ANÁLISIS DE LOS ATAQUES TIPO RANSOMWARE REALIZADOS DURANTE EL COVID 19 A LAS MIPYMES COLOMBIANAS, POR CAUSA DE VULNERABILIDADES PRESENTES EN LAS INFRAESTRUCTURAS TI Y EN EL PROCESO DE TRANSFORMACIÓN DIGITAL EN LAS ORGANIZACIONES.

LEONIDAS FIQUITIVA CASTRO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

ANÁLISIS DE LOS ATAQUES TIPO RANSOMWARE REALIZADOS DURANTE EL COVID 19 A LAS MIPYMES COLOMBIANAS, POR CAUSA DE VULNERABILIDADES PRESENTES EN LAS INFRAESTRUCTURAS TI Y EN EL PROCESO DE TRANSFORMACIÓN DIGITAL EN LAS ORGANIZACIONES.

LEONIDAS FIQUITIVA CASTRO

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

YENNY STELLA NUÑEZ ALVAREZ
DIRECTOR DE GRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con respecto y cariño dedico este trabajo a mi Madre, mi esposa y mis hijos, que tuvieron paciencia en esta etapa de estudio, dándome mucho ánimo y optimismo para lograr un logro más en mi vida.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional abierta y a Distancia (UNAD), en especial a la Ingeniera Yenny Stella Nuñez Álvarez por brindarme la oportunidad de ampliar mis conocimientos en los sistemas de información y así aportar a mi comunidad.

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ALGORITMOS DE CIFRADO: Es una operación matemática que tiene como fin cifrar un texto claro y hacerlo ilegible e incomprensible a terceros salvaguardando la confidencialidad e integridad de la información. Este cifrado que puede ser simétrico p asimétrico, se hace utilizando una clave que se requiere para el posterior descifrado.

AMENAZA: Es un evento que puede potencialmente ocurrir y producir consecuencias desfavorables para la infraestructura informática, dejándola inutilizable o afectando su integridad. Puede ser de distintas causas tales como naturales, accidentales o provocadas por agentes maliciosos.

BACKUP: Es el respaldo que se hace los datos y aplicaciones almacenadas en un sistema informático, con el propósito de mantener la disponibilidad de estos y de los servicios ofrecidos en caso de daños o ataques.

CIBERATAQUE: Se define como el aprovechamiento de un sistema de información, con base en debilidades de seguridad preexistentes conocidas por el atacante. Normalmente se ejecutan con la ayuda de códigos maliciosos que modifican características propias del sistema ofreciendo la posibilidad al atacante de provocar alteración, daño o robo de activos informáticos.

CLAVE PÚBLICA: Es un concepto extraído de la criptografía asimétrica en la que se usa una combinación de una pareja de llaves llamadas llave pública privada para cifrar los datos en donde no es posible leer la información si hace falta una de ellas. La llave pública puede ser conocida por cualquier persona y será utilizada por el destinatario del mensaje en conjunto con su llave privada para desencriptar los datos.

CLAVE PRIVADA: La llave privada al contrario de la pública en la criptografía asimétrica, debe ser mantenida en secreto puesto que es esencial para el cifrado y descifrado de los datos.

CRIPTOGRAFÍA: Se le denomina así a la técnica consistente en cifrar un mensaje transformándolo en un criptograma que resulta ser ilegible para cualquier persona que desconozca el modo de encriptación y las llaves

necesarias para revertirlo. Existen básicamente dos tipos: simétrica y asimétrica.

DISPONIBIIDAD: Consiste en la condición de accesibilidad que tiene un sistema, servicio o conjunto de datos en cualquier momento en que sean requeridos. Hace parte de los tres ejes de la seguridad de la información compuestos también por la integridad y la confidencialidad. 11

INCIDENTE DE SEGURIDAD: Es todo aquel evento que afecte alguno de las tres dimensiones de la seguridad de la información como son la disponibilidad, integridad y confidencialidad de los datos.

MALWARE: Se trata de un código diseñado con el fin de infiltrarse en un sistema con el fin de dañar, espiar o robar información. Algunos ejemplos de tipos de malware son los troyanos, gusanos, spyware, etc.

PARCHE DE SEGURIDAD: Es una serie de modificaciones que se le hacen a un software con el objeto de añadir características mejoradas de seguridad que reparen anteriores vulnerabilidades de este. Normalmente son desarrollados y distribuidos por el mismo fabricante del sistema.

PLAN DE CONTINGENCIA: Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía.

PUERTA TRASERA: También llamada "backdoor" es una debilidad de un sistema por medio de la cual un atacante puede acceder de forma no autorizada. Estos errores pueden ser producto de fallos o errores de desarrollo del software o insertadas deliberadamente con anterioridad al ataque. En algunas ocasiones se instalan con fines de lícitos.

RANSOMWARE: Es un código malicioso que se vale de tecnologías criptográficas para infectar y secuestrar los datos de un usuario o sistema cifrándolos y dejándolos

RESUMEN

Investigar y analizar el comportamiento del Ransomware (Secuestro de archivos) en las empresas de Bogotá, identificando su entrega, despliegue, Destrucción y Negociación, para obtener los accesos necesarios para encriptar los archivos aprovechando las vulnerabilidades de las compañías, siendo muy rentable en pago con criptomonedas para los ciberdelincuentes y provocando daños graves en las empresas colombianas.

ABSTRACT

Investigate and analyze the behavior of Ransomware (File Hijacking) in companies in Bogotá, identifying its delivery, deployment, Destruction and Negotiation, to obtain the necessary access to encrypt the files taking advantage of the vulnerabilities of the companies, being very profitable in payment with cryptocurrencies for cybercriminals and causing serious damage to Colombian companies.

INTRODUCCIÓN

En el siguiente trabajo se encontrará un estudio dirigido al malware ransomware, que en la actualidad se incrementó en las empresas debido a la pandemia, afectando en gran medida a los sistemas de información, ya que secuestran o encriptan la información, afectando la continuidad de un negocio, generando incertidumbre y que hacer en estos casos debido a la falta de formación en seguridad informática, para mitigar este poderoso malware es necesario comprender la taxonomía y cómo podemos evitarlo, para combatirlo y prevenir este vector de ataque.

En la investigación se analiza los niveles de afectación que produce los diferentes tipos de ransomware a partir de su origen, características y funcionamiento. El comportamiento del ransomware nos ayuda a contrarrestar los ataques cibernéticos, que a través de diferentes organizaciones y proveedores tecnológicos dedicados a resolver la taxonomía de este poderoso Programa maligno que se ha incrementado en la última década y más en la pandemia ya que las empresas han tenido que enviar a sus empleados a trabajo de Home Office y con sus computadoras propias que no tiene muchas seguridades por el desconocimiento del usuario, también se analiza los índices de ataques informáticos tipo ransomware y su nivel de impacto en la infraestructura ti y en los procesos de transformación digital en las MiPymes, obteniendo estadísticas importantes en Latinoamérica.

En los mecanismos de prevención y medidas de seguridad contra ataques de ransomware para las MiPymes colombianas, se tiene diferentes pasos de prevención, backup, mitigación y recuperación si fue víctima del tipo programa maligno ransomware evitando recuperar la información y seguir con la actividad economica de la organización.

En el trabajo de investigación se analiza las vulnerabilidades informáticas que pueden contribuir a un ataque ransomware en las MiPymes, con el objetivo de analizarlos y buscar el endurecimiento de los sistemas informáticos con diferentes herramientas de la seguridad de la informática.

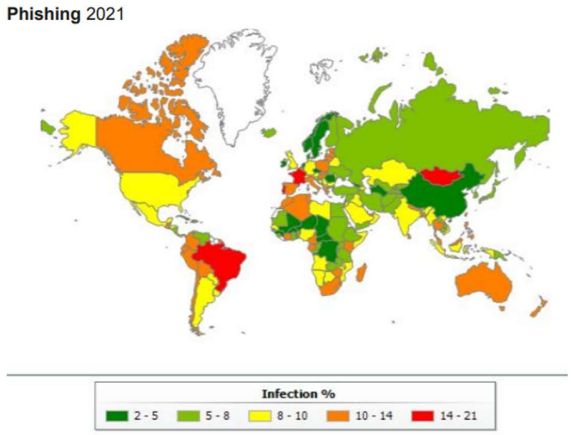
1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Al llegar la pandemia Covid 19, las compañías de Colombia se obligaron a trasladar a sus empleados al trabajo de Home Office, tras el cierre de movilidad y así evitar el contagio, en ese momento los ciberdelincuentes encontraron varias vulnerabilidades en sus sistemas, como los equipos de cómputo que la mayoría son personales y no tienen protección como antivirus, ingresos al dominio, y otras medidas de protección, al tener estas vulnerabilidades el peligroso Ransomware empezó a entregar correos maliciosos, archivos con malware y otras técnicas de Ingeniería social , que algún usuario ejecuto y el malware empieza su despliegue silenciosamente mapeando las redes internas, servidores , NAS, Backup , puerto abiertos, preparando para su destrucción o encriptación y llegando a su fase final que es pedir un rescate de sus archivos secuestrados a través de Bitcoin o cualquier otra criptomoneda.

Según la empresa de Kaspersky "El ransomware dirigido a empresas aumenta más de un 200% en Latinoamérica"[1].

