vulnerabilidades, es el control de acceso de las compañías ya que muchas veces no controlan el ingreso de personas que no laboran en la entidad. Esto es un riesgo alto ya que puede acceder a los recursos tecnológicos sin ningún control.[141]

Según los conceptos indicados anteriormente en el que se relaciona el ataque cibernético Ransomware, en donde se evidencia el comportamiento y el modus operandi ya que han surgido bastantes años, donde se evidencia los cambios y actualizaciones que ha tenido este ataque cibernético.

Las entidades colombianas están centralizadas en la utilización de los sistemas informáticos ya que requieren para el buen funcionamiento de los recursos tecnológicos, no obstante, las vulnerabilidades declinan la seguridad de la información y afectar los datos de las organizaciones causaría daños en los recursos tecnológicos, económicos y desprestigio. [142]

Para las entidades colombianas es importante mantener vigentes políticas de seguridad establecidas con el fin de asignar roles y responsabilidades. Es importante definir políticas de seguridad que direccionen el buen uso de los activos de las compañías que permita fortalecer las tecnologías de la información y la seguridad informática manteniéndolas vigentes donde se evidencie la información eficiente y clara, así mismo debe ser confidencial, con la finalidad de proteger la información de las entidades. [143]

---

[141] 3CIENCIAS. Introducción a la seguridad informática y el análisis de vulnerabilidades. [En línea]. 2018. Pag. 471 – 88. Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

[142] AMBIT. Tipos de Vulnerabilidades y Amenazas informáticas. [Sitio web] 2020. [Consultado 10 mayo 2023]. Disponible: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

[143] NSIT. 10 reconocidas instituciones de Colombia hackeadas en el 2022. [Sitio web]- 2022. [Consultado 2 mayo 2023]. Disponible: https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/

Las compañías pueden mitigar los riesgos que se lleguen a presentar en el momento en el que se evidencie o se detecte un ataque informático, permitirá tomar medidas preventivas, esto con lleva a utilizar herramientas de protección, identificar correos fraudulentos, páginas web engañosas, mantener vigente el inventario de activos de las organizaciones, implementar medidas para minimizar las amenazas.[144]

6.1 ¿CÓMO SE PUEDEN IDENTIFICAR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA DE LAS ORGANIZACIONES COLOMBIANAS?

Es importante contrarrestar los ataques cibernéticos ransomware en todas las organizaciones colombianas, estas amenazas se han identificado durante los últimos años. este software malicioso se ha incrementado de manera excesiva donde se ha desarrollado múltiples sistemas con un objetivo específico, donde se accede de manera no autorizada y procede a realizar ciertos delitos como; el hurto de información sensible, bloqueo en los sistemas o infraestructuras ti, bloqueo o secuestro de información, minado también conocida como criptomonedas maliciosas, backdoor, entre otros.[145]

Una de las cuestiones que se hacen hoy en día en relación a los ataques Ransomware es que los atacantes cibernéticos tienen éxito en el momento de acceder a un sistema de información, infraestructura TI y logran ingresar de manera no autorizada a la información o recurso tecnológico ocasione daño. Se evidencia el desarrollo de las mutaciones que puedan llegar a tener cada software malicioso teniendo en cuenta que la tecnología día a día está en constante evolución. Es así, como se ha incrementado variantes o familias relacionados a estos códigos o software maliciosos.

En la configuración, los sistemas operativos y servicios o aplicativos del servidor, en algunas ocasiones vienen por defecto, es importante verificar este tipo de configuraciones ya que muchas veces presentan fallas. Una de las razones también identificadas es la configuración de Firewalls debido a que están mal configurados y estos pueden tener reglas permisivas, donde no detecta ninguna anomalía permitiendo el paso de trafico de red sin detectar algún intruso. Actualmente, muchas compañías u organizaciones no actualizan los sistemas operativos o aplicaciones, es muy importante tener en cuenta la

[144] AMBIT. Tipos de Vulnerabilidades y Amenazas informáticas. [Sitio web] 2020. [Consultado 10 mayo 2023]. Disponible: https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas

[145] OSORIO, Andrés Felipe. Revistas UIS. Proceso para la identificación, clasificación y control del comportamiento de familias Ransomware. [En línea]. 2020. Enero – Mayo. Disponible en: https://revistas.uis.edu.co/visores/Revista_UIS_Ingenierias_Vol_19_Num_3/553768212016/

verificación periódica de estos recursos y así se puede mitigar cualquier acceso no autorizado. En la parte de desarrollo, esta vulnerabilidad se mencionan puntualmente las inyecciones de código SQL para este tipo de ataques varían según la aplicación y es así como cada escáner de vulnerabilidades usa diferentes escalas. [146]

6.1.1 Comportamiento Ransomware, es un malware que abarca ciertas fases que se describen de la siguiente manera: Análisis estático, dinámico y comportamiento. En el caso del análisis dinámico se observa que tiene un comportamiento y estructura parecidos a otros tipos de malware, estos contienen técnicas confusas o autoreplicación. Este software malicioso necesita de un playload ya que su finalidad es dañar el sistema operativo utilizando un método de ocultamiento para que no pueda ser detectado por loa antivirus.

En otros malware la función es eliminar las copias shadow del sistema operativo Windows impide los datos que están cifrados se logren recuperar o se restauren con alguna versión anterior del sistema operativo. Dado a esto funcionalidad del malware permite que el atacante bloquea todo el sistema para que la víctima no logre recuperar la información o tomar acciones para reestablecer el sistema. Ya que ante la situación el software o código malicioso cifra y captura la información, para así pedir recompensa de la misma. [147]

Se presentan varias fases de ejecución en cuanto al malware comenzando a realizar despliegues en el sistema, tomando como método de infección, para así seguir con el siguiente paso de encriptar la información adquirida de manera inusual y concluir con el proceso. De acuerdo a este proceso que realiza el malware produce llaves criptográficas y estas son remitidas a un centro de control para tomar el sistema y administrarla de manera remota.

[146] ROBAYO LÓPEZ, Javier Humberto, et al. Aseguramiento de los sistemas computacionales de la empresa Sitiosdima. net. 2015.
[147] AVILA NIÑO, Segundo Fredy Yesid, et al. Evolución e impacto del Ransomware en América Latina desde el año 2015. 2015.

6.1.2 ¿Cómo se propaga Ransomware?, por lo general, los ataques cibernéticos tienen diferentes formas de engañar a sus víctimas, es así, se evidencian vectores de amenazas a medida que los servicios o aplicaciones informáticas deben estar activos. Y es así, como se ejecuta estos vectores por falta de conocimiento por parte de los usuarios o trabajadores de las compañías, quienes no identifican los archivos ya infectado del virus o software malicioso. La manera de engañar a las víctimas es por medio de correos electrónicos o mensajes de texto ya que es el medio o función donde las organizaciones manejan este tipo de comunicaciones y es así como los atacantes envían mensajes con información engañosa y archivos adjuntos donde es implantado el software malicioso.

Otro vector implicado es la configuración de auto-run en los dispositivos extraíbles ya que son de gran uso para los usuarios y tienen variedad de funciones en la nube de los cuales son utilizados para compartir información o el mismo recurso. [148]

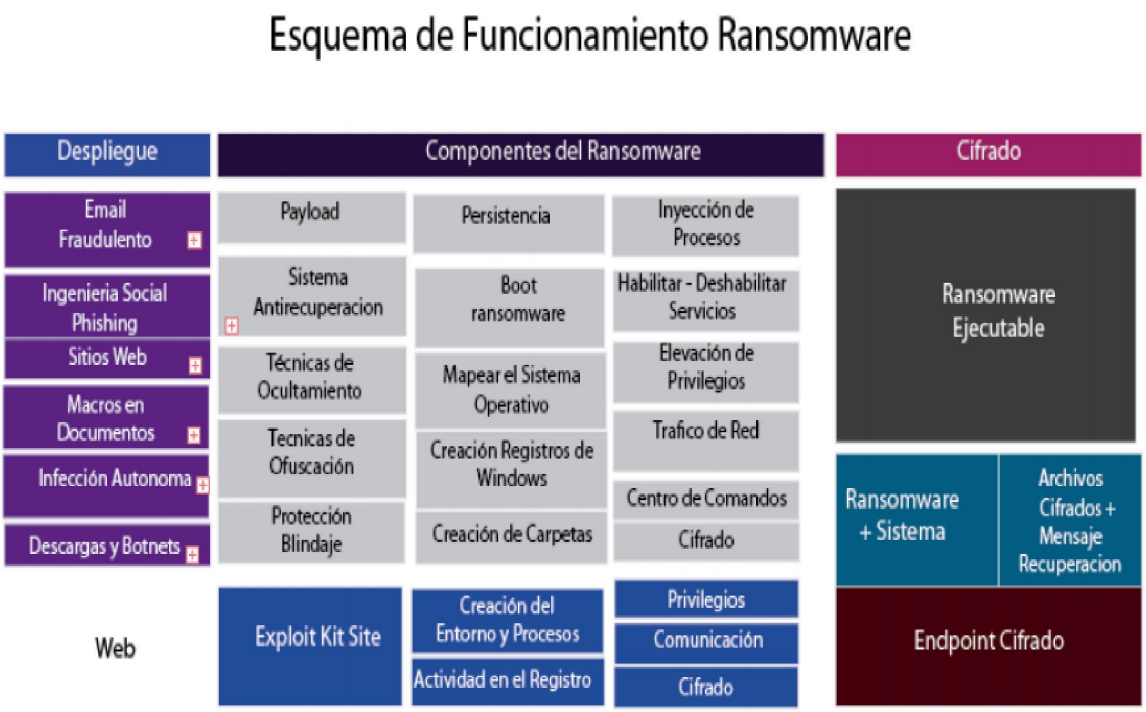
6.1.3 Ciclo de vida de Ransomware, este software malicioso utiliza fases para el ciclo de vida para atacar un sistema de información, es así, como se debe comprender los métodos técnicos del cual genera una metodología de prevención y detección que cubre las fases del ciclo de vida. Los ciberdelincuentes hacen despliegues iniciales medio de estrategias para así lograr la instalación en el recurso tecnológico final según el tipo de ransomware. Cuando el software es instalado este procede a realizar la búsqueda de determinados archivos para encriptarlos. Esto conlleva, a crea conexiones en el sistema para obtener el control y la administración del mismo. Este proceso de malware logra administrar desde de un servidor central y así proceder a realizar las siguientes funciones: como el ocultamiento de información, bloqueo, cifrado de datos y crea accesos nuevos para encriptar la información sensible con la finalidad de que las organizaciones no logren actuar a tiempo, ni recuperar la data. [149]

A continuación, será plasmando el esquema o funcionamiento de Ransomware. Según la ilustración 7.

[148] OKDIARIO. Qué es un ransomware y cómo se propaga. [En línea]. 2022. [Consultado 25 de noviembre 2022]. Disponible en: https://okdiario.com/curiosidades/que-ransomware-3302405

[149] CAMPUS CIBERSEGURIDAD. TIPOS DE RANSOMWARE Y SU CICLO DE VIDA. [En línea]. 2022. [Consultado de 22 de noviembre 2022]. Disponible en: https://www.campusciberseguridad.com/blog/item/160-tipo-de-ransomware-ciclo-de-vida

Ilustración 11. Funcionamiento Ransomware.



Fuente: REDALYC. Esquema de funcionamiento Ransomware. [En línea]. 2020. [Consultado 2 de marzo del 2022]. Disponible en: https://www.redalyc.org/journal/5537/553768212016/html/

En el esquema anterior, se puede evidenciar el funcionamiento de Ransomware. Es necesario que las organizaciones implementen medidas de protección para detener los ataques cibernéticos, adicionalmente las compañías deben contar con equipos propios, con la finalidad de detener e interrumpir los ciberataques. Sin embargo, es fundamental comprender cuál es el ciclo de vida y así mismo construir estrategias que permitan realizar las operaciones necesarias que garanticen la protección tecnológica de las organizaciones. Tomando como ejemplo el concepto de Cyber Kill Chain que es un principio que utilizaban los militares para definir y detectar cada paso de los ciberdelincuentes con el fin de atacar un objetivo específico. [150]

Se ha identificado el paso a paso de los atacantes al momento de acceder a la infraestructura de una compañía y lograr bloquear todo el esquema planeada por los

[150] STATISTA. ¿Cómo funciona un ransomware? [Sitio web]. 2017. [Consultado 15 mayo 2023]. Disponible: https://es.statista.com/grafico/9376/como-funciona-un-ransomware/

delincuentes cibernéticos. Para el principio Cyber Kill Chain donde se identificó siete pasos y se visualiza una etapa de ataque en la (Ilustración 8).

Ilustración 12. Siete fases de un ataque cibernético.

Fuente: INCIDE. Las siete fases de Ciberataque. 2020. [En línea]. [Consultado marzo del 2022] Disponible en: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

El principio Cyber Kill Chain está conformada por una serie de pasos de los cuales conlleva una etapa de ataque:[151]

Reconocimiento: En esta fase el atacante cibernético se encarga de recopilar de información sobre el objetivo. Se pude detallar la victima publica y busca información sobre la tecnología que se implementó. El atacante examina las técnicas utilizadas para lograr tomar la información o secuestrarla. Al impedir que el ciberdelincuente determina la información que se va a tomar sin autorización. Es importante mantener estrategias de

[151] NETSKOPE. ¿Qué es Cyber Security Kill Chain (cadena de exterminio de la ciberseguridad)? [En línea]. 2022. [Consultado 26 de noviembre 2022]. Disponible en: https://www.netskope.com/es/security-defined/cyber-security-kill-chain

protección y respaldo de información. Como la utilización de cifrados de información y limitantes para compartir datos.

Preparación: Para esta fase el delincuente informático previene el ataque de manera detalla sobre el objetivo. El atacante establece la creación de un archivo PDF incluye un correo electrónico con la finalidad de suplantar la identidad de alguna compañía que permita interactuar. [152]

Distribución: Para esta etapa se produce la transmisión de ataque, la utilización de esta etapa a través de la apertura de un archivo o documento que es enviado por correo electrónico accediendo por medio del método phishing.[153]

Explotación: En esta fase implica la detonación del atacante, exponiendo el equipo de cómputo propagándose en la red donde pertenece el recurso tecnológico. Sin embargo, cabe resaltar que es importante alinear soluciones de protección de seguridad para mantener los sistemas de información actualizados y protegidos por un antivirus.

Instalación: En esta fase el ciberdelincuente procede a instalar un código malicioso o malware en el equipo de cómputo de la víctima, también tiene otra forma de acceder sin necesidad de instalar algún software, sino accediendo a las credenciales o fraude CEO.

Comando y Control: En esta fase el atacante cuenta con el control absoluto del sistema de la víctima, donde podrá realizar acciones delictivas como dirigirse al servidor central identificado como C&C (Command and Control) obtiene las credenciales, procede a tomar captura de la información, toma la información confidencial e instala software y accede a la red de la víctima. [154]

Acciones sobre los objetivos: Finalmente en esta fase el atacante ya obtuvo la información, procede a propagar la acción maliciosa hacia los demás objetivos de las organizaciones. Es así, que el principio Cyber Kill Chain no es lineal sino cíclica logrando así ejecutar nuevamente todas las fases para lograr infectar a más víctimas.

---

[152] INCIDE. Las siete fases de Ciberataque. 2020. [En línea]. [Consultado marzo del 2022] Disponible en: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

[153] TARLOGIC. Cyber Kill Chain. Diseccionar las 7 fases de un ciberataque dirigido. [Sitio web] 2023. [Disponible 10 mayo 2023]. Disponible: https://www.tarlogic.com/es/blog/cyber-kill-chain/

[154] NETSKOPE. ¿Qué es Cyber Security Kill Chain (cadena de exterminio de la ciberseguridad)? [En línea]. 2022. [Consultado 26 de noviembre 2022]. Disponible en: https://www.netskope.com/es/security-defined/cyber-security-kill-chain

Conforme a lo anterior, es importante destruir esta secuencia de ataque que permita evitar amenazas cibernéticas para que las organizaciones mantengan los sistemas de información y los equipos actualizados, con la finalidad de adecuar soluciones de seguridad efectivas. Es importante tener en cuenta que cada entidad debe realizar capacitaciones de ciberseguridad y culturizar a los empleados o usuarios finales tengan bases en cuanto a conocimientos de seguridad informática, además estar en constante comunicación con el propósito de evitar el incremento de ataques. Con estas recomendaciones se logran fortalecer en parte los recursos tecnológicos. [155]

6.1.4 Principales grupos delincuenciales que usan Ransomware. Recientemente se han conocido el incremento de ataques cibernéticos que se han presentado durante el año 2020 año de la pandemia que por las situaciones presentadas se disparó las denuncias sobre los delitos cibernéticos, suplantación de identidad y secuestro de información, es así, como se da a conocer por la Interpol, la Fiscalía general de la nación una variedad de organizaciones criminales quienes constantemente están detectando y monitoreando las vulnerabilidades que se pueden presentar en grandes compañías del sector salud, instituciones educativas, servicios públicos, tecnología, las comunicaciones, entidades públicas colombianas, entre otros. [156]

Situación que ha generado un gran impacto reputacional en las organizaciones colombianas y afectando de gran manera los usuarios de diversas empresas como el gremio de la salud que se ve truncado e interrumpido los procesos médicos antes las necesidades que se requiere el mejoramiento de la salud para muchas personas vulnerables. A continuación, se describen los siguientes delincuentes cibernéticos que han atacado a diferentes compañías colombianas durante los últimos tres años.

[155] INCIDE. Las siete fases de Ciberataque. 2020. [Sitio web]. [Consultado marzo 3 de marzo 2022]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

[156] LAREPUBLICA. Empresas colombianas víctimas de ciberataques ¿Qué pasará contra el cibercrimen? [Sitio web]. 2023. [Consultado 8 marzo 2023]. Disponible en: https://www.larepublica.co/empresas/que-pasara-contra-el-cibercrimen-en-empresas-vea-las-proyecciones-de-especialistas-3539553

6.1.4.1 BlackCat, es un grupo criminal que utiliza los ataques cibernéticos ransomware con técnicas de cifrados de archivos y la finalidad es solicitar el rescate sobre la data encriptada de las compañías. La Oficina Federal de Investigación (FBI) dio un comunicado de prensa donde se indicó que existe una alerta de ransomware a quien responsabilizan al grupo criminal BlancakCat quienes han vulnerado y atacado a 60 entidades en todo el mundo. BlackCat también se hace llamar ALPHV y Noberus y se destaca por ser el primer malware, ya que está diseñado por un lenguaje de programación Rust. En el año 2021 fue su primera aparición en el que afecto, compañías de Estados Unidos. Según las investigaciones realizadas por las compañías de Cisco Talos y Kasperksy, estas dos compañías identificaron familias de ransomware en las que están relacionadas con BlackMatter, según lo informado es una herramienta que su función es exfiltrar datos llamados (Fendr).[157]

Ransomware BlackCat tiene un modelo de negocio de ransomware como servicio RaaS se basa en tomar una estructura marketing de afiliados. Esta organización opera con la intensión de no dejar malware, la intención de ellos es no dejar evidencia y que no puedan ser identificados. El servicio RaaS es rentable para los delincuentes cibernéticos ya que el software lo pueden alquilar sin dejar rastro ante las autoridades de seguridad y puede operar sin ningún problema ya que jamás serán detectados.

El modus operando de BlackCat es hurtar información a las victimas antes de la ejecución del ransomware. Después el malware toma las credenciales de los usuarios logrando acceder al sistema. Este grupo tiene como funcionalidad enviar correos electrónicos mediante un sitio web el cual tiene procedencia delictiva y engañosa. La acción de malware es encriptar los archivos del usuario, luego el mismo sistema arroja un mensaje de alerta a la víctima y este procede a bloquear el equipo de cómputo. Los atacantes cibernéticos piden un rescate por medio de criptomoneda para que la información pueda ser recuperada. [158]

BalckCat han evolucionado sus tácticas de ataques mejorando los procedimientos e implementando herramientas sofisticadas integran nuevas funcionalidades de encriptación logrando que el malware reinicie las maquinas comprometidas y estén

[157] ELCOLOMBIANO. Grupo de ciberdelincuentes “Blackcat” reconoció el ataque a EPM y empezó a filtrar información. [Sitio web]. 2022. [Consultado 8 marzo de 2023]. Disponible en: https://www.elcolombiano.com/antioquia/grupo-de-ciberdelincuentes-blackcat-reconocio-el-ataque-a-epm-y-empezo-a-filtrar-informacion-PO19710917

[158] POWERDMARC. ¿Qué es el ransomware BlackCat? [Sitio web]. 2022. [Consultado 8 marzo 202]. Disponible en: https://powerdmarc.com/es/what-is-blackcat-ransomware/

eludiendo las protecciones de seguridad. Una de sus características principales, atacan compañías de energéticas ya están dirigidas a realizar ataques a empresas estatales de servicios de energía, son más de 140 víctimas de las cuales son atacadas por este grupo criminal y su finalidad es publicar toda la información confidencial de las compañías y dejarla publica en la página de la dark web BlackCat.[159]

6.1.4.1.1 Vectores de ataque BlackCat: Los ciberdelincuentes tiene varias modalidades de engañar a las víctimas, es así, como utilizan estrategias, técnicas y métodos de engaño para logar su objetivo. Lograr acceder a la red corporativa para rastrear la información y luego encriptarla. A continuación, se describen los vectores de ataques más utilizados por los ciberdelincuentes BlackCat.[160]

- **Phishing:** Técnica más utilizadas por los delincuentes cibernéticos que logran engañar a sus víctimas por medio de mensajes de correo electrónico que contiene información que aparenta ser confiable como entidades bancarias, compañías de energía, entre otros. Con este tipo de mensajes logran la confianza de sus víctimas, quienes proceden a acceder a los archivos o link de sitios web acceden a estos medios, pero se direcciona a una página fraudulenta o realizan la descarga de archivos de software malicioso. Con esta modalidad logran engañar a los usuarios ya que ellos proporcionan los datos personales e información confidencial de la compañía. Después de acceder al sistema y lograr detectar la información confidencial la encriptan y proceden a solicitar el rescate de la información o del sistema o infraestructura.

- **Explotación de vulnerabilidades:** BlackCat utiliza la explotación de aplicaciones expuestas y vulnerables que existen en un sistema o red corporativa. Y se dirige a los sistemas operativos de Microsoft Windows, también acceden a entornos VMWare EXSI y distribuciones de Linux, donde proceden a hacer la explotación de las vulnerabilidades logrando afectar las aplicaciones que estén expuestas en internet. Su objetivo es capturar información confidencial mediante herramientas controladas por los hackers logrando cargar el ransomware afectando la

[159] POWERDMARC. ¿Qué es el ransomware BlackCat? [Sitio web]. 2022. [Consultado 8 marzo 202]. Disponible en: https://powerdmarc.com/es/what-is-blackcat-ransomware/

[160] MASTERHACKS. Los operadores del ransomware BlackCat están mejorando su arsenal de malware. [Sitio web]. 2022. [Consultado 11 marzo 2023]. Disponible en: https://blogs.masterhacks.net/noticias/hacking-y-ciberdelitos/los-operadores-del-ransomware-blackcat-estan-mejorando-su-arsenal-de-malware/

integridad, disponibilidad y confidencialidad de la infraestructura TI de las compañías. [161]

- **Compra de credenciales robadas en la Deep Web:** BlackCat logra captar credenciales de usuarios en el mercado negro como nombres y contraseñas de acceso a diferentes plataformas, servicios, aplicaciones y dispositivos tecnológicos. Son descubiertos por la dark web donde se han encontrado más de 100.000 brechas de datos de las cuales se encuentra información acceso de cuentas bancarias, servicios de streaming, cuentas y contraseñas de administradores de las diferentes aplicaciones o servicios de compañías. Con esta información pueden vulnerar fácilmente la infraestructura TI y servicios de una organización. [162]

- **Denegación de servicio:** El objetivo de BlackCat es inhabilitar el uso del sistema, servicios, aplicaciones y dispositivos de las entidades, con la finalidad de bloquear todos los servicios que estén en curso. Con este tipo de ataque logra afectar en gran manera la información de la compañía. Los ataques de denegación de servicios lo realizan por medio de DDoS el cual realiza varias peticiones empleando una gran cantidad de números de ordenadores o direcciones IP, logrando que la función de hacerlo se haga de manera constante y al mismo tiempo y con la identificación que se haga en el mismo servicio. Logrando que no sea detectado por los administradores del sistema, por la razón que se envían varias IP y es más difícil bloquearlas ya que son envíos al mismo tiempo. De esta manera el atacante cibernético logra tomar el dominio de los ordenadores y estos son reclutados por medio de la infección de malware convirtiéndose en bots y controlan los recursos tecnológicos de manera remota.[163]

La organización criminal BlackCat utiliza algunos de los métodos ya mencionados, con la finalidad de acceder a la red corporativa, recursos tecnológicos, servicios e información confidencial de la compañía adquiriendo todos los privilegios del sistema y propagando

[161] MASTERHACKS. Los operadores del ransomware BlackCat están mejorando su arsenal de malware. [Sitio web]. 2022. [Consultado 11 marzo 2023]. Disponible en: https://blogs.masterhacks.net/noticias/hacking-y-ciberdelitos/los-operadores-del-ransomware-blackcat-estan-mejorando-su-arsenal-de-malware/

[162] BLOG AXUR. Cómo funciona la venta de credenciales corporativas en Deep & Dark Web. [Sitio web]. 2023. [Consulta 15 mayo 2023]. Disponible: https://blog.axur.com/es/como-funciona-la-venta-de-credenciales-corporativas-en-deep-dark-web

[163] COMPUTERWEEKLY. BlackCat, el nuevo ransomware que va a la caza del Active Directory. [Sitio web]. 2022. [Consulta 12 mayo 2023]. Disponible: https://www.computerweekly.com/es/noticias/252516548/BlackCat-el-nuevo-ransomware-que-va-a-la-caza-del-Active-Directory

el malware en todo el sistema para proceder a hurtar y encriptar la información manteniendo el dominio de la infraestructura tecnológica de las organizaciones sin ser detectados.

Como se evidencia en la ilustración 10, se puede observar la ruta de infección más común que utiliza este tipo de organizaciones criminales.

Ilustración 13. Ruta de infección.