Figura 1 Estadística de Phishing 2021



Fuente:" Ciberataques América Latina. [Sitio web] [Consultado 14 de abril de 2022] Disponible en: https://latam.kaspersky.com/blog/ciberataques-

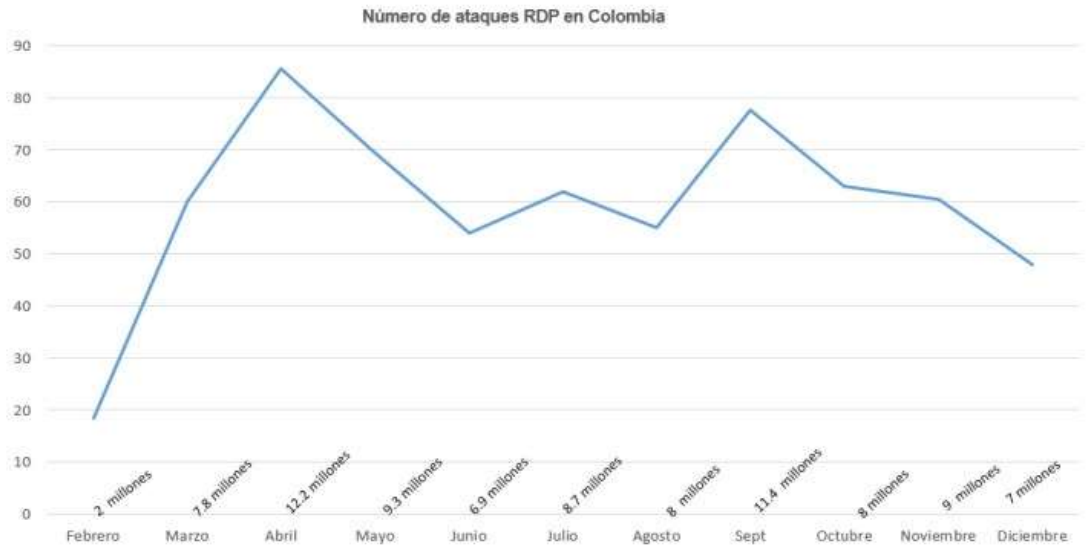
[1] RANSOMWARE [Sitio Web] [Consultado 14 de abril de 2022] Disponible en: https://latam.kaspersky.com/blog/el-ransomware-dirigido-a-empresas-aumenta-mas-de-un-200-en-latinoamerica/23784/#:~:text=Sin%20embargo%2C%20al%20comparar%20los,sanitaria%20%E2%80%93%20con%20una%20actividad%20m%C3%A1s

en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/"

Colombia sufre más de 91 millones de ataques de acceso remoto en 2021

En febrero de 2020, Colombia registró 2 millones ataques, los cuales ascendieron a 7.8 millones en marzo del mismo año, representando un crecimiento de 290% entre el "antes de la pandemia» y el «durante la pandemia». Este aumento fue mayor que el crecimiento global registrado de 197% (de 93 millones a 277 millones de febrero a marzo de 2020)[2].

Figura 2 Ataques RDP en Colombia



Fuente: "ATAQUES DE ACCESO REMOTO RDP. [Sitio Web] [Consultado el 14 de abril de 2022] Disponible en: https://prensariotila.com/32980-colombia-sufre-mas-de-91-millones-de-ataques-de-acceso-remoto-en-2020/"

[2] ATAQUES DE ACCESO REMOTO RDP. [Sitio Web] [Consultado el 14 de abril de 2022] Disponible en: https://prensariotila.com/32980-colombia-sufre-mas-de-91-millones-de-ataques-de-acceso-remoto-en-2020/

La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad

Tasa anual de correos electrónicos maliciosos por tamaño de organización

Tabla 1 Estadística de correos maliciosos

Tamaño de la organización	Tasa de correo malicioso (1 en)
1-250	323
251-500	356
501-1 000	391
1 001-1 500	823
1 501-2 500	440
2 501+	556

Fuente: "Symantec (2019), ISTR - Internet Security Threat Report, Volume 24, Mountain View, USA, February [en línea] https:// docs.broadcom.com/doc/istr-24-2019-en."

Tabla 2 Cantidad de correos electrónicos maliciosos por tamaño de organización

Tamaño de la organización	Usuarios afectados (1 cada)
1-250	323
251-500	356
501-1 000	391
1 001-1 500	823
1 501-2 500	440
2 501+	556

Fuente: "Symantec (2019), ISTR - Internet Security Threat Report, Volume 24, Mountain View, USA, February [en línea] https:// docs.broadcom.com/doc/istr-24-2019-en."

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué mecanismos de seguridad se pueden implementar en las infraestructuras TI y en los procesos de transformación digital en las Mipymes para evitar que sean víctimas de un ataque tipo Ransomware?

2 JUSTIFICACIÓN

Dar a conocer a las empresas colombianas la importancia de proteger el activo más importante que es la información dando a conocer la taxonomía del peligroso ransomware, definiendo mecanismos de protección y ayudar a mitigar el impacto que puede tener una empresa. Al conocer cómo funciona puede actuar preventivamente protegiendo los servidores, Backup, Bases de Datos, Archivos de producción, ERP y demás sistemas con una debida revisión de sus políticas de seguridad, realizando pentesting para reducir vulnerabilidades y vectores de ataques.

En la llegada de la pandemia que inicio el marzo del año 2020, en Colombia se decretó el aislamiento o emergencia sanitaria del Covid 19. Entre las medidas de prevención que el gobierno colombiano decreto fue realizar una cuarentena y aislar a las personas y dejo trabajar a ciertos sectores productivos con permisos especiales, en la mayoría de los empleados junto con las organizaciones tomaron varias medidas para que su personal siguiera trabajando entre ellas Home Office, sin tener en cuenta el riesgo tecnológico que eso implicaba, y que aprovecharon los ciberdelincuente, por la poca capacitación en seguridad informática y la debilidad de infraestructura tecnológica, ya que no se contaba con los recursos económicos, llevando a las empresas a realizar una transformación tecnológica para salvaguardar la información e implementar la seguridad de la información en cada una de las organizaciones.

En consecuencia de las emergencia sanitaria y con los diferentes vectores de ataque como el tipo de malware ransomware, las organizaciones analizaron la importancia de analizar su infraestructura tecnológica interna como las seguridad de sus empleados en su labor desde casa, para ello se analizó el tipo de ataque desde sus inicios a la actualiza y poder realizar las medidas de aseguramiento con su transformación tecnológica, capacitación y controles de seguridad, para fortalecer la seguridad informática y de la información en las Mipymes.

Esta investigación de este trabajo aborda los niveles de afectación, índices de ataques, mecanismos de prevención y las diferentes vulnerabilidades para el conocimiento de las Mipymes y que puedan realizar una transformación digital en cada organización y no ser afectados por tipo de malware ransomware.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

- Analizar los ataques tipo Ransomware realizados durante el Covid 19 a las MiPymes Colombianas a causa de vulnerabilidades presentes en las infraestructuras TI y en el proceso de transformación digital para la generación de mecanismos de seguridad que salvaguarden la información de las organizaciones.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer los niveles de afectación que produce los diferentes tipos de ransomware a partir de su origen, características y funcionamiento.

- Contrastar con base a las fuentes documentales los índices de ataques informáticos tipo Ransomware y su nivel de impacto en la infraestructura TI y en los procesos de transformación digital en las MiPymes.

- Proponer mecanismos de prevención y medidas de seguridad contra ataques de ransomware para las MiPymes colombianas.

- Identificar las vulnerabilidades informáticas que pueden contribuir a un ataque ransomware en las MiPymes.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La presente investigación se centrará en el análisis del virus ransomware y sus consecuencias en la perdida de información en las empresas colombianas. El ransomware por lo tanto es un programa malicioso que infecta a los archivos, principalmente a los documentos de procesadores de texto u hojas de cálculo.

Las compañías colombianas y su evolución la información ya se guarda en forma digital en servidores de datos y sus Backus los guardan en una NAS, discos o repositorios documentales compartiéndolos por la red con los permisos que otorga el servidor a sus usuarios finales, para asegurar esta información se necesita personal calificado y recursos tecnológicos. El autor Fabián Martínez Portantier, un experto en seguridad informática nos dice "no es tan importante la cantidad de recursos que invertimos, sino que debemos considerar la inteligencia con la cual implementamos dichas medidas"[3].

Las compañías deben tener claro las capacitaciones en seguridad informática, al abrir un correo con un archivo ejecutable puede infectar más de 400.000 archivos. A pesar llegan correos a las bandejas de entrada de los usuarios con información falsa de empresas reconocidas, dejando que el usuario descargue el ejecutable, infectando a la mayor parte de la empresa.

Entonces, para que las empresas no estén vulnerables y que puedan protegerse, una de las primeras medidas es la capacitación del personal para que informen al área de sistemas para su revisión, pero existe una estrategia de enfoque por partes, en primer lugar, es la capacitación del personal, la segunda medida son políticas de seguridad de la información y procedimientos de seguridad, la tercera es la seguridad física en el caso que pase el ataque se debe utilizar el ultimo recursos que son los backups internos y externos.

[3] Seguridad Informática: virus ransomware, el Secuestro virtual de datos. PosibleMedina Carranza, Facundo Martin. [Consultado 31 de marzo 2022]. [online]. Disponible en: https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/13925/MEDINA%20CARRANZA%20FACUNDO%20MARTIN.pdf?sequence=1&isAllowed=y

En el caso que no se tengan esos Backups, las empresas empiezan a perder tiempos en la recuperación de sus procesos, ya que pierden información importante generando una crisis interna de incertidumbre, por eso el negocio para los hackers es tan lucrativo, aunque muchas otras no tienen el dinero para pagar el rescate.

En el estado colombiano no es fácil encontrar a estos delincuentes digitales ya que no es una tarea fácil, ya que el rescate ahora es en bitcoin, que es una moneda que operan con diversas herramientas como el mezclador de direcciones que, como explican en Bitcoin.org, cuando se envían los bitcoins anónimamente a un destinatario utilizando como navegador TOR, una red que permite no revelar la identidad de los usuarios que hace mucho más complicado el rastreo de los atacantes.

Las empresas que no toman medidas de este poderoso Malware pueden tener consecuencias económicas, teniendo consecuencias con sus colaboradores, proveedores y temas legales, afectando a varias familias colombianas y el desprestigio de la compañía.

Las organizaciones también deben realizar una transformación digital que nace a partir de varios efectos en las Mipymes que generan nuevos actores, estructuras, practicas tecnológicas, valores y creencias que reemplazan o complementan las reglas existentes dentro de las organizaciones, en su taxonomía de la transformación digital se encuentran 4 categorías; Razones que pueden ser internas o externas, objetos, procesos y resultados[4].

Por lo transformación digital ha sido relevante en la última década y más en la pandemia, ya que acelero esta transformación digital en la forma como trabajamos desde casa y su interacción con las Mipymes y dar llegar a una productividad eficiente y verificando la seguridad digital a través de controles e infraestructura para salvaguardar el activo más importante que es la información.

Con lo anterior expuesto esta investigación está orientada al manejo de estrategias que deben tomar las compañías para no tener perdidas considerables.

[4] Delgado Fernández, T. (2021). Taxonomía de Transformación Digital. Revista Cubana De Transformación Digital, 1(1), 4–23. Recuperado a partir de https://rctd.uic.cu/rctd/article/view/62 (Original work published 21 de abril de 2020)

4.2 MARCO CONCEPTUAL

RANSOMWARE

El Ransomware es un tipo de malware peligroso que, al infectar nuestros sistemas de información, para que el ciber delincuente encuentre las vulnerabilidades del sistema y con los privilegios pueda encriptar la información dejando a las empresas colombianas en estado de alerta por no seguir con su operación con normalidad, el atacante deja información para que pueda ser rescatada la información con un pago con criptomonedas.