Fuente: ZIBERSEGURTASUN, BlackCat Ransomware. [Sitio web]. 2022. [Consultado 10 marzo 2023]. Disponible en: https://www.zibersegurtasun.eus/sites/default/files/2022-08/bcsc-malware-blackcat-tlpwhite.pdf

En la imagen anterior se puede observar los ataques cibernéticos malware tienen un flujo de infección que se propaga convirtiéndose a un ransomware. Este tipo de infecciones tienen una variación constante a medida que van evolucionando, estos van tomando fuerza con la finalidad de darse a conocer en el medio tecnológico a nivel mundial. [164]

El grupo criminal BlackCat fueron los responsables del ataque cibernético que sufrieron algunas entidades colombianas como por ejemplo la Alcaldía de Santa Fe de Antioquia,

[164] INFOBAE. Grupo de ciberdelincuentes "BlackCat" reconoce el ataque a EPM y comienza a filtrar información. [Sitio web]. 2022. [Consultado 10 marzo 2023]. Disponible en: https://www.infobae.com/america/colombia/2022/12/27/grupo-de-ciberdelincuentes-blackcat-reconoce-el-ataque-a-epm-y-comienza-a-filtrar-informacion/

las empresas de EPM Medellín y la Alcaldía de Medellín quienes tuvieron una gran afectación en los servicios de energía, servicios de pago en línea, bloqueo de acceso a otros productos utilizados por la comunidad fueron afectados en gran manera deshabilitando por varios días el sistema tecnológico y servicios de las organizaciones colombianas afectando en gran manera la información y datos personales, logrando afectar la confidencial, integridad y disponibilidad de las compañías. [165]

6.1.4.2 RansomHouse, es un grupo criminal según fuentes oficiales como el FBI la Interpol opera desde España quienes están especializados en atacar empresas de medicina, como hospitales y farmacias importantes en el mundo. En el mes de diciembre del año 2021, comenzó la actividad delictiva quienes publicaron un ransomware llamado White Rabbit donde RansomHouse hizo el desarrollo del malware. Esta organización criminal ataco por primera vez a la compañía Saskatchewan Liquor and Gaming Authority (SLGA) es una empresa canadiense que se encarga de controlar y regular las bebidas alcohólicas cannabis y juegos de azar logrando acceder a la información y solicitar el rescate de la misma. RansomHouse acceden a la página Dark Web donde se publica información, direcciones URL de las víctimas que son atacadas y extorsionadas con la finalidad de aumentar la exposición a las empresas afectadas por los ataques que ocasionan los delincuentes cibernéticos. Desde ese entonces se han visto afectadas empresas como AMD quienes lograron a la red y hurtaron 450GB de datos, en este caso no contactaron a la compañía, sino que procedieron a vender los datos obtenidos sobre la plataforma que este tipo de criminales cibernéticos utilizan para subir información sensible y confidencial de las organizaciones. Es así como RansomHouse ha logrado acceder a la red corporativa de grandes compañías como países como Canadá, Estados Unidos, Colombia, Alemania y países del África. [166]

En el mes de marzo del año 2022, se han reportado ataques cibernéticos que relacionan a RansomHouse ya que se reportó un ataque cibernético para el banco Jefferson Credit Union en la ciudad de Alabama (Estados Unidos) hurtando la información de esta compañía afectándola en gran manera. La compañía Dellner Couplers que su actividad

[165] INFOBAE. Grupo de ciberdelincuentes “BlackCat” reconoce el ataque a EPM y comienza a filtrar información. [Sitio web]. 2022. [Consultado 10 marzo 2023]. Disponible en: https://www.infobae.com/america/colombia/2022/12/27/grupo-de-ciberdelincuentes-blackcat-reconoce-el-ataque-a-epm-y-comienza-a-filtrar-informacion/

[166] CARACOL. RansomHouse: ¿Quiénes son y a quiénes han atacado? [sitio web]. 2022. [Consultado 11 marzo 2023]. Disponible en: https://caracol.com.co/2022/12/21/ransomhouse-quienes-son-y-a-quienes-han-atacado/

es el gremio de la manufactura ferroviaria del país de Suecia. Otra empresa víctima de ataque por RansomHouse fue la aerolínea AHS Group de Alemania. Uno de los supermercados más grandes de Sur África fue la compañía Shoprite Group quienes también fueron víctimas de esta organización criminal.

El 28 de noviembre del 2022 la compañía Keralty quienes prestan servicios médicos en Colombia, afectando en gran manera todos los servicios médicos y la deshabilitación de la página oficial de Sanitas, causando el no acceso a miles de pacientes en el país y no solo afecto la plataforma, sino que hurtaron la información de pacientes, personal administrativo, historias clínicas, balances financieros, información de proveedores, entre otros servicios prioritarios de Colsanitas y medicina prepagada. Se ha identificado que la finalidad es lograr un lucro económico ya que al obtener información confidencial de las organizaciones obligan a los responsables de cada compañía a realizar los pagos ya que por temor a perder la información y por prestigio de la compañía. Entonces, la compañía solicita que la información y tomar el control del sistema de la compañía. En el caso de la compañía Keralty no se ha logrado obtener información al respecto si ellos realizaron el pago solicitado por estos delincuentes cibernéticos.[167]

6.1.4.2.1 Vectores de ataque RansomHouse: Los atacantes cibernéticos RansomHouse utilizan técnicas fraudulentas con la finalidad de acceder al sistema y hurtar información confidencial para solicitar el rescate de la misma y ganar un lucro económico o en algunos casos, realizar la venta de la información adquirida y publicarla en la página Black web. Es así, como se identificaron los vectores de ataque más utilizados por este grupo criminal cibernético. [168]

- **Denegación de servicio:** RansomHouse utiliza este vector de ataque con la finalidad de bloquear las plataformas o servicios web de las compañías. La denegación del servicio también la podemos llamar DoS que corresponde a un ataque a una red corporativa, sistema y equipos de cómputo, con esta técnica

[167] INFOBAE. Responsables del ciberataque a Sanitas revelaron nueva información privada de la empresa. [Sitio web]. 2022. [Consulta 5 mayo 2023] Disponible: https://www.infobae.com/colombia/2023/02/02/responsables-del-ciberataque-a-sanitas-revelaron-nueva-informacion-privada-de-la-empresa/

[168] ITRESELLER. Las nuevas técnicas de extorsión o phishing obligarán a las empresas a blindarse en 2023. [Sitio web]. 2022. [Consultado 11 marzo de 2023]. Disponible en: https://www.itreseller.es/seguridad/2022/12/las-nuevas-tecnicas-de-extorsion-o-phishing-obligaran-a-las-empresas-a-blindarse-en-2023

RansomHouse logra que la red sea inestable dejando el sistema inhabitado impidiendo acceso a los sitios web, mientras realizan la propagación del malware, comienza a rastrear información confidencial de las compañías procediendo a captura la información para luego encriptarla. Que en el momento de tener secuestrada la información logran cobrar por el rescate de la misma, en algunas ocasiones este grupo criminal RansomHouse extrae y publica la información más sensible y esta es almacenada en la Black web, para luego ser vendida a otras empresas que sea de interés de la organización afectada. [169]

- **Phishing - Correo electrónico de spam:** Los delincuentes cibernéticos utilizan técnicas por medio del método Phishing que consiste en enviar correos electrónicos que no son legítimos y estos contienen publicidad engañosa, sitios web con procedencia delictiva o archivos que su contenido es un malware. Con este tipo de técnicas se evidencia como logran engañar a las victimas logrando su objetivo, ya que los usuarios proceden a acceder a links o archivos y ellos procede a hacer la descarga del malware, con la finalidad de propagar el ransomware en el sistema accediendo a las aplicaciones, servicios, recursos tecnológicos para bloquear y dejar inhabilitada la red corporativa. Para así, mismo acceder a la información confidencial de la compañía para solicitar el rescate de la misma y ganar un lucro económico.[170]

- **Protocolo de escritorio remoto:** RansomHouse utilizan esta técnica quienes acceden al escritorio de un equipo de cómputo se controlado a distancia por un usuario remoto. La manera en como acceden a los dispositivos o equipos de cómputo es con la utilización del protocolo de Microsoft quienes utilizan las conexiones remotas a otros equipos de cómputo. La conexión remota se realiza mediante el protocolo TCP 3389, logrando que los usuarios pueden tener el control del acceso remoto por medio de este protocolo permitiendo el acceso a la red mediante un canal cifrado, por consiguiente, los usuarios toman el acceso remoto a los equipos de la compañía. Pero el RDP es un vector de ataque muy peligroso ya que se evidencio varios equipos conectados en la red y la gran mayoría están conectados al puerto 3389 y estas abiertos sin ningún control o seguridad de protección, permitiendo tener una brecha de seguridad y para los delincuentes

[169] NORDVPN. ¿Qué es el RDP, y cómo usarlo con seguridad? [Sitio web]. 2021. [Consultado 11 marzo 2023]. Disponible en: https://nordvpn.com/es/blog/acceso-remoto-rdp/

[170] ITDIGITALSECURITY. Estos son los tres principales vectores de ataque del ransomware. [Sitio web]. 2021. [Consultado 11 marzo 2023]. Disponible en: https://www.itdigitalsecurity.es/actualidad/2021/09/estos-son-los-tres-principales-vectores-de-ataque-del-ransomware

delictivos es muy fácil hacer el rastrear de motores de búsqueda como Shodan que le permitan localizar equipos y dispositivos tecnológicos que estén configurados con este puerto. [171]

- **Sitios web maliciosas:** Otro de los vectores de ataque utilizados por los RansomHouse son los sitios web de procedencia delictiva, estos hackers utilizando técnicas como la ingeniería social logrando persuadir a sus víctimas para que accedan a los sitios web o que realicen la descarga de archivos que contienen malware, cuando las victimas acceden a los links enviados automáticamente son enviados a una página maliciosa que aparenta ser legitima de alguna compañía o banco. Estos sitios son desarrollados por los ciberdelincuentes y estos contienen código malicioso que se descarga en el equipo o dispositivo de la víctima con esta técnica los hackers proceden a escanear las vulnerabilidades que tiene el dispositivo. Cuando lo logran detectar ejecutan el código asegurándose que las víctimas no se darán cuenta de lo sucedido ya que se está propagando el virus y el atacante procederá a cifrar la información y solicitará el rescate de los datos encriptados. [172]

[171] NORDVPN. ¿Qué es el RDP, y cómo usarlo con seguridad? [Sitio web]. 2021. [Consultado 11 marzo 2023]. Disponible en: https://nordvpn.com/es/blog/acceso-remoto-rdp/

[172] ITDIGITALSECURITY. Estos son los tres principales vectores de ataque del ransomware. [Sitio web]. 2021. [Consultado 11 marzo 2023]. Disponible en: https://www.itdigitalsecurity.es/actualidad/2021/09/estos-son-los-tres-principales-vectores-de-ataque-del-ransomware

6.1.4.3 LockBit, este grupo criminal quienes se dedican a la utilización de software malicioso, con la finalidad de cifrar datos e información el cual ofrece una solución a las víctimas de la empresa a través de un modelo de servicio "Recovery As A Service". LockBit es conocido por los ataques cibernéticos realizados por ellos, la intensión de estos es atacar entidades bancarias, comerciales, compañías de transportes y servicios, entre otros. Estos delincuentes cibernéticos utilizan técnicas de ataque con la finalidad de engañar a sus víctimas y lograr acceder a la información confidencial y acceder a la red corporativa logrando bloquear las plataformas, sitios web y servicios de las organizaciones. En el mes de septiembre del año 2019, esta organización delictiva comenzó por primera vez en realizar ataques cibernéticos que en ese entonces se apodada "Virus .abcd", con este nombre inicialmente lo tomaron como extensión de archivos con la intensión de cifrar los archivos existentes y pertenecientes a las víctimas, es así como se dio a conocer los países quienes fueron afectados por este grupo cibernético y que el objetivo fue compañías como China, Ucrania, Indonesia, Estados unidos, Alemania, Francia y países bajos. [173]

Como se indicó anterior, LockBit opera como un servicio RaaS como un modelo de negocio que es muy recurrente para la ciberdelincuencia que consiste en desplegar ataques de ransomware sin tener la necesidad de tener conocimientos de codificación. El servicio RaaS tiene una serie de características que proporciona código malware el cliente atacante puede personalizar con la finalidad de adaptarlo. De esta manera, el atacante lo despliega mediante un servidor de comando y control C&C, con el objetivo de almacenar los archivos del ataque para cualquier servicio que se requiera como servicios en la nube, entre otros.

LockBit tiene tres etapas de ataque; explotar, infiltrase e implementar. La primera etapa explotar, se presenta debilidad en la red donde y se detecta brechas de seguridad. Pueden utilizar el método de ingeniera social. En la segunda etapa infiltrarse, ingresan al sistema logran configurar el malware, para obtener los privilegios del sistema, sin ser detectado por el administrador. Logra acceder y lanzar los ataques procede en inhabilitar los servicios o plataforma de la compañía. Para la tercera etapa implementar, el atacante procede a cifrar, el ransomware comienza a propagarse las maquinas adquiridas por el delincuente cibernético. Su acción es cifrar los archivos las víctimas, solo podrá recuperar los datos, si se pagan el rescate solicitado por el atacante. LockBit utiliza herramientas

[173] GDEMPRESA. LockBit, el software malicioso que atemoriza a las empresas. [Sitio web]. 2022. [Consultado 11 marzo 2023]. Disponible en: https://gdempresa.gesdocument.com/tendencias/lockbit-software-malicioso#:~:text=Como%20decimos%2C%20LockBit%20es%20un,no%20tanto%20en%20los%20particulares

de descifrado. La victima encuéntrala las indicaciones para restaurar el sistema. Estas tres etapas la victima deberá contactar a LockBit. Realiza el pago para obtener la data y el control del sistema. [174]

6.1.4.3.1 Vectores de ataque LockBit: El modus operandi de los delincuentes cibernéticos LockBit tienen métodos de engaño que logran acceder al sistema, sin ser detectados por el administrador del sistema. [175]

- **Phishing:** Técnica utilizada por medio de envíos de correos electrónicos, estos mensajes tienen contenido engañoso en el que se visualiza archivos con código malicioso y link con procedencia engañosa. Estas técnicas son muy recurrentes en los atacantes cibernéticos ya que su finalidad es engañar a las víctimas para lograr acceder al sistema y obtener información confidencial de las compañías.

- **Campañas de spam:** Este vector de ataque es utilizado de manera constante por LockBit utilizada por ransomware estas campañas contiene archivos comprimidos y están acompañados por código malicioso y este debe ser ejecutado por la víctima o tiene otra modalidad incluyen en el correo un link en el cual lo dirección a una página web descargando el archivo y este contiene el malware, tomando la acción de propagarse en el sistema, con este método el objetivo final y es obtener información clasificada de las organizaciones.

De acuerdo con lo anterior, LockBit fueron los responsables de atacar el 1 de febrero del año 2023 a la alcaldía de Medellín y la persona afectada fue la secretaria de seguridad y convivencia de Medellín donde se evidencia la publicación sobre la información tomada por los delincuentes y que fue tomada información confidencial y sensible de once agencias del sistema integrado de Emergencias Seguridad (SIESM).[176]

---

[174] GDEMPRESA. LockBit, el software malicioso que atemoriza a las empresas. [Sitio web]. 2022. [Consultado 11 marzo 2023]. Disponible en: https://gdempresa.gesdocument.com/tendencias/lockbit-software-malicioso#:~:text=Como%20decimos%2C%20LockBit%20es%20un,no%20tanto%20en%20los%20particulares

[175] ELTIEMPO. Peligrosa banda de ciberdelincuentes se atribuyó ataque a seguridad de Medellín. [Sitio web]. 2023. [Consultado 11 marzo de 2023]. Disponible en: https://www.eltiempo.com/colombia/medellin/lockbit-banda-se-atribuye-ataque-a-seguridad-de-medellin-739779#:~:text=El%20ataque%20se%20lo%20atribuy%C3%B3,'Recovery%20As%20A%20Service

[176] INFOBAE. Ciberataque a la Secretaría de Seguridad de Medellín: qué es el grupo Lockbit, que se adjudicó el delito. [Sitio web]. 2023. [Consultado 12 marzo 2023]. Disponible en: https://www.infobae.com/colombia/2023/02/07/ciberataque-a-la-secretaria-de-seguridad-de-medellin-que-es-el-grupo-lockbit-que-se-adjudico-el-delito/

6.1.4.4 ViceSociety, es una organización criminal que se dedican a la extorsión de ransomware, ellos se centran en las organizaciones educativas y el gremio de la medicina. Esta sociedad criminal proviene de Rusia quienes son los responsables en atacar organizaciones de Europa y países cercanos. Este grupo cibernético fue creado en el mes de enero del 2021, pero la primera aparición fue en el mes de mayo del año 2021. ViceSociety es grupo criminal que utiliza la intrusión, exfiltración y la extorsión. Según las investigaciones realizadas por la Oficina Federal de Investigaciones (FBI) y la (CSA) identificaron que este grupo cibernético se ha centralizado en atacar al sector de la educación. Se identificó que ViceSociety no ha desarrollado sus propias herramientas de ataque pero se basan en la utilización de kits de herramientas de ransomware llamadas Hello Kitty, Zeppelin y Five Hands.[177]

ViceSociety realiza los ataques es mediante de la encriptación de datos, toma todos los archivos y los deja inaccesibles. Después cobra el rescate para que la víctima los pueda desencriptar. Los archivos encriptados se adjuntan con una extensión de la siguiente manera: v-society [ID_de_la_victima]. Con esta extensión aparecerá el proceso de encriptación y después aparece la nota de rescate.

Las victimas al ver este mensaje enviado por los delincuentes se deben comunicar con los delincuentes en un tiempo establecido por ellos, en el que les darán siete días. La idea de estos delincuentes cibernéticos es vender las claves para que los archivos sean desencriptados. Para el caso de que no lo logre la víctima, la información será publica en las páginas de la red oscura.[178]

Se reportó que la banda ViceSociety realizo un ataque al Consejo Superior de Investigaciones Científicas (CSIC) compañía de España realizando la afectación de manera masiva que afecto a 149 institutos y sedes territoriales. Este ataque cibernético masivo se realizó con el malware en el que inhabilito varios servicios y el correo electrónico. Este grupo criminal ataca compañías con la finalidad de realizar robo de la data. En Colombia se reportó tres empresas afectadas por este grupo de hackers, la Universidad Javeriana, Salud Total y Conferías quienes tuvieron grandes afectaciones en los servicios, páginas web y secuestro de información confidencial de las compañías. Las organizaciones colombianas detectaron a tiempo el ataque proporcionado por

[177] UNAALDIA. Los atacantes del ransomware Vice Society adoptan métodos de cifrado robustos. [Sitio web]. 2022. [Consulado 12 marzo 2023]. Disponible en: https://unaaldia.hispasec.com/2022/12/los-atacantes-del-ransomware-vice-society-adoptan-metodos-de-cifrado-robustos.html

[178] DEVEL GROUP. Los atacantes de rasomware de ViceSociety adoptan métodos de cifrado robustos. [Sitio web]. 2022. [Consultado 12 marzo 2023]. Disponibles en: https://devel.group/blog/los-atacantes-de-ransomware-de-vice-society-adoptan-metodos-de-cifrado-robustos/

ViceSociety, tomaron acciones rápidas. Ya que lograron reiniciar los servidores impidiendo que tomaran la data y este grupo delictivo lograra tomar información para ser publicada en la Deep Web. [179]

6.1.4.4.1 Vectores de ataque ViceSociety: Este grupo cibernético ViceSociety tienen variedad de técnicas para lograr obtener un ataque en compañías de sectores como la educación, el gremio de la medicina y entidades estales. [180]

- **Phishing**: La utilización de este método consiste en enviar correos masivos a diferentes víctimas de una organización el contenido de estos correos tiene páginas web ficticias y archivos con software malicioso. Una de los factores que se destaca este grupo criminal, cuando ellos logran encriptar la información después de a ver accedido a la red corporativa, ellos tienen la técnica que le envían un mensaje a las victimas indicando que deberán pagar cierta cantidad de dinero y ellos les entregarán las contraseñas para que ellos puedan desencriptar los archivos, ellos determinan un tiempo para el contacto de los delincuentes. Si esto no se realiza, los atacantes cibernéticos procederán a publicar toda la información en la página negra que ellos por lo general utilizan para este tipo de extorción. [181]

- **Identificación de vulnerabilidades:** Los ViceSociety utilizan métodos donde procede a buscar redes para identificar las vulnerabilidades que se puedan presentar en una red corporativa como puertos abiertos donde el administrador del sistema no configure restricciones, permisos, bloqueos, no se determina los privilegios. Esto un punto de debilidad en un sistema, es así, como acceden los atacantes y proceden a acceder de manera no autorizada.

- **RaaS:** la utilización de este método de ataque por parte del grupo criminal ViceSocierty consiste en la utilización de un modelo comercial, es decir, toman un software ya creado, realizan el ataque implementando las técnicas y habilidades del software ya utilizado. Logran acceder a la red corporativa y lograr acceder a la información para capturar los datos personales o información confidencial de las

[179] INFOBAE. Las 34 empresas que fueron hackeadas en Colombia durante 2022. [Sitio web[. 2023. [Consultado 12 marzo de 2023]. Disponible en: https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/

[180] INFOBAE. Hackeo al Senado: el grupo de ciberdelincuentes Vice Society filtró 30 mil archivos. [Sitio web]. 2022. [Consultado 12 marzo del 2023]. Disponible en:https://www.infobae.com/tecno/2022/03/14/hackeo-al-senado-el-grupo-de-ciberdelincuentes-vice-society-filtro-30-mil-archivos/

[181] NORDVPN. ¿Qué es el RDP, y cómo usarlo con seguridad? [Sitio web]. 2021. [Consultado 11 marzo 2023]. Disponible en: https://nordvpn.com/es/blog/acceso-remoto-rdp/

compañías. Después de esta acción envían un mensaje donde se indica que se deben contactar en un tiempo determinado. Los atacantes proporcionan claves para que la víctima logre recuperar los archivos afectados, de lo contrario serán publicados en la Deep Web.[182]

6.1.4.5 Ragnarok, este grupo criminal se tiene muy poca información dado que son muy celoso en cuanto al origen de ellos. Según la investigación realizada es una banda que opera desde el año 2019. Se identificó que este grupo criminal lanzaron ataques cibernéticos a servidores Citrix ADN sin parches, operando con el envió una publica indicando que daría una clave maestra para lograr descifrar los archivos a las víctimas, su modus operandi se trata de cifrar archivos de la víctima usando AES-256 y RSA-4096 con la condición de agregar extensiones (Thor y Hela). Su procede es enumerar a las víctimas en el portal web utilizados por los delincuentes indicando una breve inscripción de cómo debían descifrar los archivos capturados por ellos. [183]

Los archivos escaneados los encriptan por los delincuentes Ragnarok. Estos son recolectados por ellos y lo agregan a una extensión: “ragnarok_cry”, el cifrado realizado por los atacantes aparecerá en otro archivo llamado: “1.jpg”. Con esta acción terminan el proceso, finalmente se visualizará un archivo de texto: How_To_Decrypt_My_Files.txt en el escritorio del equipo de cómputo. Ransomware está diseñado para el cifrado de archivos y solicitan la recuperación de la información con un lucro económico. Este grupo cibernético utilizan algoritmos criptográficos simétricos o asimétrico. La utilización de las criptomonedas las requiere los atacantes ya que es el método de pago y así logran que no sean rastreados. [184]

Ragnarok en el medio se conoce como ransomware Ware Ragnar Locker, en el mes de abril del año 2020 este grupo cibernético hurto 10 TBytes de información de la empresa de energía portuguesa EDP extorsionando a la compañía, en el que les exigia realizar el pago y así poder recuperar los datos robados. Este ataque tomo datos de extractos bancarios, acuerdos confidenciales de los proveedores, registros de empleados. Esta

---

[182] INFOBAE. Hackeo al Senado: el grupo de ciberdelincuentes Vice Society filtró 30 mil archivos. [Sitio web]. 2022. [Consultado 12 marzo del 2023]. Disponible en:https://www.infobae.com/tecno/2022/03/14/hackeo-al-senado-el-grupo-de-ciberdelincuentes-vice-society-filtro-30-mil-archivos/

[183] PCRISK. ¿Qué es Ragnarok? [Sitio web]. 2022. [Consultado 12 marzo 2023]. Disponible en: https://www.pcrisk.es/guias-de-desinfeccion/9578-ragnarok-ransomware

[184] UNAALDIA HISPASEC. Se publican las claves de descifrado del ransomware Ragnarok. [Sitio web]. 2021. [Consultado 13 marzo 2023]. Disponible en: https://unaaldia.hispasec.com/2021/08/se-publican-las-claves-de-descifrado-del-ransomware-ragnarok.html

banda cibernética ha atacado a varias compañías de Europa afectando en gran manera y si no se hace el pago la data será publicada en la página negra.[185]

6.1.4.5.1 Vectores de ataque Ragnarok: Los métodos más utilizados por el grupo criminal Ragnarok que les ha permitido acceder a la red corporativo y lograr el propósito de hurtar la información confidencial y datos personal para tener un lucro económico que en muchas ocasiones lo han logrado, debido a que las compañías por el temor de perder la información proceden a pagar y que no se haga pública la información ya que podrían perder prestigio. [186]

- **Campañas de spam:** La utilización de este vector de ataque realizado por Ragnarok consiste en el envío de correos masivos donde su contenido son archivos de códigos maliciosos o link con procedencia maliciosa. Estos métodos contienen malware, logran engañar a las víctimas con la finalidad de lograr un lucro económico de lo contrario se hará la propagación del virus en los equipos de cómputo. Con este paso las victimas proceden a realizar la búsqueda de información y luego encriptar la información, su objetivo es extorsionar solicitando dinero para hacer la devolución de los datos, sino se realiza lo indicado por los ciberdelincuentes publicaran la información en la Deep Web.[187]

- **Phishing:** Es uno de los métodos más utilizados por los ciberdelincuentes ya que realizan el envío de correos masivos y su contenido es software malicioso, la victima toma el contenido del correo como legítimo y procede a acceder a los links enviados o la descarga de los archivos, es así como se propaga el malware contaminado de virus los archivos más relevantes de las víctimas, se procede con el cifrado de los datos y el atacante procede con los mensajes solicitando la recuperación de la información secuestrada. [188]

- **Explotación de vulnerabilidades:** Es una de las técnicas más utilizadas por este grupo criminal dado que comenzando con el escaneo de la detección de vulnerabilidades en una red corporativa hasta lograr acceder, realizan cambios en

---

[185] UNAALDIA HISPASEC. Se publican las claves de descifrado del ransomware Ragnarok. [Sitio web]. 2021. [Consultado 13 marzo 2023]. Disponible en: https://unaaldia.hispasec.com/2021/08/se-publican-las-claves-de-descifrado-del-ransomware-ragnarok.html

[186] BLOG. SEGUINFO. Ransomware Ragnarok. [Sitio web]. 2021. [Consultado 13 marzo 2023]. Disponible en: https://blog.segu-info.com.ar/2021/08/publican-claves-maestras-de-ransomware.html?m=0

[187] ¿Qué es el spam y cómo evitar que tus campañas terminen en el correo no deseado? [Sitio web] 2020. [Consultado 11 marzo 2023]. Disponible en: https://www.brevo.com/es/blog/que-es-el-spam-y-como-evitarlo/