El Malware, en todas sus formas y variantes es una amenaza preocupante para las empresas como para los usuarios. Se debe estar alerta y verificar los mecanismos para la protección de activo más importante la información. La educación de seguridad informática juega un papel importante en la prevención de este.

CRIPTOVIROLOGÍA

Es la disciplina informática que se encarga de estudiar el uso de criptografía como ciencia para la construcción de softwares maliciosos. Técnicas y mecanismos para enmascarar y no dejarla visible a terceros, se puede utilizar para realizar el bien o para no utilizarlo de forma adecuadas.

CRIPTOGRAFÍA

Es un término proveniente del griego y que traduce "escritura oculta", y está definida en función de la criptología como las técnicas de codificación que buscan alterar la representación lingüística de la información de tal forma que sea ininteligible a sistemas o personas no autorizadas. Actualmente se ha ampliado su campo de acción al diseño de sistemas, algoritmos y protocolos para dotar de seguridad a los datos, las comunicaciones y a las entidades que gestionan la información[5].

[5] Pastor Franco, José, Sarasa López, Miguel Ángel, Salazar Riaño, José Luis, "Criptografía digital: fundamentos y aplicaciones", Ed. Prensas Universitarias de Zaragoza, 1998.

A través de la historia se puede observar que constantemente se usan métodos distintos para acceder a la información digital de diversas maneras; uno de los más frecuentados es a través del Ransomware, un malware que desde el 2009 ha ido creciendo rápidamente[6] y se ha expandido por todo el globo terráqueo. La distribución de este malware lo hace un delincuente cibernético con fines delictivos. Actualmente se pueden encontrar en el mundo diferentes tipos de Ransomware que se enfocan en el secuestro de información, entre ellos uno muy conocido a nivel mundial es el "Fake police Ransomware". Este Ransomware se enfoca principalmente en el defacing de un portal de la policía o FBI, para recaudar dinero a cambio de la información "legalmente" confiscada. Además de las posibles variaciones de este malware, desarrollo un método de propagación vía spam por email, el cual valida en un servidor el idioma y región de la víctima para traducir el mensaje por completo.

[6]Ataques de ransomware durante 2019. [Sitio Web] [Consultado 20 de Julio 2022] Disponible en: https://unaaldia.hispasec.com/2020/01/ataques-de-ransomware-durante-2019.html

4.3 MARCO HISTÓRICO

Las formas de los ataques de un ransomware como se muestra en la siguiente figura:

Figura 3 Cómo las empresas y las personas reciben ataques de ransomware

Fuente: "Elaboración propia"

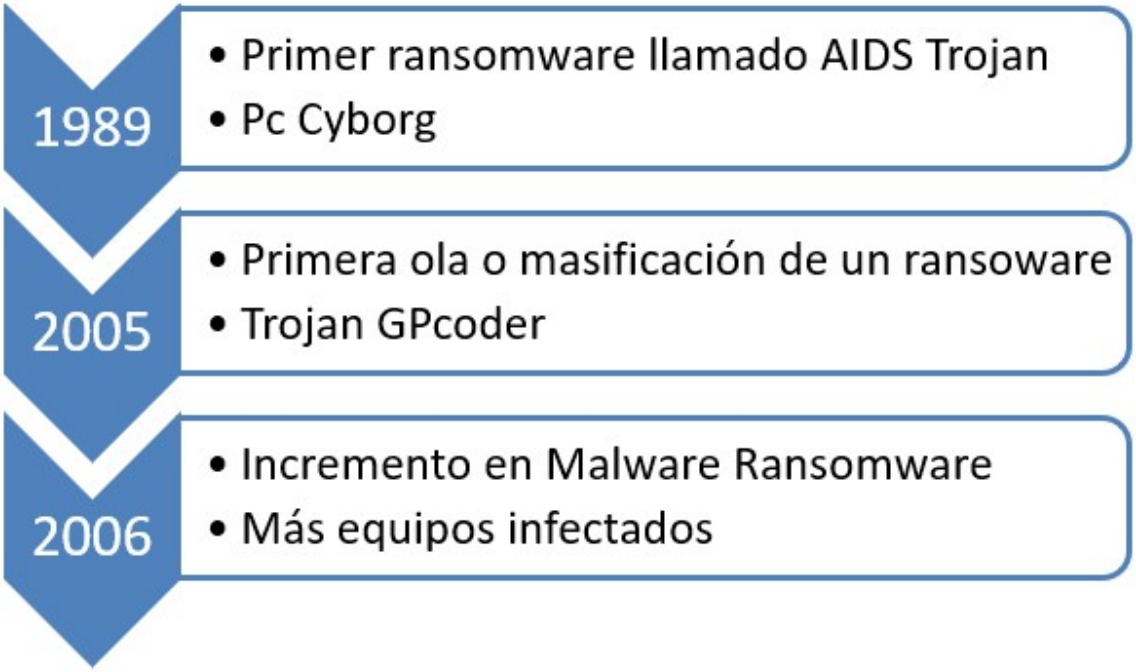
4.3.1 HISTORIA

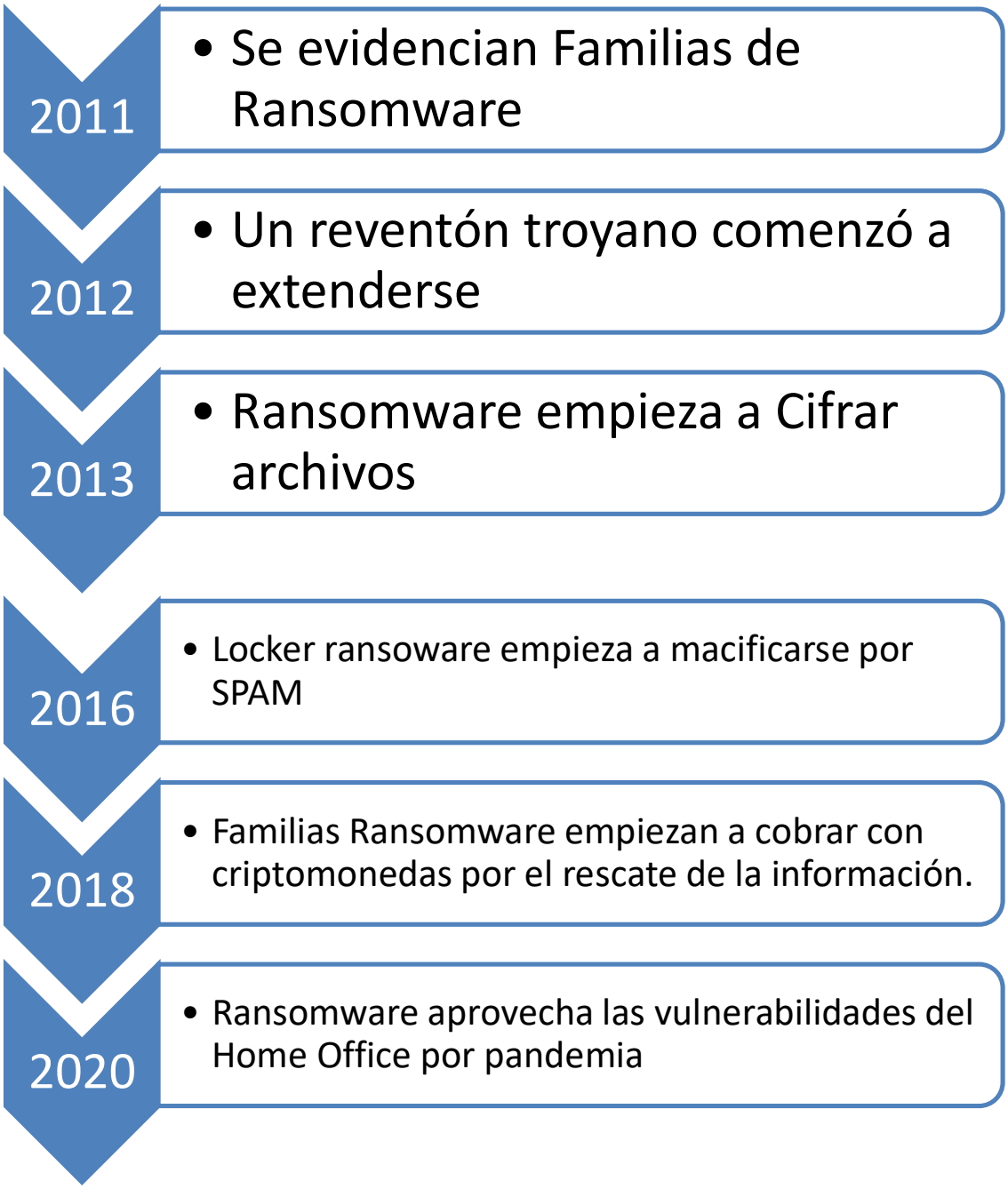
Los ataques de ransomware ocurren con mucha frecuencia en el espacio de Internet. Este tipo de ciberdelito se ha detectado en más de 150 países hasta la fecha. Las organizaciones se enfrentan a nuevos tipos de ataques de ransomware y cada vez es más difícil para los profesionales de TI recopilar las claves para desbloquear los sistemas informáticos, ya que sin ellos es imposible volver al uso normal. Palmer D. señaló que "el ransomware es una forma de malware, malware que cifra archivos y documentos en cualquier cosa, desde una sola PC hasta una red completa, incluidos los servidores. Las víctimas a menudo no tienen muchas opciones; pueden recuperar el acceso a su red cifrada pagando un rescate a los delincuentes detrás del ransomware, o restaurando desde copias de

seguridad, o esperando que la clave de descifrado esté disponible de forma gratuita.

En la siguiente figura muestra la línea de tiempo del malware ransomware.

Figura 4 Timeline de la historia del ransomware





Fuente: Ataques de ransomware: riesgos, medidas de protección y prevención. [ONLINE]. 2021.[14 noviembre 2021]. Disponible en: Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/9548507

El primer ransomware se creó en 1989 y se llamó "AIDC Trojan" o "PC Cyborg". Hasta 2005 aparecieron varios gusanos ransomware. Más tarde, algunos gusanos ransomware incluso imitaron los productos de Windows. Hay dos tipos de estos ciberdelincuentes. El primero es el cripto-ransomware: cifra archivos y datos; mientras que este último está diseñado para bloquear computadoras y se llama acertadamente "casillero de ransomware"[7].