[188] NORDVPN. ¿Qué es el RDP, y cómo usarlo con seguridad? [Sitio web]. 2021. [Consultado 11 marzo 2023]. Disponible en: https://nordvpn.com/es/blog/acceso-remoto-rdp/

los privilegios del sistema, con esta brecha de seguridad identificada, accedan al sistema y con esto tiene el privilegio de acceder al sistema y datos de la compañía, con el objetivo de bloquear el sistema y el cifrado de la información. [189]

6.1.4.6 Pysa, este grupo cibernético conocido por su abreviatura Protect Your System Amigo, lo que se conoce de este grupo criminal realizo su aparición por primera en el mes de diciembre del año 2019 se identificó el método de ataque fue con el modelo de Ransomware as a service (RaaS). Se identificó que es la tercera evolución de ransomware mas detectada en el año 2021. El año de la pandemia se reportó el robo masivo de información confidencial en el que se calculó 747 víctimas. Según información reportada por el FBI han atacado países de Europa y Estados Unidos. En el año 2020 han mejorado sus técnicas de ataque quienes han utilizados otros modelos de amenazas. Según las investigaciones del FBI y la agencia de ciberseguridad de Francia se identificó las empresas afectadas fueron sectores de educación como universidades e institutos de educación de alto nivel, agencias gubernamentales de Europa, sector salud y proveedores. Este grupo delincuencial tiene una página donde se pública la información hurtada de las organizaciones, adicional a esto también publican archivos exfiltrados de las compañías que no realizan el pago para la recuperación de la información. [190]

En el 2021, se reportó un total de 307 víctimas quienes corresponde a países como España, Francia, Latinoamérica, Brasil, Argentina, México y Colombia. El modo de ejecución para este tipo de ataques es la creación de hilos de creación para proceder a realizar el cifrado, ingresa al sistema para ser modificado el registro y después procede a preparar el script para lograr examinar el sistema de archivos del equipo de cómputo generando dos listas llamadas Allowlist y Blacklist, se hace un rastreo de detección de archivos con diferentes extensiones e identifican el tamaño de los archivos. Por último, se incluyen directorios críticos que afectaran el funcionamiento del sistema, logran cifrar todo archivo encontrado. La anterior descripción es la forma en como trabajando los atacantes Pysa para violentar la seguridad de la red corporativa y extraer la información confidencial.[191]

---

[189] KEEPCODING. ¿Qué es la configuración de seguridad incorrecta? [Sitio web]. 2021. [Consultado 5 mayo 2023]. Disponible: https://keepcoding.io/blog/que-es-la-configuracion-de-seguridad-incorrecta/

[190] THEHACKERNEWS. Los investigadores comparten un análisis en profundidad del grupo de ransomware PYSA. [Sitio web]. 2022. [Consultado 15 marzo 2023]. Disponible en: https://thehackernews.com/2022/04/researchers-share-in-depth-analysis-of.html

[191] Pcrisk. ¿Qué es Pysa? [Sitio web]. 2022. [Consultado 14 marzo del 2023]. Disponible en: https://www.pcrisk.es/guias-de-desinfeccion/9666-pysa-ransomware

De acuerdo, a lo anterior en Colombia se reportó la afectación de tres compañías quienes fueron víctimas de un ataque cibernético que afecto la información sensible y confidencial de las compañías Famisanar, SiesaCloud y Red de salud de Ladera denegando todas las operaciones y servicios siendo uno de los delitos más cometidos a través de internet.[192]

6.1.4.6.1 Vectores de ataque Pysa: El grupo criminal utiliza estrategias de operación humana, es decir, engañando a sus víctimas con técnicas de extorción y engaño. Uno de los análisis que realiza el grupo Pysa es la detección de usuarios que desconocen estos métodos de ataque ya que para ellos es una vulnerabilidad detectada con la finalidad de acceder al sistema o red corporativa. Se ha descubierto que el grupo delincuencial Pysa descarga el ransomware en el sistema, quienes utilizan herramientas de pentesting realizando tareas de reconocimiento con la finalidad de recolectar credenciales, contraseñas, modificación de perfiles y privilegios de acceso al sistema.

- **Phishing:** Una de las características que define el grupo criminal Pysa es su comportamiento en cuanto a la operatividad humana, expone a los usuarios el desconocimiento en temas de ciberseguridad. Es así, como utilizando en método de Phishing (Correo electrónico) que consiste en enviar correos masivos con el contenido de software malicioso, páginas web con procedencia delictiva, logrando que las victimas a raíz del mensaje enviado se sienta en la confianza de acceder a los links o realizar descargas de los archivos adjuntos que contienen código malicioso. De esta manera logran descargar el malware en el sistema obteniendo la propagación del ransomware, para que el software malicioso acceda a la información sensible y luego encriptarla, a fin de cobrar el rescate de los datos accedidos de manera no autorizada. [193]

- **Spearphishing:** Este vector de ataque es uno de los más utilizados por los delincuentes cibernéticos dado que su manera de engañar lo realizan a un objeto especifico, utilizando el envío de correos electrónicos logrando obtener información personal de la víctima. [194]

[192] Pcrisk. ¿Qué es Pysa? [Sitio web]. 2022. [Consultado 14 marzo del 2023]. Disponible en: https://www.pcrisk.es/guias-de-desinfeccion/9666-pysa-ransomware
[193] CYBEREASON. Informe de análisis de amenazas: dentro del destructivo ransomware PYSA. [Sitio web]. 2021. [Consultado 15 marzo del 2023]. Disponible en: https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-destructive-pysa-ransomware
[194] WELIVESECURITY. Ransomware PYSA: características de uno de los grupos más activos de 2021. [Sitio web]. 2021. [Consultado 15 marzo 2023]. Disponible en: https://www.welivesecurity.com/la-es/2021/12/27/ransomware-pysa-principales-caracteristicas/

- **Protocolo RDP:** Este método es también uno de los más utilizados por el grupo Pysa ya que acceden a la red corporativa detectando la vulnerabilidad que se llegue a presentar en la conectividad del acceso remoto, si detectan algún equipo pueden tomar el control remoto de esa máquina logrando acceder al sistema de la compañía, luego proceden a descargar el ransomware con la finalidad de capturar la información confidencial de la compañía para cobrar el rescate de la misma. [195]

- **Suplantación de identidad:** Esta técnica usada por los delincuentes cibernéticos consiste en hacerse pasar por la víctima con el propósito de engañar y extorsionar a personas allegadas de persona afectada para obtener un lucro económico y dañar la reputación de la víctima.

- **Smishing:** Este método de ataque consiste en el envío de mensajes de texto a la víctima, el contenido del mensaje lo hacen ver como legítimo de una compañía, banco, entidad pública, red social, entre otros quienes utilizan técnicas de ingeniera social con la finalidad de engañar al usuario y poder obtener los datos personales como accesos a cuentas bancarias, contraseñas de accesos a bancos. [196]

6.1.4.7 BlackByte, esta organización criminal hizo su primera aparición en el mes de septiembre del año 2021, cuyas publicaciones se visualizaron en la página web de extorsión, su principal característica de este grupo es modificar los nombres de los archivos y luego son bloqueados para no permitir el acceso. [197]

Se conoció que la compañía Retail ABCDIN tuvieron un ataque cibernético, la modalidad implementada fue el cifrado de datos. La afectación generada a esta compañía fue de 1.5 millones de RUTs clientes logrando tomar captura de pantalla y publicaron los datos sensibles de la compañía y fue publicada en la página Deep web. [198]

El grupo cibernético ransomware Blackbyte desde el 2021 han realizado ataques en tres organizaciones del sector de infraestructuras criticas donde se han centrado para realizar

---

[195] NORDVPN. ¿Qué es el RDP, y cómo usarlo con seguridad? [Sitio web].2021. [Consultado 15 marzo 2023]. Disponible: https://nordvpn.com/es/blog/acceso-remoto-rdp/

[196] INCIBE. Smishing. [Sitio web]. 2022. [Consultado 15 marzo 2023]. Disponible:https://www.incibe.es/aprendeciberseguridad/smishing

[197] PCRISK. ¿Qué es el ransomware BlackByte? [Sitio web]. 2021. [Consultado 15 marzo de 2023]. Disponible en: https://www.pcrisk.es/guias-de-desinfeccion/10872-blackbyte-ransomware

[198] CRONUP. Ransomware BlackByte afectó a empresa nacional de Retail. [Sitio web]. 2021. [Consultado 15 marzo 2023]. Disponible en: https://www.cronup.com/ransomware-blackbyte-afecto-a-empresa-nacional-de-retail/

extorsión y ataques en empresas de Estados Unidos. Según lo informado por el FBI y el servicio de los Estados unidos, han alertado que la utilización de técnicas más utilizadas en RaaS con la finalidad de atentar contra el sector financiero, sector salud e instalaciones gubernamentales. Por consiguiente, encripta archivos en sistemas host de Windows de los que se incluyen servidores virtuales y físicos. [199]

Uno de los ataques cibernéticos más conocidos fue la liga nacional de fútbol americano San Francisco 49ers, tomaron los datos financieros y encriptaron la información. Se dio a conocer que la banda cibernética BlackByte realizo publicaciones en el blog de ellos donde se visualizaba datos de la liga de nacional de futbol se filtraron 300 MB de archivos. BlackByte está utilizando una herramienta llamada ExByte que consiste en la extracción de datos personales e información confidencial, con la finalidad de acceder a dispositivos y equipos de cómputo y estos deben tener sistemas operativos Windows. Esta herramienta fue implementada por este grupo cibernético crea filtros con funciones de ataques de doble extorsión la intensión de estos delincuentes cibernéticos es el pago por la recuperación de la data. [200]

Según la investigación realizada por el centro Cibernético de la Policía Nacional se confirmó que la entidad colombiana INVIMA fue por los atacantes cibernéticos BlackByte, ya que se halló malware. Su modus operandi es la utilización del servicio RaaS. Encripta archivos del sistema Windows, servidores virtuales y físicos. La técnica utilizada fue explorar las vulnerabilidades de la red corporativa del INVIMA accediendo al software Microsoft Exchange Server para obtener el acceso del inicio de la red, logrando captar la información y realizar el cifrado de la misma. [201]

---

[199] CRONUP. Ransomware BlackByte afectó a empresa nacional de Retail. [Sitio web]. 2021. [Consultado 15 marzo 2023]. Disponible en: https://www.cronup.com/ransomware-blackbyte-afecto-a-empresa-nacional-de-retail/

[200] PORTAL CCI ENTEL. BlackByte utiliza nueva herramienta de robo de datos para doble extorsión. [sitio web]. 2022. [Consultado 15 marzo de 2023]. Disponible en: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1400/

[201] ITECHSAS. Ciberataque a Invima por BlackByte deja pérdidas por $15.000 millones semanales. [Sitio web]. 2022. [Consultado 15 marzo del 2023]. Disponible en: https://www.itechsas.com/blog/ciberseguridad/ciberataque-a-invima-por-blackbyte-deja-perdidas-por-15-000-millones-semanales/

6.1.4.7.1 Vectores de ataque BlackBye: Este grupo cibernético tiene modalidad es realizar ataques por medio de la detección de vulnerabilidades en el sistema, empleando un modelo comercial de ciberdelincuencia accediendo a ransomware ya implementados por otros atacantes, les permite registrarse en el sistema para después colocarlo como modelo de tradición de distribución de software. Que procede a bloquear el sistema o archivos de una organización. Se detectaron vectores de ataque más utilizados por BlackByte. [202]

- **Explotaciones de vulnerabilidades de ProxyShell:** Este vector de ataque consiste en detectar las vulnerabilidades existentes en el servidor de Microsoft Exchange, logrando ejecutar y eliminar las tareas (taskmgr) y el monitor de recursos (resmon) utilizando un comando de PowerShell para así lograr detener todos los servicios de Windows Defender. BlackByte procede a tener el control y el reconocimiento de la red y la preparación del sistema. Este grupo criminal logra capturar la información para luego encriptarla. El último paso, es la extorción a las victimas indicando que será publicada la información confidencial a través de un sitio o web oscura. [203]

- **Campañas de phishing:** Uno de los vectores más atractivos para los delincuentes son los usuarios de las compañías, ya que por su falta de desconocimiento. Engañan a las víctimas ya que se envían correos electrónicos. Logrando que accedan a este tipo de correos con la finalidad de realizar la descarga de malware en los dispositivos y equipos de cómputo. Proceden a escanear la información más relevante realizando el cifrado de los datos para luego extorsionarlos, luego solicitan el rescate de la data robada. Situaciones como estas las víctimas acceden a realizar el pago para evitar que la información sea publicada en los blogs que manejan los atacantes. [204]

[202] ITECHSAS. Ciberataque a Invima por BlackByte deja pérdidas por $15.000 millones semanales. [Sitio web]. 2022. [Consultado 15 marzo del 2023]. Disponible en: https://www.itechsas.com/blog/ciberseguridad/ciberataque-a-invima-por-blackbyte-deja-perdidas-por-15-000-millones-semanales/

[203] ECUCERT. Blackbyte Ransomware. [Sito web]. 2021. [Consultado 15 marzo del 2023]. Disponible en: https://www.ecucert.gob.ec/wp-content/uploads/2022/02/alerta-malware-blackbyte.pdf

[204] BLEEPINGCOMPUTER. El ransomware BlackByte utiliza una nueva herramienta de robo de datos para doble extorsión. [Sitio web]. 2022. [Consultado 16 marzo del 2023]. Disponible en: https://www.bleepingcomputer.com/news/security/blackbyte-ransomware-uses-new-data-theft-tool-for-double-extortion/

6.1.4.8 Avaddon, es un grupo cibernético quienes realizando ataques a diferentes compañías con la finalidad de acceder al sistema para tomar control de los servicios y cifrar la información sensible de las organizaciones. Su primera aparición fue en el mes de diciembre del año 2019 logrando reclutar afiliados a un foro de hacking diseñado por ellos, para un programada llamado Ransomware as a Service ofreciendo una amplia capacidad de configuraciones y múltiples opciones de acceso a los sistemas. Los ataques cibernéticos han afectado a empresas y organizaciones en todo el mundo y que incluye países de Latinoamérica. [205]

Las modalidades que adoptaron es el método doxing que consiste en hurtar la información de los sistemas comprometidos, antes de realizar el cifrado este grupo criminal procede a enviar amenazas, quienes les indicaran la publicación de la data, sino acceden a realizar los pagos correspondientes ellos realizaran la publicación de la data retenido. Los ciberdelincuentes adelantan ataques de DDoS sobre sitios de las víctimas, con la finalidad de interrumpir el funcionamiento del sistema e inhabilitar el acceso de los usuarios. Cuando Avaddon accede al sistema toma el reconocimiento para identificar las bases de datos, el backup de información, copias de seguridad y realizan el escaneo de privilegios en la red corporativa. Avaddon es utilizado por correos phishing con códigos maliciosos y estos contienen extensión .zip. [206]

Al realizar la investigación de este grupo cibernético Avaddon se puede evidencia la manera en como utilizan diversas técnicas de ataque. Es por esto, que Colombia también fue afectada por estos atacantes cibernéticos, como le sucedió a la compañía FebanColombia que es un Fondo de empleados del Grupo Bancolombia quien fue una de las entidades atacadas por Avaddon con este se comprueba que las compañías colombianas tienen vulnerabilidades que aún no se han resuelto y apuntan la falta de capacitación en ciberseguridad y esto ocasiona grandes brechas de seguridad.

---

[205] SEMANA. Avaddon, el ataque tipo ransomware que amenaza a Latinoamérica. [Sitio web]. 2021. [Consultado 16 marzo del 2023]. Disponible en: https://www.semana.com/economia/capsulas/articulo/avaddon-el-ataque-tipo-ransomware-que-amenaza-a-latinoamerica/202132/

[206] HERALDODEMEXICO. Avaddon, una amenaza para América Latina. [Sitio web]. 2021. [Consultado 16 marzo del 2023]. Disponible en: https://heraldodemexico.com.mx/opinion/2021/6/25/avaddon-una-amenaza-para-america-latina-310029.html

6.1.4.8.1 Vectores de ataque Avaddon: los ataques utilizados por Avaddon más usados es él envió de ransomware y este viene acompañado de ransomware de doble extorsión. Esto nos lleva a pensar que es una modalidad más peligrosa para las compañías de todo el mundo debido a las complicaciones que esto puede ocasionar. Es así como se detalla algunos de los vectores de ataque más comunes en Avaddon.

- **Doble extorsión:** Esta es una de las modalidades más usadas en los atacantes cibernéticos quienes con sus capacidades y experiencia logran cifrar los datos personales e información confidencial de las compañías, esto viene acompañado de una solicitud de rescate para que la víctima realice el pago, si esto no se cumple los atacantes proceden a publicar la información en blogs o paginas denominadas Deep Web, al publicar esta información corre el riesgo que competencias y personas malintencionadas obtengan la confidencial y disponibilidad de la empresa. [207]

- **Doxing:** Este es uno de los métodos más usados por Avaddon consiste en revelar información de una compañía o victima a través de páginas o blogs creadas por estos atacantes. La información se publica sin el consentimiento de la víctima esto lo realizan con la finalidad de revelar las identidades de las organizaciones, ocasionando desprestigio a la víctima o compañía afectada. [208]

- **Correos de phishing:** Este es un vector de ataque más utilizados para los delincuentes cibernéticos, por medio del envío de correos electrónicos que contienen archivos con código malicioso y estos tienen una extensión .zip, en otras ocasiones tienen links donde se direcciona a una página maliciosa, pero se puede visualizar como una página legitima de una entidad bancaria o gubernamental. [209]

De acuerdo a lo anterior, los métodos de ataque de los principales grupos cibernéticos que han afectados diversas empresas en Colombia. Afectaron en gran manera. De esta manera se evidencio en la finalización del año 2022 y comienzos del año 2023 un incremento de ataques de ransomware bastante alto, según las investigaciones

---

[207] UNAALDIA HISPASEC. El ransomware Avaddon empieza a utilizar ataques DDoS como extorsión. [Sitio web]. 2021 [Consultado 17 marzo de 2023]. Disponible en: https://unaaldia.hispasec.com/2021/01/el-ransomware-avaddon-empieza-a-utilizar-ataques-ddos-como-extorsion.html

[208] kaspersky. Doxing: definición y explicación. [Sitio web] 2022. [Consulta 1 mayo 2023]. Disponible: https://latam.kaspersky.com/resource-center/definitions/what-is-doxing

[209] BLEEPINGCOMPUTER. El ransomware BlackByte utiliza una nueva herramienta de robo de datos para doble extorsión. [Sitio web]. 2022. [Consultado 16 marzo del 2023]. Disponible en: https://www.bleepingcomputer.com/news/security/blackbyte-ransomware-uses-new-data-theft-tool-for-double-extortion/

realizadas de 34 compañías en Colombia tuvieron una afectación en sectores educativos, salud, servicios públicos, entidades gubernamentales, tecnología, manufactura, entre otros sectores. Como se observa en la ilustración 11 se visualiza los grupos delincuenciales y las empresas afectadas por ransomware.

Ilustración 14. Principales grupos cibernéticos.

Fuente: INFOBAE. Las 34 empresas que fueron hackeadas en Colombia durante 2022. [Sitio web]. 2023. [Consultado 16 marzo de 2023]. Disponible en: https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/

De esta manera podemos observar Colombia registro más de 54 mil denuncias por delitos cibernéticos, sobre los casos más comunes son los ataques Ransomware y afectan los dispositivos y equipos de cómputo. Esta modalidad es uno de los ataques más agresivos que ha tenido las compañías colombianas, sino por la afectación generada al destruir o publicar la data delas compañías. Este incremento determina la falta de cultura cibernético por parte de los empleados. Es importante tener presente que la

ciberseguridad es de interés de todos aquellos que a diario interactúan en internet, con los recursos tecnológicos y el ciberespacio. [210]

Es muy importante capacitar a los usuarios para que tenga claro los diversos métodos de ataque y no estén expuestos a los atacantes cibernéticos ya que el modelo de engaño es lograr persuadir a los usuarios por medio de la ingeniera social. Las organizaciones colombianas deben implementar nuevas estrategias e invertir en la infraestructura tecnológica, programas de seguridad digital ya que este es un valor agregado. Esto hace parte de una mejora y es una necesidad. Realizar campañas de capacitación de ciberseguridad.

[210] EL TIEMPO. Colombia el segundo país con más ciberataques en 2022. [Sitio web]. 2022. [Consultado 16 marzo de 2023]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-el-segundo-pais-con-mas-ciberataques-en-2022-746276

7 RECOMENDACIONES PARA EL FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA EN LAS ENTIDADES COLOMBIANAS

Hoy en día las entidades colombianas han incrementado su preocupación para mejorar el funcionamiento de los procesos y recursos tecnológicos, lo ideal es mejorar las estratégicas y las políticas de seguridad ya implementadas en las organizaciones. Es importante mantenerse la competencia en términos de calidad, costos y tecnología. Ya que como podemos notar hoy en día es una evolución constante para tener un crecimiento en lo económico y así mismo mantener una buena reputación. Teniendo en cuenta, que el personal de las entidades es un factor fundamental ya que no cuentan con el conocimiento en temas de ciberseguridad: También es importante realizar capacitaciones en seguridad informática. Esto podría fortalecer un poco más la red corporativa y así se evitarían que los atacantes cibernéticos logren detectar esta vulnerabilidad que es tan notoria. Fortalecer la infraestructura tecnológica, generando así un fortalecimiento en la red corporativa. Y no se generaría más problemas a futuro. Esto conlleva, que los intrusos no se puedan aprovechar de las debilidades del personal no capacitado. Se recomienda que las compañías realicen campañas de concientización sobre los riesgos a los que están expuesto al no tener el conocimiento sobre la protección de la seguridad de la información. [211]

Es fundamental que todas las entidades colombianas mantengan una conciencia colectiva, teniendo en cuenta la importancia de valorar y asegurar los activos de las organizaciones. Una de las recomendaciones más importantes para la implementar las estrategias de protección en los sistemas de información. Podemos basarnos en el modelo de seguridad y privacidad de la información con la finalidad de mejorar los estándares de seguridad de la información de las entidades públicas y privadas. Este documento permitirá que todas las organizaciones del estado colombiano puedan generar un plan de seguridad de la información y así poder dar el cumplimiento al documento descrito y desarrollado para tal fin. Este plan de seguridad permitirá tener una orientación más clara y asertiva con la finalidad de detectar las vulnerabilidades existentes en un sistema de información.

[211] PORAFOLIO. Siete consejos para proteger los sistemas informáticos de su compañía. [En línea]. 2017. [Consultado 20 de noviembre 2022]. Disponible en: https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755

7.1 ¿QUÉ PLANES DE TRABAJO SE PUEDEN IMPLEMENTAR PARA MITIGAR LOS ATAQUES CIBERNÉTICOS EN LAS ORGANIZACIONES COLOMBIANAS?

Es importante tener en cuenta que toda organización debe tener políticas de seguridad y procedimientos establecidos para mantener la seguridad en los sistemas de información y la infraestructura ti. ya que cada entidad pública y privada debe contrarrestar los ataques cibernéticos, debido a que los atacantes cibernéticos están constantemente evolucionando y mutando nuevos códigos maliciosos e implementando mecanismos y técnicas, desarrollan estrategias que logren acceder a la red o infraestructura tecnológica sin ser identificados. [212]

De este modo, es importante tener planes de acción para mitigar y evitar amenazas cibernéticas. A continuación, se documenta dos fases para lograr cumplir y establecer los planes de trabajo para las entidades colombianas.

7.1.1 **Fase de Prevención**, es fundamental construir entornos informáticos que eviten el acceso a los atacantes cibernéticos y así mismo crear entornos preventivos que logren bloquear los accesos no autorizados e incorporando medidas de prevención. Como las que se describen a continuación, se pueden implementar medidas preventivas corporativas: [213]

- Fomentar el desarrollo al interior de las compañías de buenas prácticas en cuanto a la gestión de fuga de información.
- Determinar políticas de seguridad de las cuales estén acompañadas con métodos para los ciclos de vida de la data.
- Determinar roles y niveles de acceso de la data o cualquier sistema que se requiera.
- Disponer de un sistema de distribución de información
- Administración y control de dispositivos extraíbles, es decir, USB, discos duros extraíbles, CD, entre otros.
- Crear políticas de clean desk se establece un código de responsabilidad compartida entre los usuarios finales, manteniendo la seguridad y en las estaciones de trabajo.

---

[212] INFOSECURITYMEXICO. Ciberseguridad, amenazas y estrategias. [Sitio web]. 2022. [Consultado 3 de marzo 2022]. Disponible en: https://www.infosecuritymexico.com/es/ciberseguridad.html#ciberataques

[213] INCIBE. Ransomware: una guía de aproximación para el empresario. [Sitio Web]. 2020. [Consultado 3 marzo 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

- Implementar un sistema de control de acceso, cabe aclarar que esta medida aplica para los accesos físicos de las instalaciones de la compañía, este sistema aplique en los equipos de cómputo y sistema de comunicación.
- Proponer planes de formación en relación a ciberseguridad y la seguridad de la data, fomentar buenas prácticas en el manejo de los recursos tecnológicos. Teniendo en cuenta que se debe sensibilizar a los usuarios finales.
- Realizar contratación de personal especializado en materia de ciberseguridad, cuya finalidad es proteger todas las entidades públicas y privadas, ante cualquier incidente de riesgo o amenazas cibernéticas. Tener en cuenta el uso inadecuado de los recursos tecnológicos.
- Generar un plan de respuestas ante cualquier incidente presentado.

De acuerdo a la anterior y tomando como base la fase de prevención, se puede implementar medidas preventivas legales, estas permiten dar un cumplimiento de protección de datos y el reglamento de desarrollo (LOPD y RLOPD), es importante establecer principios que esto conlleva para el desempeño de cada función de los trabajadores o usuarios finales. Se identificaron los siguientes ítems:[214]

- La aceptación de la política de seguridad para todos los usuarios de la compañía.
- Cláusulas contractuales para los empleados en relación en la conservación y uso de la información brindada por la compañía.
- Cláusulas contractuales a proveedores externos en cuanto a la confidencialidad de la compañía.
- Determinar una política de seguridad para el manejo de los recursos tecnológicos de la compañía. Definir las políticas el alcance de uso de los medios extraíbles que estén en disposición del usuario por parte de la compañía y control de funciones.