Algunos de los ataques más preocupantes tienen como objetivo la infraestructura nacional. Durante el ataque de WannaCry, por ejemplo, el NHS se vio gravemente afectado y se enfrentó a demandas de pagos de $ 300 o $ 600 por computadora para restaurar el acceso. El apagón provocó importantes retrasos en hospitales y cirugías en todo el país.

El ransomware puede ser una de las formas más comunes de malware en la actualidad, pero no siempre es así. El malware, como cualquier virus, promueve amenazas que pueden adaptarse y evolucionar con su entorno. A medida que nos volvemos más conectados y nuestras economías se vuelven más digitales, nos enfrentamos a una creciente amenaza de ciberataques, con ransomware en el corazón de nuestro arsenal de ciberdelincuentes modernos.

4.3.2 CIBERVÁNDALOS A CIBERDELINCUENTES

Los orígenes del ransomware se remontan a 1989, cuando las víctimas desprevenidas se infectaron con el "troyano del SIDA". Este se distribuyó a través de disquetes que se enviaron a las víctimas a través del servicio postal normal. Aunque el mundo no estaba preparado para un ataque de este tipo, el virus luchó por propagarse en ese momento porque pocas personas usaban computadoras personales e Internet aún se encontraba en sus primeras etapas. Además de esto, la tecnología de cifrado todavía era limitada en ese entonces.

A pesar de sus inicios, el ransomware no era una forma popular de malware en la década de 1990 y principios de la de 2000, ya que el objetivo principal era ganar notoriedad a través de bromas cibernéticas y vandalismo, y los piratas informáticos usaban gráficos para comunicar el ataque al usuario. Estos gráficos eran a veces divertidos y creativos, tanto

[7] Ataques de ransomware: riesgos, medidas de protección y prevención. [ONLINE]. 2021.[14 noviembre 2021]. Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/9548507

que algunos de ellos han sido inmortalizados en un Museo de Malware en línea donde se puede interactuar con virus de antaño, sin sus elementos maliciosos.

Un ejemplo infame de este período es el virus MS Blaster, también conocido coloquialmente como el virus 'LoveSan'. El virus obligó al sistema a reiniciarse después de 60 segundos e incluyó dos mensajes ocultos en el código: '¡¡Solo quiero decir LOVE YOU SAN !!' y 'Billy Gates, ¿por qué haces esto posible? ¡¡Deje de ganar dinero y arregle su software!! '.

La diferencia entre los primeros desarrolladores de ransomware y los de hoy es que los atacantes en ese entonces solían escribir su propio código de cifrado, lo que a veces conducía a una mala ejecución del ataque. Los delincuentes de hoy confían en métodos de piratería más sofisticados, como bibliotecas estándar que resultan mucho más difíciles de descifrar. Otro método que los piratas informáticos han desarrollado con el tiempo, que ayudó a que el ransomware se expandiera y se convirtiera en una forma más frecuente de ciberataque, son los juegos de herramientas descargables un poco menos sofisticados, pero igualmente dañinos. Estos permiten a los atacantes con menos habilidades técnicas realizar ataques con éxito. El mercado de ransomware se ha expandido hasta el punto de que los ciberdelincuentes avanzados monetizan el ransomware ofreciendo programas de ransomware como servicio.

4.3.3 NEGOCIO PRÓSPERO

El ransomware ha prosperado en la economía digital actual gracias a la aparición de criptomonedas casi imposibles de rastrear. Entonces, ahora, en lugar de recibir una actualización descarada para hacerle saber que ha sido pirateado, lo primero que la mayoría de las personas y organizaciones escuchan de un ataque exitoso es cuando el orquestador comienza a pedir bitcoins.

Los primeros ejemplos de ransomware en su forma moderna se vieron en la forma de Cryzip en 2006. Aunque Cryzip fue un ataque a pequeña escala, abrió con éxito el camino para variaciones de ransomware más dañinas como CryptoLocker y CryptoWall. No fue hasta 2013 que vimos la madurez completa de estas variaciones modernas de ransomware en la forma que conocemos ahora, lanzada cuatro años después de que Bitcoin fuera lanzado como software de código abierto. Estos virus se distribuyeron a través de un simple archivo adjunto y, evadiendo las

técnicas de prevención habituales, procedieron a encontrar y cifrar rápidamente los datos de sus víctimas. La siguiente parte fue simple: pague o pierda sus datos.

La variante de ransomware CryptoLocker infectó más de 250.000 sistemas entre septiembre y diciembre de 2013 y sus ingresos alcanzaron más de $ 3 millones antes de que se desconectara en 2014. Se desarrolló una herramienta en línea para recuperar archivos cifrados comprometidos por CryptoLocker mediante el análisis de su modelo de cifrado. Desafortunadamente, esta no fue una forma de detenerlo, ya que los ciberdelincuentes lograron desarrollar diferentes variaciones de este virus conocido como CryptoWall y TorrentLocker. De hecho, desde principios de 2014 hasta principios de 2016 pasarán a la historia del ransomware como una era de CryptoWall, que era el ransomware más utilizado, dirigido a cientos de miles de personas y empresas. El valor de los delitos de CryptoWall superó los 18 millones de dólares a mediados de 2015. Se estima que para 2019, el ciberdelitolos costos alcanzarán los $ 2 billones, según lo informado por Forbes, mientras que se estima que el ciberdelito le costará a la economía global $ 445 mil millones (£ 401 mil millones) cada año. 2

4.3.4 INDUSTRIA MULTIMILLONARIA

La monetización es el elemento clave que ha diferenciado al ransomware de los modelos de virus tradicionales. CryptoLocker y CryptoWall inspiraron a toda una nueva generación de ciberdelincuentes imitadores. Solo necesita mirar las cifras para descubrir por qué los ataques de ransomware se han acelerado rápidamente. Los expertos en seguridad han estimado que se depositaron mil millones de dólares en Bitcoincarteras asociadas con ransomware ciberdelincuentes solo en 2016. Esto lo convierte en un negocio increíblemente lucrativo y es la razón por la que los delincuentes ahora miran más allá de la humilde computadora personal hacia objetivos más valiosos como los gobiernos, la industria de servicios públicos y empresas más grandes. Este fue el objetivo de los recientes ataques globales de WannaCry y NotPetya, que infectaron a las principales empresas y la infraestructura nacional en busca de mayores presupuestos capaces de pagar mayores cantidades de rescate.

A principios de este año, NotPetya ransomware atacó a empresas en Europa, Oriente Medio y Estados Unidos. Con un precio de 300 dólares en bitcoins por computadora, el ataque comenzó en Ucrania, donde entre los

afectados se encontraban organizaciones gubernamentales, el Banco Nacional de Ucrania y la planta de energía nuclear de Chernobyl. Se extendió a otras organizaciones en diferentes países, entre ellos la empresa de logística Maersk, la empresa de alimentos Mondelez y el despacho de abogados DLA Piper. La policía cibernética de Ucrania informó que el ataque parece haber sido sembrado a través de un mecanismo de actualización de software que estaba conectado al programa de contabilidad que las empresas que trabajaban con el Gobierno de Ucrania necesitaban utilizar y que afectó a más de 2.000 computadoras.

La tendencia más reciente entre los ciberdelincuentes, como se ha visto en los últimos meses, han sido los ataques a redes de televisión como HBO. En este caso, se revelaron datos personales del elenco de 'Game of Thrones', incluidos correos electrónicos, números de teléfono y guiones. Los piratas informáticos afirmaron haber robado 1,5 TB de datos y pidieron un rescate de varios millones de dólares, amenazando con lanzar la última temporada del programa de televisión masivamente popular. Según los piratas informáticos que llevaron a cabo el ataque, una intrusión exitosa en la red de HBO tomó seis meses y $ 500,000 en exploits de día cero que les permitieron identificar los agujeros en los sistemas de software.

4.3.5 RESQUICIO DE ESPERANZA

Todos estos ejemplos parecen pintar un panorama sombrío, pero hay un lado positivo. A medida que evolucionan los ataques, también lo hacen los esfuerzos de ciberseguridad para abordar el desafío. Por ejemplo, WannaCry fue interceptado por un experto en seguridad que activó un dominio de "autodestrucción". Una mayor conciencia de los ataques cibernéticos conduce a un mayor enfoque e inversión en tecnologías de prevención. Sin embargo, el ransomware y otros virus seguirán evolucionando a la par.

Como respuesta a un número creciente de ataques de ransomware, se ha formado una comunidad de sombreros blancos: piratas informáticos o expertos en seguridad que se especializan en pruebas de penetración y desarrollan diversas metodologías de prueba para desafiar la seguridad existente del sistema de información de una organización. Los sombreros blancos pueden usar muchos métodos diferentes al probar la seguridad:

por ejemplo, un grupo de piratas informáticos de seguridad llamado OurMind pirateó las cuentas de Twitter de Marvel para promocionar sus servicios al tuitear a más de cuatro millones de seguidores de Marvel. El tweet decía que el truco había sido con fines de prueba de seguridad y sugería que las personas podrían ponerse en contacto con OurMind para obtener ayuda.

No es una sorpresa que la necesidad de los sombreros blancos y la piratería ética haya aumentado a medida que más y más organizaciones se dan cuenta de la necesidad de adoptar un enfoque proactivo y preventivo para proteger sus sistemas antes de que ocurra un ataque. Fomentar la piratería ética es una forma de evitar el daño potencial de futuros ciberataques y descubrir vulnerabilidades en redes, productos y software. De esa manera, las organizaciones pueden abordar los problemas y solucionarlos antes de que los ciberdelincuentes los descubran.

Las organizaciones que desean protegerse de una amenaza creciente para sus sistemas y su reputación no deben esperar a que un ataque tenga éxito antes de invertir en sus sistemas de seguridad. La protección contra la amenaza del ransomware significa actuar ahora y armarse con armas igualmente escalables y avanzadas para combatir una amenaza compleja y en evolución que no muestra signos de desaceleración.

4.4 MARCO LEGAL

4.4.1 LEY 1273 DE 2009

"Por medio de la cual se crea un nuevo bien jurídico tutelado denominado 'de la protección de la información y de los datos' y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."[8]

CAPITULO I (Atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos que tiene los siguientes artículos**)**

- Artículo 269A: Acceso abusivo a un sistema informático[9].
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.
- Artículo 269H: Circunstancias de agravación punitiva

CAPITULO II (De los atentados informáticos y otras infracciones**)**

Artículo 269I: Hurto por medios informáticos y semejantes.
Artículo 269J: Transferencia no consentida de activos

4.4.2 LEY 599 DE 2000

Por la cual se expide el código penal colombiano. "En su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad

[8] ÁLVARO URIBE VÉLEZ. Fabio Valencia Cossio. LEY 1273 DE 2009. [ON LINE]. 2009.[14 DE noviembre del 2021] Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf
[9] Ibidem

individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:
Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles."[10]

[10] OJEDA, J. E., RINCÓN, F., ARIAS, M. E., DAZA, L.A. "Delitos informáticos y entorno jurídico vigente en Colombia." [En línea]. 2010. [14 de noviembre de 2021} disponible en: (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003).