7.1.2 Fase de Detección, es importante detectar los incidentes que se lleguen a presentar en una fuga de información ante cualquier entidad, es así, como se determina una buena gestión para la detección de cualquier amenaza que se llegue a presentar y lograr mitigar los riesgos y amenazas. Sin embargo, se pueden definir medidas legales y corporativas. [215]

[214] INCIBE. Ransomware: una guía de aproximación para el empresario. [Sitio Web]. 2020. [Consultado 3 marzo 2022]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

[215] INFOSECURITYMEXICO. Ciberseguridad, amenazas y estrategias. [Sitio web]. 2022. [Consultado 3 de marzo 2022]. Disponible en: https://www.infosecuritymexico.com/es/ciberseguridad.html#ciberataques

Para esta fase se implementarán medidas de detección legales, a continuación, se describen de la siguiente manera:

- Según el reglamento de protección de datos, se debe reconocer y registrar los incidentes y estos deben ser plasmados en documentos de seguridad de la compañía, debe ser actualizado periódicamente. Debe plasmar: tipo de incidencia, fecha en el que fue detectado, quien lo notifica, nombre de la persona quien hace la notificación, efecto que deriva la incidencia y las medidas a tomar.

- La compañía debe tener un documento de tratamiento de datos, en el que se plasme los registros, el método de recuperación, nombre de la persona quien realizo la recuperación y nombre la información que fueron recuperación.

En esta fase se toman medidas legales también aplican las medidas de detección corporativas, de las cuales se describen de la siguiente manera:

- Estructurar protocolos internos en cuanto a la gestión de incidentes donde se identifique la criticidad y se tomen las medidas correspondientes.
- Mantener personal especializado que logren gestionar y manejar cualquier situación que se llegue a presentar.
- Identificar los riesgos que se presenten en las organizaciones, evidenciar el activo afectado determinando las causas, los posibles efectos, establecer el origen, determinar el nombre y fecha del ataque.
- Realizar auditorías periódicas con la finalidad de detectar las posibles fallas que se presenten en los procesos, aplicaciones o recursos tecnológicos.
- Llevar a cabo buenas prácticas para el manejo de los recursos tecnológicos y hacer buen.
- Administrar correctamente los permisos asignados a los usuarios según el rol o función. Es importante monitorear los accesos a los que se le dará uso según función y cargo.
- Implementar mecanismos y sistemas de seguridad perimetral, mantendrán el control de los accesos no autorizados de personas a la red corporativa, infraestructura y sistemas de información. [216]

[216] UNIR. Seguridad perimetral informática: Objetivos y plataformas. [Sitio web]. 2023. [Consultado 19 de febrero 2023]. Disponible en: https://www.unir.net/ingenieria/revista/seguridad-perimetral-informatica/

7.1.3 Recomendaciones para mitigar los ataques Ransomware, es importante aprender medidas de prevención y protección que permitirán cuidar la infraestructura y los recursos tecnológicos para las organizaciones. Es importante tener una protección adecuada para evitar y minimizar los ataques cibernéticos.

Cuando se realiza un Análisis sobre los ataques cibernéticos existentes actualizaciones que han afectado a las organizaciones, se debe proteger y resguardar los sistemas informáticos y la data. Se deben tomar acciones para la protección de la información:[217]

- **Realizar copias de seguridad**: Se debe garantizar las copias de seguridad de información, ya que en el momento de sufrir un ataque existirá un respaldo de la data.

- **Implementación de protección en la red:** La protección contra ransomware no se limita en bloquear la red o puertos sino forzar la seguridad con anti-spyware, firewall, antivirus, entre otros.

- **Plan en contingencia en caso de ataques cibernéticos:** Se debe tener un plan de contingencia que den respuestas a incidentes con la finalidad de evitar tiempos de inactividad.

- **Adquirir expertos en el campo de ciberseguridad:** Lo ideal es destinar nuevos recursos con personal especializado en ciberseguridad y deben estar capacitados en el caso que se lleve a presentar cualquier eventualidad.

- **No realizar los pagos solicitados por los ciberdelincuentes:** Hay que tener en cuenta que los atacantes logran convencer a las víctimas para que accedan a pagar con la condición de recuperar la información. Por eso es importante que las organizaciones realizan respaldos, backup de información. En el caso que se llegue a presenta no será necesario hacer esos pagos para la recuperación de los datos o lograr restaurar los archivos.

- **Siempre estar alerta:** Es importante tener métodos de detección de intrusos, que se puedan detectar a tiempo y se logre proteger el sistema y la data.

[217] TECNOZERO. Sophos pública su estudio: El estado del ransomware en 2021. [Sitio web]. 2021. [Consultado 20 de noviembre 2021]. Disponible en: https://www.tecnozero.com/antivirus-y-anti-ransomware/sophos-publica-su-estudio-el-estado-del-ransomware-en-2021/

- **Sensibilizar a los usuarios:** Es importante realizar capacitaciones periódicas sobre el manejo y el funcionamiento de los aplicativos, equipos de cómputo. La finalidad es identificar si existe algún acceso indebido a páginas web o correos electrónicos. Se logre tomar las precauciones necesarias para no acceder a enlaces de procedencia sospechosa. Ya que pueden contener contenido de malicioso como Malwar.[218]

- **Protección de redes inalámbricas:** Es necesario proteger las redes inalámbricas y redes locales, reforzar las contraseñas y controlar el acceso a usuarios que no pertenezcan a la entidad y quieran acceder a las redes inalámbricas ya que estas son una de las vulnerabilidades. Los atacantes se provechan de esta situación y acceden a la red de las compañías. Es importante tomar las siguientes medidas: [219]

  - Utilizar contraseñas con ciertos parámetros exigentes, esto con el fin de que no sean detectadas. Y realizar los cambios de contraseñas periódicamente.
  - Es muy importante cifrar los datos, habilitar el cifrado en la configuración de cada conexión que se realicen.
  - Protección contra malware, se recomienda instalar aplicaciones antimalware y estas deben tener actualizadas automáticas.
  - Realizar cambio del nombre del SSID de los dispositivos a utilizar.

- **Recuperación de información:** Se debe tener en cuenta en el momento de detectar un acceso ilegal en el sistema o infraestructura TI se debe llevar a cabo un plan de recuperación con la finalidad de recuperar el sistema informático y reestablecer el sistema de la organización. Realizar copias de seguridad, backup de información, entre otros.

  Para esta medida de recuperación se deben desarrollar planes de continuidad de negocio donde se contemplen ciertas excepciones donde se originan las amenazas cibernéticas y demás riesgos como hurto de información o bloqueo del

[218] ALSINA RODRÍGUEZ, Juan. (2015). Recomendaciones para prevenir ciberataques (Bachelor's thesis, Universidad Piloto de Colombia). 1-5 p. Disponible en: http://polux.unipiloto.edu.co:8080/00002056.pdf
[219] ESEDSL. Consejos para proteger tus redes inalámbricas. [En línea]. 2020. [Consultado 2 noviembre 2022]. Disponible en: https://www.esedsl.com/blog/consejos-proteger-tus-redes-inalambricas

sistema. Se sugiere realizar informes, en el que se plasme todas las pruebas necesarias que permitan hacer la respectiva investigación. [220]

- **Fortalece la seguridad de la información:** Cuando se identifican las necesidades a nivel de seguridad informática. Es fundamental incluir una serie de recomendaciones que permitirán salvaguardar los sistemas de información y la infraestructura TI. Es importante disponer de un esquema de ciberseguridad. Teniendo en cuenta las siguientes recomendaciones:[221]

  - Implementar mecanismos de defensas para el tráfico de la red de las compañías.
  - Fortalecer las políticas de seguridad y configurar las reglas firewall, manteniendo el control y la administración constante de estos dispositivos.
  - Establecer un servidor Proxy que filtre el contenido de las páginas web.
  - Segmentar la red corporativa esto evitara los ataques cibernéticos. Se evitará la propagación en la red.
  - Sistema de Detección de Intrusión de red enviara alertas ante cualquier ataque o riesgo que se llegue a presentar.
  - Mantener actualizado el sistema operativo, aplicaciones de la entidad y estos cuenten con parches de implementación.
  - Establecer políticas de restricción en la utilización de software.
  - Establecer privilegios para los usuarios finales según los roles requeridos por la entidad.
  - Realización de backup, copias de seguridad y planes de recuperación.

De acuerdo a lo anterior, es importante tomar estas medidas necesarias para mantener a salvo la información de las compañías. Toda organización debe tener medidas para asegurar la infraestructura tecnológica, logrando reducir las brechas de seguridad.

Es importante mantener la seguridad de la información en las entidades colombianas, es así, como se describe en el siguiente cuadro los controles de seguridad según las normas

---

[220] REVISTA SEGURIDAD 360. 10 consejos de ciberseguridad personal. [En línea]. 2022. [Consultado 3 marzo 2022]. Disponible en: https://revistaseguridad360.com/destacados/consejos-de-ciberseguridad/

[221] OWASP. Guía Contra Ransomware. [En línea].2020. [Consultado 4 de marzo 2022]. Disponible en: https://owasp.org/www-pdf-archive/Guia_Contra_Ransomware.pdf

ISO/IEC 27001 y NIST que se pueden implementar para mitigar y minimizar las brechas de seguridad. Tabla 1.

Tabla 1. Controles de seguridad para ataques cibernéticos Ransomware.

Grupo delincuencial	Vector de ataque	Controles ISO27001	Controles NIST
BlackCat	Phishing.	A.9.1.1 Política de control de acceso.	CCS7. Protección del Correo Electrónico y del Navegador.
RansomHouse	Denegación de servicio.	A.9.4.1 Restricción de acceso a la información.	CCS9. Limitar y Controlar los Puertos de Red, Protocolos y Servicios.
LockBit	Campañas de spam.	A.9.2.3 Gestión de derechos de acceso privilegiado.	CCS8. Defensas Contra el Malware Avanzado de Correo Electrónico y del Navegador.
ViceSociety	RaaS	A.9.1.2 Acceso a redes y servicios de red.	CCS11. Configuraciones Seguras de Dispositivos de Red (Firewalls, Routers y Switches).
Ragnarok	Explotación de vulnerabilidades.	A.9.4.3 Sistema de Gestión de Contraseñas.	CCS2. Inventario de Software Autorizado y no Autorizado.
Pysa	Spearphishing.	A.9.2.1 Registro de usuarios y anulación de registro	CCS3. Configuraciones Seguras de Software y Hardware para Dispositivos Móviles, Portátiles, Equipos de Escritorio y Servidores.
BlackByte	Explotaciones de vulnerabilidades de ProxyShell.	A.9.1.2 Acceso a redes y servicios de red	CCS4. Proceso Continuo de Identificación Y Remediación de Vulnerabilidades.

Avaddon	Doble extorsión.	A.9.2.3 Gestión de derechos de acceso privilegiado.	CCS13. Protección de los Datos.

Fuente: Elaboración propia.

Es recomendable que todas las organizaciones implementen controles de seguridad, con la finalidad de mantener estrategias que permitan controlar los datos y los sistemas de información, logrando minimizar los riesgos que se puedan presentar al estar expuestos ante un ataque cibernético. Manteniendo a salvo los activos de la compañía. Realizar de inventario tanto software y hardware, con esta información se tendrá más control sobre aquellas aplicaciones que puedan ser blanco de ataque cibernético.

Los controles de seguridad que se puedan aplicar a las entidades colombianas son las mejores prácticas con la finalidad de tomar acciones a tiempo y monitorear la red corporativa, la infraestructura tecnológica y siempre manteniendo una mejora continua.

8 CONCLUSIONES

En la presente monografía proporciona una visión detalla ante las amenazas cibernéticas más persistentes que refiere los ataques ransomware, en las que se han enfrentado las organizaciones colombianas durante los últimos cinco años. Es así, que se toma como referencia la información recolectada, por fuentes especializadas en ciberseguridad, reportes y estadísticas dadas por las autoridades competentes y expertos en ciberseguridad CIRT, en las que se identificaron métodos, técnicas y vectores de ataque donde se compromete la seguridad cibernética y la estabilidad de operaciones de las entidades públicas. Esto con lleva a tener impactos significativos como perdida de información, daño en los recursos tecnológicos, exposición de datos sensibles y afectación en la reputación empresarial. Ante estas situaciones los atacantes cibernéticos han logrado en algunos casos cobrar rescate económico por la información secuestrada.

Es importante resaltar que, aunque se han detectado comportamientos recurrentes y tendencias en los ataques ransomware en Colombia, las entidades se enfrentan a grandes desafíos en cuanto a las políticas de seguridad, infraestructura tecnológica y cultura organizacional. Por lo anterior, es necesario tener estrategias bien estructuradas con la finalidad de minimizar el impacto ante los ataques cibernéticos, con el propósito de adaptarse a las necesidades de cada entidad colombiana.

La evolución que ha tenido ransomware durante los últimos años, se ha notado notalmente ya que se han implementado nuevas tácticas y con el nuevo surgimiento de variables más avanzadas y destructivas como: WannaCry, NotPetya y Ryuk, en las que han afectado de manera masiva a grandes compañías colombianas, en los que van dirigidos los ataques cibernéticos a sectores como salud, servicios públicos, entidades financieras, educación, entre otros.

Por esta razón, es fundamental que las organizaciones lleven a cabo acciones preventivas de seguridad cibernética, concientización en temas relacionados con ciberseguridad al personal, respaldo de información, implementación de soluciones y medidas de seguridad en ciberseguridad más robustas, actualización y aplicación de parches de seguridad. Por otro lado, disponer de planes de soluciones a incidentes que proporcionen a las entidades actuar de forma efectiva ante un ataque cibernético.

Finalmente, esta monografía permite proporcionar una visión más integral en la que resaltar que los ataques ransomware y ante el crecimiento de amenazas cibernéticas,

surge la necesidad de unir fuerzas entre el gobierno colombiano y empresas de ciberseguridad que puedan implementar medidas de prevención robustas y sólidas para poner en marcha soluciones de seguridad avanzadas y planes de recuperación ante ataques cibernéticos. Con la finalidad de proteger la integridad de la información y fortalecer las defensas cibernéticas, que permitan resguardar la información, evitando la propagación del malware en todo el sistema.

9 RECOMENDACIONES

Para minimizar los riesgos ante estos ataques cibernéticos es importante tener en cuenta la siguiente recomendación con la finalidad que cuenten con medidas preventivas necesarias logrando mitigar este tipo de amenazas en los sistemas de información.

Disponer de un plan de acción en seguridad cibernética en el que abarque medidas preventivas, en las que se obtengan respuestas ante incidentes que se lleguen a presentar. Con el objetivo de disminuir los riesgos asociados a los ataques cibernéticos y tener el conocimiento para dar manejo en el caso de que se materialicen. También es importante construir procesos sistemáticos para el análisis de ataques cibernéticos ransomware en el que se logre recopilar y examinar información detalla de estos eventos y que han afectado a os organizaciones colombianas dentro de un periodo especifico. [222]

Teniendo en cuenta lo anterior, es importante incluir los siguientes aspectos: mantener actualizados los sistemas de información, recurso tecnológico, implementar soluciones firmes como la detección de intrusos, antivirus, uso de firewall en el que se definan políticas de seguridad solidas en el que controle e impida el acceso de intrusos o tráfico no autorizado. Se recomienda que toda entidad de uso de herramientas de seguridad, esto permitirá proteger la red donde se pueda controlar y monitorear el tráfico de la red.

Realizar un análisis detallado de los ataques ransomware, es importante para recopilar información minuciosa sobre los estudios de ataques cibernéticos, en el que se puedan abarcar informes de incidentes generados de seguridad que han sucedido en las organizaciones colombianas. Estudiar los casos para identificar las vulnerabilidades o posibles fallas que se presentaron en las organizaciones colombianas afectadas. Esta identificación ayudará a descubrir técnicas utilizadas por los ciberdelincuentes y el uso de ransomware, esto ayudara a establecer los vectores de ataque, cual fue el método de propagación de ransomware y las peticiones de rescate. Con la identificación de estas acciones es importante tener en cuenta, realizar sugerencias para mejorar la seguridad de la información y prevenir este tipo de ataques.

Realizar una evaluación exhaustiva de las vulnerabilidades existentes en las entidades colombianas que puedan ser explotadas por un ataque ransomware. Con el propósito de

[222] PORTAFOLIO. Siete consejos para proteger los sistemas informáticos de su compañía. 2017. [Sitio web]. [Consultado 02 de marzo 2022]. Disponible en: https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755

identificar las brechas de seguridad y las posibles debilidades de un sistema y lograr reducir el riesgo sobre los impactos presentados en las organizaciones. Se debe tener en cuenta, la importancia de hacer un análisis detallado sobre las vulnerabilidades más comunes en los sistemas de información, red corporativa y recurso tecnológico. Cabe destacar que se deben realizar informes de seguridad, análisis de incidentes reportados anteriormente y bases de datos de vulnerabilidades conocidas. Una vez identificadas las vulnerabilidades se debe dar priorizar teniendo en cuenta la criticidad explotación de los ataques cibernéticos. Con esta información detallada, las organizaciones se enfocarán en los recursos en la mitigación de las vulnerabilidades más críticas, logrando reducir el impacto que puede ocasionar este tipo de ataques cibernéticos. [223]

Basándonos en lo anterior, se deberán desarrollar estrategias para fortalecer la seguridad, implementando parches de seguridad, mejorar las políticas de seguridad de autenticación y capacitación del personal de las organizaciones.

Fomentar un programa integral de concienciación en seguridad cibernética, como capacitaciones que sean dirigidos a los usuarios y los administradores del sistema de las entidades colombianas. Esto con el fin de fomentar buenas practicas, en el que puedan identificar posibles amenazas o ataques cibernéticos para evitar caer en la trampa de los ciberdelincuentes. Diseñar materiales de capacitación que planteen aspectos importantes de ciberseguridad, el reconocimiento de phishing, detección de accesos indebidos como páginas web con procedencia fraudulenta y el uso seguro de contraseñas o accesos de sistemas de información. [224]

De este modo, es importante promover una cultura en ciberseguridad dentro de las compañías incentivando la comunicación más asertiva entre diferentes áreas de las organizaciones según el nivel jerárquico. Y por último crear canales de comunicación en el que permitan reportar incidentes cibernéticos en los que se lleguen a presentar.

---

[223] MINTIC. Gobierno Nacional eleva recomendaciones ante variantes de los ataques Ransomware "WannaCry". 2017. [Sitio web]. [Consultado 02 de marzo 2022]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/51612:Gobierno-Nacional-eleva-recomendaciones-ante-variantes-de-los-ataques-Ransomware-WannaCry

[224] MICROSOFT. Las contraseñas deben cumplir los requisitos de complejidad. 2021. [Sitio web]. [Consultado 02 de marzo 2022]. Disponible en: https://docs.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

BIBLIOGRAFÍA

ACIS. ¿Cómo va Colombia en materia de Ciberseguridad? [Sitio web]. 2020. [Consultado 16 de agosto 2021]. Disponible de: https://acis.org.co/portal/content/noticiasdelsector/%C2%BFc%C3%B3mo-va-colombia-en-materia-de-ciberseguridad

ALSINA RODRÍGUEZ, Juan (2015). Recomendaciones para prevenir ciberataques (Bachelor's thesis, Universidad Piloto de Colombia). 1-5 p. Disponible en: http://polux.unipiloto.edu.co:8080/00002056.pdf

ANGARITA PINZÓN, Cristian y GUZMÁN FLÓREZ, Camilo. (2017). Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá. 22-29 p. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/15321/1/Cibersecurity%20Home.pdf

ASUNTOS LEGALES. Los ataques cibernéticos aumentaron 30% durante el primer semestre de este año según la Fiscalía. [Sitio web]. 2021. [Consultado 28 de agosto 2021]. Disponible en: https://www.asuntoslegales.com.co/actualidad/los-ataques-ciberneticos-aumentaron-30-durante-el-primer-semestre-de-este-ano-3198212

CÓRDOBA BAHAMON, José (2016). Malware: una puerta a la cibercriminalidad (Bachelor's thesis, Universidad Piloto de Colombia). 4-8. Recuperado de: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2711/Trabajo%20de%20grado3357.pdf?sequence=1&isAllowed=y

CUJABANTE VILLAMIL, Ximena y BAHAMÓN JARA, Martha. (2020). Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares. Revista Científica General José María Córdova, 18(30), 357-377 p. Disponible en: http://www.scielo.org.co/pdf/recig/v18n30/2500-7645-recig-18-30-357.pdf

DIAROTI. Trend Micro ha lanzado una campaña informativa sobre el Ransomware. [Sitio web]. 2016. [Consultado 29 de agosto 2021]. Disponible en: https://diarioti.com/el-ransomware-en-cifras-y-lo-que-las-organizaciones-deben-saber/98938

DIGITALOO Kaspersky: Más del 25% de ataques Ransomware fue dirigido a empresas. [Sitio web]. 2017. [Consultado 29 de agosto 2021]. Disponible en: https://www.digitaltoo.com/2017/12/05/2017-kaspersky-mas-25-ataques-ransomware-fue-dirigido-empresas/

DOCUMENTO CONPES 3854. (2016). Política Nacional de Seguridad Digital. 12-26 p. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

DOCUMENTO CONPES 3995. (2020). Política Nacional de Confianza y Seguridad Digital. Recuperado de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

EL COLOMBIANO. Hackers secuestraron datos de la Alcaldía de Santa Fe de Antioquia. [En línea]. 2021. Disponible en: https://www.elcolombiano.com/antioquia/seguridad/hackers-secuestran-datos-de-alcaldia-de-santa-fe-de-antioquia-EC15421126

EL ESPECTADOR, "En 2015 aumentaron en 40% los ataques cibernéticos, dice la Policía", 26 de marzo de 2016. [Sitio web]. 2016. [Consultado 29 de agosto 2021]. Disponible en: http://www.elespectador.com/noticias/judicial/20 15-aumentaron-40-los-ataques-ciberneticos-dice-policiarticulo-623568

EL HERALDO. Ciberataque golpeó a 11 empresas y una entidad pública en Colombia. [Sitio web]. 2017. [Consultado 29 de agosto 2021]. Disponible en: https://www.elheraldo.co/ciencia-y-tecnologia/ciberataque-golpeo-11-empresas-y-una-entidad-publica-en-colombia-361747

EL TIEMPO. Los distintos ataques afectan principalmente a empresas y agencias gubernamentales del país. [En línea] (2019). [Consultado 30 de agosto 2021]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesos-al-ano-380830

EUROPAPREES. "El éxito del 'ransomware': cómo se distribuye y qué hacer para prevenirlo". [En línea]. (2016). [Consultado 30 de agosto 2021]. Disponible en: https://www.europapress.es/portaltic/software/noticia-exito-ransomware-distribuye-hacer-prevenirlo-20160709105953.html

EUROPAPRESS. El 'malware' móvil genera más dinero que el 'ransomware' en 2017, según Check Point. [En línea]. 2017. [Consultado 30 de agosto 2021]. Disponible en: https://www.europapress.es/portaltic/ciberseguridad/noticia-malware-movil-genera-mas-dinero-ransomware-2017-check-point-20180222164727.html

ELCONFIDENCIAL. Como el Ransomware se está convirtiendo en la mayor amenaza de Internet. [En línea]. 2017. [Consultado 30 de agosto 2021]. Disponible en: https://www.elconfidencial.com/tecnologia/2015-12-14/como-el-ransomware-se-esta-convirtiendo-en-la-mayor-amenaza-en-internet_1119003/

GALLEGO YUSTE, Alberto (2012). Delitos informáticos: malware, fraudes y estafas a través de la red y cómo prevenirlos (Bachelor's thesis). Disponible en: https://e-archivo.uc3m.es/handle/10016/16868#preview

CEBALLOS LOPEZ, Adriana y BAUTISTA GARCÍA Fredy. (2020). Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo. 12-15 p. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

GONZÁLEZ SOLARTE, Nancy. (2020). Casos de estudio de cibercrimen en Colombia. Universidad Nacional Abierta y a Distancia. Colombia. Nariño. 34 – 37 p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36606/nagonzalezso.pdf?sequence=1&isAllowed=y

GRANMA. La maldición del momento: el ransomware. [En línea]. 2021. [Consultado 6 de noviembre 2021]. Disponible en: https://www.granma.cu/ctrl-f/2021-09-21/la-maldicion-del-momento-el-ransomware-21-09-2021-23-09-29

GUTIÉRREZ TORO, Daryo. Amenazas cibernéticas y su impacto en las organizaciones del sector industrial y servicios de Colombia en la última década. Universidad Nacional Abierta y a Distancia. Riohacha, Colombia. 23 – 30 p. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31937/dlgutierrezt.pdf?sequence=1&isAllowed=y

IDB (2020). [En línea]. Ciberseguridad riesgos, avances y el camino a seguir en América Latina y el Caribe Banco Interamericano de Desarrollo. 20-31 p. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

MEDINA CARRANZA Facundo. (2017). Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible. 13-32 p. Disponible en: https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/13925/MEDINA%20CARRANZA%20FACUNDO%20MARTIN.pdf?sequence=1&isAllowed=y

MINTIC.. Ante posibles ataques cibernéticos, alcaldías y gobernaciones se capacitarán gracias a convenio entre MinTIC y Asobancaria. [Sitio web]. 2021. [Consultado 26 de septiembre 2021]. Disponible en: https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/162457:Ante-posibles-ataques-ciberneticos-alcaldias-y-gobernaciones-se-capacitaran-gracias-a-convenio-entre-MinTIC-y-Asobancaria

SCIELO. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. [Sitio web]. 2020. [Consultado 30 de noviembre 2021]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199

ELESPECTADOR. “Recomendaciones para evitar ataques. [Sitio web]. 2017. [Consultado 30 de noviembre 2021] .Disponible en:”https://www.elespectador.com/judicial/en-2015-aumentaron-en-40-los-ataques-ciberneticos-dice-la-policia-article-623568/

SECURE2. El estado del ransomware 2021. [Sitio web]. 2021. [Consultado 30 de noviembre 2021] Disponible en: https://secure2.sophos.com/es-es/medialibrary/Gated-Assets/white-papers/sophos-state-of-ransomware-2021-wp.pdf

SEMANA. El año de los ciberataques en Colombia, estas son las alarmantes cifras. [Sitio web]. 2021. [Consultado 30 de noviembre 2021]. Disponible en: https://www.semana.com/economia/empresas/articulo/el-ano-de-los-ciberataques-en-colombia-estas-son-las-alarmantes-cifras/202125/

VALOYES MOSQUERA, Amancio. (2019). Ciberseguridad En Colombia. Universidad Piloto de Colombia. Bogotá. 1-12 p. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

VANGUARDIA. ¿Cómo va Colombia en materia de Ciberseguridad?. 2021. [Sitio web]. Disponible en: https://www.vanguardia.com/tecnologia/como-va-colombia-en-materia-de-ciberseguridad-MD3656079

XATAKA. Empresas y entidades públicas colombianas también son víctimas de ataques de ransomware. [Sitio web]. 2017. [Consultado 12 de septiembre 2021]. Disponible en: https://www.xataka.com.co/seguridad/empresas-y-entidades-publicas-colombianas-tambien-son-victimas-de-ataques-de-ransomware