5 NIVELES DE AFECTACIÓN QUE PRODUCE LOS DIFERENTES TIPOS DE RANSOMWARE A PARTIR DE SU ORIGEN, CARACTERÍSTICAS Y FUNCIONAMIENTO.

El comportamiento del ransomware nos ayuda a contrarrestar los ataques cibernéticos, que a través de diferentes organizaciones y proveedores tecnológicos dedicados a resolver la taxonomía de este poderoso Malware que se ha incrementado en la última década y más en la pandemia ya que las empresas han tenido que enviar a sus empleados a trabajo de Home Office y con sus computadoras propias que no tiene muchas seguridades por el desconocimiento del usuario.

El ransomware viene desarrollado para diferentes sistemas operativos con la intención de bloquear información, robo, secuestro de información que pide un rescate a través de las criptomonedas así se han invisibles y que nos puedan ser rastreados por los entes de control.

Uno de los ransomware que más se ha escuchado y que causo un daño grande es WannaCry, a partir del 2017 afecto muchas empresas en Europa y también en Rusia con ataques exponenciales hasta la fecha.

Las organizaciones han realizado diferentes estrategias de contención para frenar la amenaza de ransomware, estableciendo procesos y procedimientos para identificar, reducir y erradicar el malware, para dar solución inmediata.

El éxito de ransomware en sus ataques, que se realizan mutaciones creando nuevos y más poderosos, que dificultan la contención dando la creación de Familias de este malware, Para en el caso de WannaCry, se ha estimado que las diferentes variantes de ransomware han generado pérdidas de alrededor de los 300 millones de euros.

5.1.1 COMPORTAMIENTO DE UN RANSOMWARE

En la revisión de este Malware tiene diferentes etapas que son: el análisis dinámico, análisis estático, análisis en su comportamiento o ejecución e ingeniería inversa.

Análisis dinámico: Permite conocer de forma rápida y efectiva que acciones realiza en un sistema.

Análisis estático: se analiza el código fuente del ensamblador no ejecutando el software malicioso.

Análisis en su comportamiento: se analiza como interactúa con los demás componentes informáticos, redes, consolas, puertos, sistemas operativos, etc.., para ejecutar su software malicioso.

Ingeniería inversa: estudio del código malicioso para estudiar el comportamiento de las vulnerabilidades que explota este software malicioso.

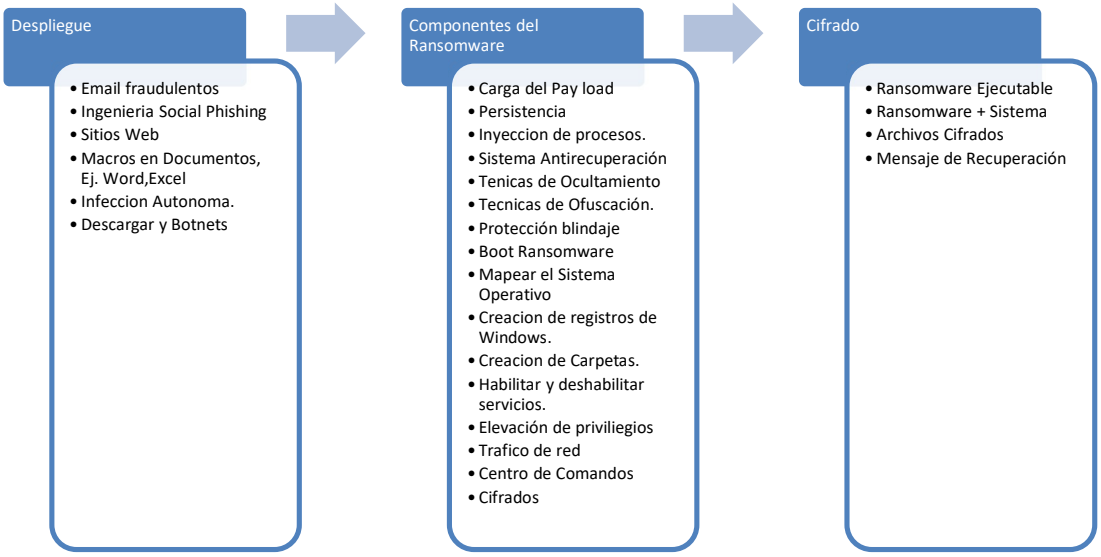
Durante su análisis en su comportamiento que su estructura y comportamiento son similares a diferentes tipos de malware como gusanos o troyanos que tiene técnicas de ofuscación e igualdad en sus payload y su facilidad de replicación, todos los malware necesitan un payload que es el componente principal que a su vez lo ocultan para que no sea detectado por los antivirus

Algunos ransomware elimina las copias de Windows, para que nos facilite la recuperación de la información, al no recuperarla le indican a la víctima la forma del rescate de la información.

En las fases del ransomware siguen un orden que son:

- Despliegue por diferentes canales de comunicación.
- Verificación del sistema Operativo.
- Inicio de la infección.
- Encriptación de la información o cifrado.
- Generar llaves que las envían a Centro de comando y Control (C&C)

Figura 5 Fases de infección de un malware.



Fuente: "Elaboración propia"

5.1.2 FORMAS DE DISTRIBUCION

El malware del ransomware aprovecha las ventajas que tiene la ingeniería social, para enviar vectores de Ataque que un usuario por su desconocimiento por lo general lo realizan por correo electrónico por la importancia que tiene en las compañías, oras formas es por la utilización de memorias USB que regalan en las calles o que se encuentras y por la curiosa ejecutan un autorun.

El protocolo RDP. Los cibercriminales atacan estos equipos explotando vulnerabilidades del protocolo y rompiendo credenciales débiles utilizando fuerza bruta o contraseñas filtradas. Los equipos con RDP no deberían ser accesibles desde Internet en absoluto.

Correos phishing. Un ataque de phishing por correo electrónico busca engañar a los usuarios para robarles sus credenciales, luego, esas credenciales se utilizan para acceder a sistemas clave en los que se instala el Ransomware. También, los correos pueden incluir adjuntos con código malicioso, que una vez abierto por el usuario infecta su equipo automáticamente. Los empleados son la primera línea de defensa contra

este ataque, hay que entrenarlos acerca de los peligros del phishing para que sepan cómo actuar ante estos ataques[11].

Vulnerabilidades del SW. Una vez adentro, pueden robar información sensible y desplegar el Ransomware por toda la red de la empresa. Necesitas identificar y eliminar las vulnerabilidades con un programa de Vulnerability Management para mantener un registro actualizado de tus sistemas y su seguridad.

5.1.3 CICLO DE VIDA

El ciclo de vida un ransomware se compone de 6 etapas:

Distribución: La forma más común de diseminación de malwares es a través del phishing. No sólo sucede por correo electrónico, hay muchos anuncios en sitios web, aplicaciones y software para descargar y, en casos extremos, pen drives que los delincuentes dejan en lugares estratégicos o los llevan a las empresas con alguna excusa para que alguien los abra.

Infección: A partir de ese momento, cuando se accede a un archivo o enlace infectado, se inserta en el equipo el código portado por el malware, iniciando los procesos necesarios para llevar a cabo las actividades maliciosas. Este paso varía según el malware que se esté ejecutando, lo que puede suceder durante una actualización o apagado, al abrir un programa en particular en la computadora o en cualquier otro caso.

Es a partir de esta acción que el código se activa, deshabilitando duplicados y sistemas de reparación y recuperación de errores, programas defensivos y similares.

Comunicación: Una vez activo, el malware comienza a comunicarse con los servidores de claves de cifrado, obteniendo una clave pública que permite cifrar los datos de la víctima. En estos servidores, donde se almacenan los códigos de modificación de los archivos. Empiezan a funcionar desde el momento en que se conecta el malware.

Búsqueda de archivos: El ransomware realiza un escaneo sistemático en la computadora de la víctima en busca de archivos específicos del

[11] Ransomware – Top 3 Vectores de Ataque 2021, [ONLINE]. 2021. Disponible en: https://m3security.mx/ransomware-top-3-vectores-de-ataque-2021/

sistema que son importantes para el usuario y que no se pueden copiar fácilmente, como archivos con extensión .jpg, .docx, .xlsx, .pptx y .pdf.

Cifrado: En este punto se lleva a cabo el proceso de mover y renombrar los archivos definidos en el paso anterior, mezclando la información para que el sistema informático del usuario ya no pueda dar acceso al usuario, ahora es necesario descifrarlos para recuperarlos.

Pedido de rescate: Por lo general, primero aparecerá un mensaje en la pantalla de la computadora infectada. Esto significa que el hacker advierte que ha secuestrado los datos y solo los devolverá si el usuario realiza un pago de rescate. Una vez realizado el pago, el ciberdelincuente envía a la víctima una clave de cifrado para desbloquear la computadora**.**

5.1.4 TIPOS DE RAMSONWARE

Se lista los diferentes tipos de ransomware que se a utilizado en secuestrar la información de las organizaciones.

REVETON: Se declara una autoridad legal y legítima.

CRYPTOLOCKER: es un ransomware de cifrado de archivos que cifra los registros privados.

CRYPTOLOCKER.F Y TORRENTLOCKER: es un virus troyano.

CRYPTOWALL: Lo aplica como un código Java Script como parte de un archivo adjunto de correo electrónico.

FUSOB: Es un tipo de malware que afectará a los teléfonos móviles.

WANNACRY: es el último ransomware ejecutado en mayo de 2017 y se dirige principalmente a MS-Windows.

En la figura 5 muestra un mensaje cuando fue atacado por un malware de tipo ransomware, se observa e indica que debe hacer para rescatar la información.

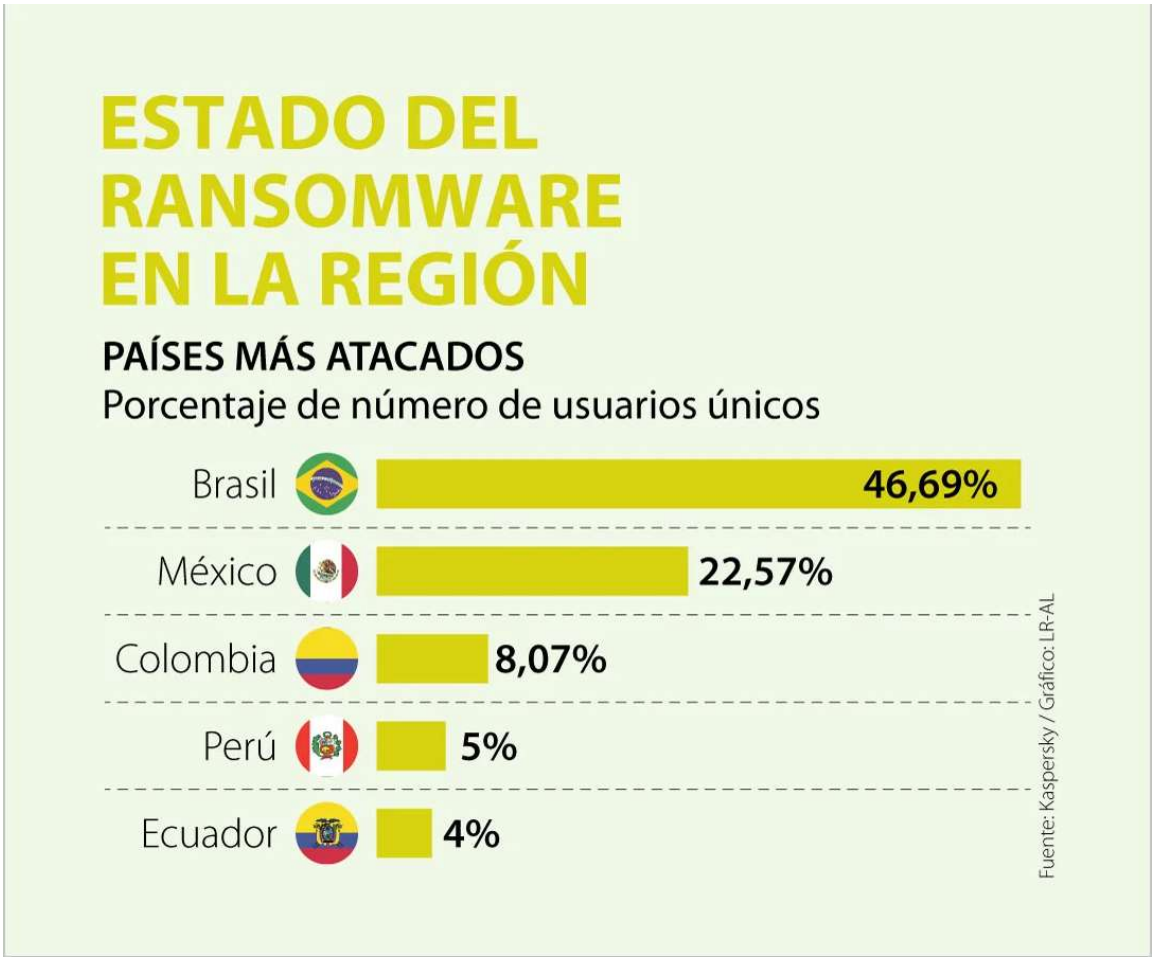
Figura 6 Ransomware

Fuente: "Ransomware. [Sitio Web] [Consultado el 20 de mayo 2022] Disponible en: **https://www.nomoreransom.org/en/ransomware-qa.html"**

5.1.5 ANALISIS DE NIVELES DE AFECTACIÓN DEL RANSOMWARE

En la revisión estadística de los países de Latinoamérica, se evidencia en la figura 6, el comportamiento del ransomware y como primer país afectado es Brasil con un 46%[12].

Figura 7 Ransomware en Latinoamérica



Fuente:" Ransomware Latinoamérica [Sitio Web] [Consultado el 14 de abr. de 22] Disponible en: https://www.larepublica.co/internet-economy/este-ano-se-han-hecho-5000-ciberataques-por-dia-de-ransomware-en-latinoamerica-3075409"

[12] DIAZ RHENALS, Karina. Análisis de fenómenos ransomware, su afectación en la ciberseguridad y herramientas de contraataque en MiPymes. [en lí-nea] Montevideo: Facultad de Ingeniería, 2022-02-16. [Fecha consulta: 14 de abril 2022].

En el caso que se haya materializado un ataque del tipo ransomware, realmente la gravedad de las consecuencias depende de la recuperación de la información, es decir el tiempo que dura en recuperar su actividad economica en una Mipymes, entre más tiempo mayor son los niveles de afectación en las pérdidas económicas, en el inicio de la operación del negocio, su productividad en el daño de imagen o reputación y las sanciones que conlleva.

En una Mipymes las diferentes consecuencias se ven de forma directa impactando a sus clientes y sus proveedores, llevando a la perdida de la imagen corporativa e incertidumbre en los empleados.

Las consecuencias son las siguientes:

Responsabilidad civil o penal

En el caso que no se puede recuperar rápidamente los cliente o proveedores puede realizar acciones legales contra las organizaciones que pueden pedir indemnización por los daños y perjuicios por el incumplimiento de contratos que están sujetos a la productividad que produzca daños por negligencia.

Daños económicos por no actividad de la empresa.

El malware tipo ransomware afecta directamente las finanzas de las Mipymes afectadas en las que se encuentran:

1. Perdida de información sensible o confidencial.
2. Costos por el secuestro de la información.
3. Costos por la contratación de expertos o consultores expertos en ciberseguridad.
4. Costo en las sanciones o multas por incumplimiento.
5. Costo en la investigación del ataque del ransomware.
6. Costo en la restauración de la información.
7. Gastos en la interrupción del negocio.
8. Costos por perdida de confianza los sus clientes.
9. Pérdida de confianza trabajadores cualificados.

Reputación ante sus clientes y proveedores.

La reputación da un golpe económico bastante grave a las Mipymes ya que sus clientes pierden la confianza y eso se ve reflejado en las finanzas de las organizaciones, y generando consecuencias legales.

6 ÍNDICES DE ATAQUES INFORMÁTICOS TIPO RANSOMWARE Y SU NIVEL DE IMPACTO EN LA INFRAESTRUCTURA TI Y EN LOS PROCESOS DE TRANSFORMACIÓN DIGITAL EN LAS MIPYMES.

6.1 CIFRAS ALARMANTES

- El porcentaje de los ataques de ransomware estuvieron dirigidos a países de Latinoamérica es del 60%[13].
- En un 85% aumentaron las víctimas de ransomware en el último año.
- El 80% de las organizaciones fueron atacada por un ransomware.
- Se estima que se registró un ataque de ransomware cada 11 segundos en 2021.
- En la actualidad se han creado 32 nuevas familias de ransomware fueron descubiertas en 2021, un aumento del 26% respecto al año anterior.
- Con un 15,5%, Conti fue la variante de ransomware más activa del mercado 2n 2021 y lo siguen Sodinokibi con un 7.1%.
- Conti recibió la mayor cantidad de pagos por rescates unos 13 millones de dólares.
- Le siguió Sodinokibi con 12.13 millones de dólares y DarkSide con 4.6 millones de dólares.

[13] RANSOMWARE EN AMERICA [Sitio Web] [Consultado el 26 de mayo 2022] Disponible en: http://globalcyber.cl/

- El valor de 5,4 millones de dólares fue la mayor demanda por un rescate solicitada por atacante. El valor promedio de rescates solicitados se aproximadamente es de 2.2 millones.

- En 2021, los ataques de ransomware contra los gobiernos aumentaron hasta tres veces el punto más alto del año anterior.

6.2 COSTOS GLOBALES POR DAÑOS POR RANSOMWARE

A continuación, en la siguiente tabla muestra los costos asociados a los ataques del malware tipo ransomware y su proyección al año 2028.

Tabla 3 Costos globales de un ransomware

AÑO	COSTO
2015	$325 Millones
2017	$5 Billones
2021	20 Billones
2024	42 Billones
2026	71,5 Billones
2028	157 Billones

Fuente: "Cybersecurity ventures. [Sitio Web] [Consultado el 20 de mayo 2021]. Disponible en: https://cybersecurityventures.com/"

6.3 RANSOMWARE EN COLOMBIA

Según el Ingeniero Wilson Prieto director de ciber inteligencia I+D+i GAMMA INGENIEROS dice lo siguiente:

"El ransomware es uno de los tipos de programas maliciosos más utilizados, y la falacia de dernières années tiene un impacto significativo en el mundo de los ciberataques. Para los grupos organizados de ciberdelincuencia, es un negocio altamente rentable con millones de dólares en ingresos, falta de acción a nivel corporativo y la oportunidad de acceder fácilmente con la educación adecuada en el ciberespacio. Higiene del usuario. La utilidad definitiva. En este sentido, el ataque al sistema US Colonial Pipeline, que provocó la interrupción e interrupción inminente de los servicios de gas natural en mayo del año pasado, tiene un impacto significativo en los activos de países críticos donde este tipo de amenazas es sumamente grave y grave. Muestra que puede dar. Impacto en los seres humanos, el medio ambiente y la economía.

En el caso de Colombia, en los últimos años, gracias a diversas investigaciones, se ha logrado registrar ciertas actividades y agentes maliciosos como Spalax [14], APT-C-36 [15], Blackyte. Su método de operación durante la fase de reconocimiento con el objetivo de hacerse pasar por una agencia gubernamental de identificación a través de phishing en línea (correo electrónico o comunicación de phishing dirigida a personas, organizaciones o empresas específicas) por varios métodos., Varias campañas maliciosas han sido lanzado. El acceso remoto y varios recursos respaldan el ciclo de vida del enemigo, lo que le permite eludir la seguridad del sistema y, en última instancia, provocar el robo y la eliminación de información. Uno de los ataques que marcan el 2022 en nuestro país estaba dirigido a los observadores gubernamentales de alimentos y drogas y se cree que está relacionado con una variante de Blackbyte a través de ransomware. Servicio como Servicio (RaaS), terminología utilizada el 11 de febrero de 2022, Aviso Conjunto de Seguridad Cibernética de la Oficina Federal de Investigaciones (FBI) y el Servicio Secreto de los Estados Unidos.

Actualmente, con respecto a las amenazas de ransomware, Cyber Edge Group, una firma consultora de investigación y marketing que se especializa en proveedores de servicios de seguridad y necesidades de proveedores de servicios anunció en el Informe de Defensa de Amenazas Cibernéticas 2022. Los encuestados enfatizaron que las amenazas cibernéticas más alarmantes están relacionadas con ransomware, mostrando organizaciones que lograron atacar en 2021 (93,9 %), de las cuales (53,1 %) %). Esta amenaza, estas consecuencias, sugieren que Japón enfrenta importantes desafíos a nivel gubernamental y empresarial".

[14] Porolli, M. (2021, junio 12). Operación Spalax: Ataques de malware dirigidos en Colombia. WeLiveSecurity. [Sitio Web] [Consultado 20 de mayo 2022] Disponible en: https://www.welivesecurity.com/la-es/2021/01/12/operacion-spalax-ataques-malware-dirigidos-colombia/

[15] Informe de información de Nobuyoshi Kiyasu | Seguimiento del caso. (2019, febrero 18). APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations. Centro de inteligencia de amenzas de Qi Anxin. [Sitio Web] [Consultado el 20 de mayo 2022] Disponible en: https://ti.qianxin.com/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/

7 MECANISMOS DE PREVENCIÓN Y MEDIDAS DE SEGURIDAD CONTRA ATAQUES DE RANSOMWARE PARA LAS MIPYMES COLOMBIANAS.

El ransomware es una forma de malware encargo de cifrar archivos en un dispositivo, inutilizando los archivos y los sistemas que dependen de ellos, para que el ciberdelincuente busque que le den una recompensa a cambio de descifrar los archivos. En la pandemia del Covid 19 a las Mipymes colombianas se incrementó este tipo de incidente del Ransomware.

El incidente del ransomware puede afectar los procesos comerciales dejando a las Mipymes dejarlas sin operación y no pueden brindar servicios de misión crítica como la facturación, ventas y otros procesos esenciales de cada organización.

Los impactos económicos y reputacionales de este tipo de malware ransomware durante la interrupción inicial que dejo el ataque y que las Mipymes se demoran en recuperarse se convierte en un rete de las empresas. A continuación, se analizará las mejores prácticas de prevención del malware ransomware, lista de verificación de respuestas del ransomware y herramientas para su prevención.

Es importante que las empresas tomen diferentes medidas que existen en la actualidad, para combatir un Ransomware y minimizar sus efectos. Se va a verificar las siguientes medidas, la prevención, mitigación y como recuperar los sistemas.

7.1 PREVENCIÓN

Se puede pensar en la prevención como las medidas que se toman antes de que ocurra un ataque, con el objetivo de prevenirlo o reducir sus efectos. La prevención del es probablemente la medida más eficaz, ya que, si se evita el ataque o si está dispuesto a recuperar todos los archivos afectados por un ataque, el ataque no tendrá consecuencias.

En esta medida que son recomendables para cualquier Ransomware y en general se debe tener presente los siguientes puntos.

- Tener parcheado los Sistemas Operativos y programas que utilicen diariamente en la operación de cada empresa.

- Realizar la configuración del Firewall restringiendo los puertos que no necesitemos.
- Instalar un Antivirus con detención de Ransomware.
- Restringir el acceso al Wifi, cambiar constantemente las contraseñas.
- Aplicar la política de contraseñas de la empresa, contraseñas robustas.
- Aplicar los filtros de Spam de los correos.
- Capacitación constante a los empleados.
- No pagar rescate

7.2 BACKUP

El más eficiente para contrarrestar un Ransomware es el Backup, por ello es el más importante en el caso que nos lleguen a secuestrar los archivos, que es la razón de un ransomware encriptar y pedir un pago para descifrarlos, al tener una copia podemos continuar con el negocio o lo servicios prestados y recuperar el 100% de información. Y realmente es lógico realizarlo.

La organización en su plan de respaldo de backups protegerá los archivos importantes para que puedan ser recuperados en caso de pérdida de información. Esto es muy importante ya que él tiene muchas causas por las cuales los usuarios pueden experimentar este problema. Por ejemplo, la vida útil limitada de los discos duros el robo o pérdida de dispositivos y el malware antes mencionado.

Recuerde que las copias de seguridad se pueden ejecutar los ransomware . Por esta razón no se recomienda conectar permanentemente unidades de cinta a la misma red de producción ya que de esta manera en caso de que esta red se infecte pueden verse afectadas. Por otro lado, es importante para el que los usuarios que no tengan un disco duro que posean el mantengan una copia de seguridad de su información con el dispositivo respaldado porque si lo roban o lo pierden lo harán también perderá el respaldo.

Prevención para el tipo de Ransomware:

1. Aplicar el Parche para la vulnerabilidad MS17-010
2. Apartar los equipos que fueron involucrados.

3. Desactivar el servicio SMBv1.
4. En los puertos 137/UDP / 138/UDP y los puertos 139/TCP Y 445/TCP. Estos puertos se deben bloquear en las empresas.
5. El Netbios se debe bloquear.
6. En el navegador TOR bloquearlo, ya que por ese medio envían las llaves de encriptación.

7.3 MITIGACION

Medidas necesarias si la organización fue víctima de un ataque de ransomware , realizando la investigación para detectarlo lo antes posible donde está, y no perder más información. Tener presente que un ransomware la principal forma de ejecución es la encriptación de archivos, el comportamiento se puede evidencias en tres etapas:

1. El malware ransomware abre el documento, realiza la encriptación y cierra el documento.
2. El malware ransomware lee un documento realiza una copia, lo encripta y elimina el original.
3. El malware ransomware lee un documento, realiza una copia del archivo y lo encripta y el archivo original lo sobrescribe para eliminar la información.

En la administración de tareas se puede revisar el comportamiento de la lectura de archivos, pero se puede confundir con otros programas, el cual es importante refinar el sistema.

También se puede revisar la entropía[16], que significa la incertidumbre de la información al realizar la comparación de un archivo encriptado aumenta rápidamente su entropía, la mejora es hacer que realice la comparación del archivo que se está sobrescribiendo con el valor resultante de su entropía[17].

[16] N. Smart *et al.*, “Cryptography: An Introduction (3rd Edition),” vol. 3, p. 436.
[17] UNA MEDIDA DE LA INCERTIDUMBRE BASADA EN LA ENTROPÍA PARA CUANTIFICAR EL IMPACTO DE LA PÉRDIDA DE INFORMACIÓN DE LOS SISTEMAS DE GESTIÓN. [2021][online] Disponibles en: https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/4849/Schwarz_Diaz_Max.pdf?sequence=1&isAllowed=y

En las preferencias del ransomware[18] en los tipos de archivos con extensiones .doc, pdf, jpg, etc.… que son los archivos que utiliza diariamente el usuario, el cual tiene más de 116 extensiones, el cual encripta la información y cambia de extensión, ejemplo. LOCK, en este caso revisar estos tipos de extensiones.

Ya detectado el malware ransomware, revisar que este eliminado, se tiene que aislar el equipo, para que no propague el virus en la red de nuestro sistema, que el equipo no tenga conexión a internet, para que no enviara o reciba información y realizar lo siguiente:

- Inmediatamente desmontar las unidades de red que tenga el equipo.
- Desconexión de la red del equipo involucrado.

En el caso que no se pueda realizar lo anterior apagar el equipo y evitar que encripte más archivos y revisar el disco de forma segura.

7.4 ¿INFECTADOS QUE HACER?

- Desconectar inmediatamente las conexiones de red.
- Desconectarse de internet y apagar el WIFI en casos extremos.
- Verificar que la contraseña del equipo no este bloqueado.
- Reportar al caso a la autoridad competente de Colombia.
- Tener presente la documentación o evidencia del ataque, hora, fecha, equipos, tipos de ransomware.
- Visite www.nomoreransom.org y utilizar las herramientas gratuitas si el ransomware está en el listado.
- Formatee los equipos y reinstale el sistema operativo.
- Restaurar las copias de seguridad o backup
- Revisar con una conexión segura a internet y descargar las actualizaciones de los sistemas operativos[19].

[18] Julian Bhardwaj, "Techniques in ransomware explained," Naked Security, 2012. [Online]. Available: https://nakedsecurity.sophos.com/2012/09/14/new-technique-in-ransomware-explained/. [Accessed: 08-Dic-2021].
[19] NO MÁS RANSOMWARE. [2021][ONLINE] [Consultado el 08 de diciembre] Disponibles en: https://www.nomoreransom.org/en/prevention-advice-for-businesses.html

7.5 RECUPERACION

Teniendo en cuenta que la empresa ya fue afectada por el malware ransomware y que le afectaron en gran medida los documentos que se encuentran encriptados, es conocer el tipo de ransomware que lo afecto y visitar la página www.nomoreransom.org, el cual tiene herramientas de desencriptación si existe el nombre en el listado, también presente que debe tener un backup de la organización y restaurarlo cuando tenga segura la red, antes no.

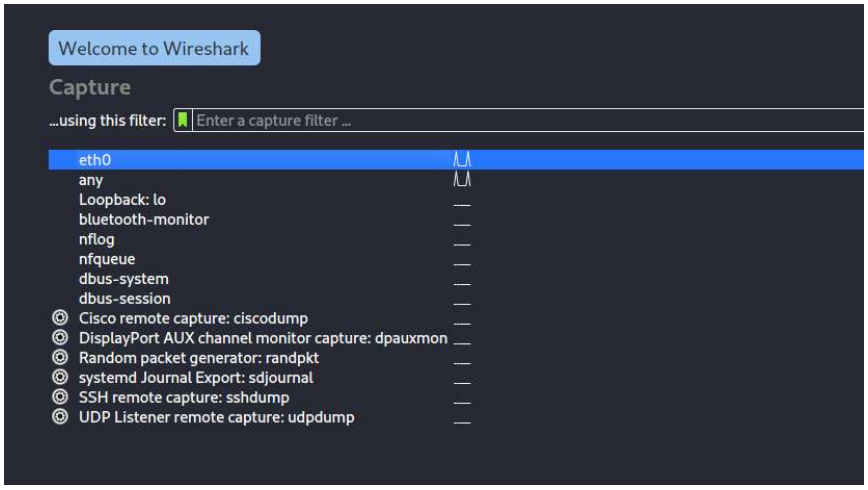
Recuperación de la contraseña.

En el caso que realice el rescate los ciberdelincuentes le enviaran la contraseña en el mejor de los casos sin garantía, por ello no es bueno, ni recomendable pagar ese rescate de información ya que incentiva al delincuente.

Pero hay otra forma con una herramienta de Sniffing como Wireshark y que no ayuda a interceptar la clave, a continuación, se debe seguir estos pasos:

1. Descargar e instalar Wireshark

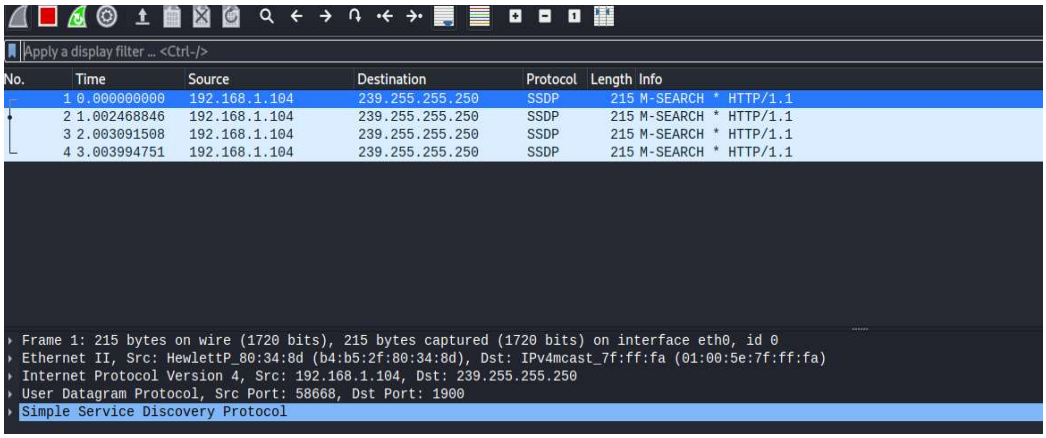
Figura 8 Wireshark



Fuente: "Elaboración propia"

2. Ejecutar Wireshark y empezar a analizar los paquetes.

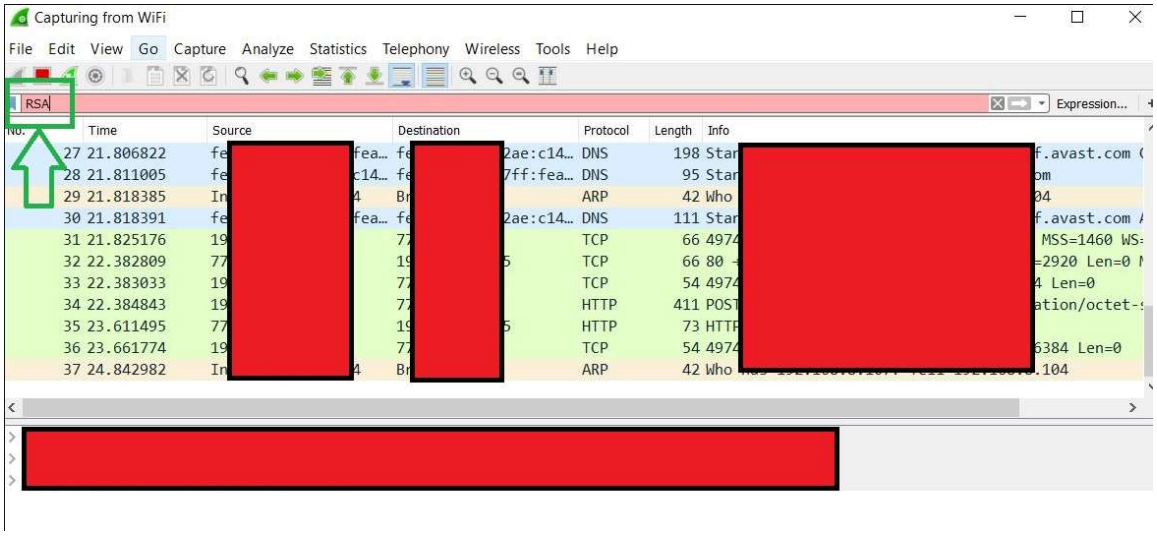
Figura 9 Escaneo de paquetes



Fuente: "Elaboración propia"

3. Encuentra el paquete que busca de tipo RSA

Figura 10 RSA

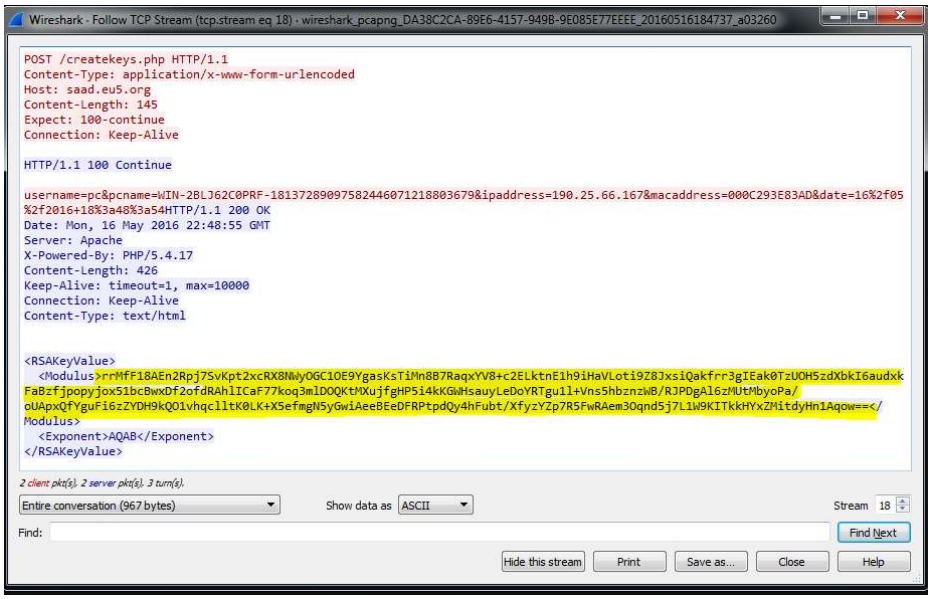


Fuente: https://sensorstechforum.com/wp-content/uploads/2016/05/2.jpg

4. Encontrar la llave.

En el momento de realizar la verificación se encuentra la clave RSA.

Figura 11 Llave RSA



Fuente: https://sensorstechforum.com/wp-content/uploads/2016/05/wireshark-solution2-sensorstechforum.png

Volcado de memoria

Existe otra forma de revisar la clave, en la ejecución de ransomware el necesita utilizar la memoria, para ello se utiliza archivo que se guardar en C:\Windows\Minidump con herramientas forenses[20] se puede realizar[21].

7.6 ANALISIS DE INDICES DE ATAQUES INFORMATICOS

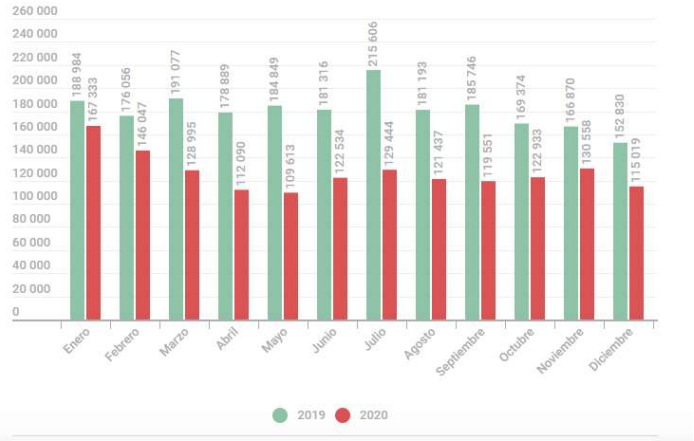
En 2019, el número total de usuarios únicos que encontraron ransomware en todas las plataformas fue de 1 537 465. En 2020, este número se redujo a 1 091 454, una disminución del 29%[22].

[20] K. Amari, K. A. Mil, and C. Cid, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory Techniques and Tools for Recovering and Analyzing Data from Volatile Memory GCFA Gold Certification Techniques and Tools for Recovering and Analyzing Data from Volatile Memory 3," *SANS Inst.*, p. 61, 2009.

[21] Chris Hoffman, "Windows Memory Dumps: ¿What Exactly Are They For?," *Hot-To Geek*, 2014. [Online]. Available: https://www.howtogeek.com/196672/windows-memory-dumps-what-exactly-are-they-for/. [Accessed: 08-Dic-2021].

[22] Ransomware [Sitio Web] [Consultado el 14 de abr. de 22] Disponible en: https://securelist.lat/ransomware-by-the-numbers-reassessing-the-threats-global-impact/93569

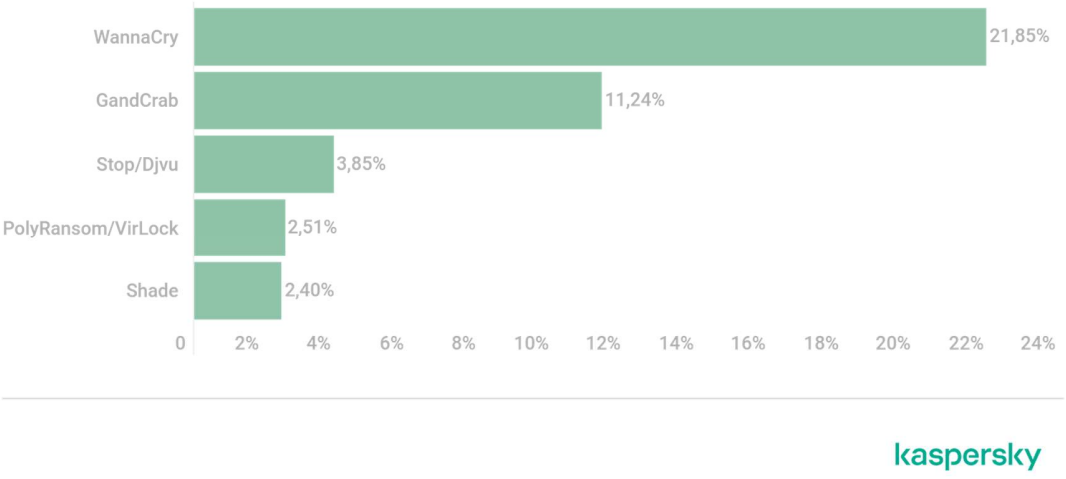
Figura 12 Índice Usuarios único Ransomware



Fuente:" Ransomware [Sitio Web] [Consultado el 14 de abr. de 22] Disponible en: https://securelist.lat/ransomware-by-the-numbers-reassessing-the-threats-global-impact/93569/"

En Colombia se han materializado familias de ransomware en la figura muestra el porcentaje de afectación.

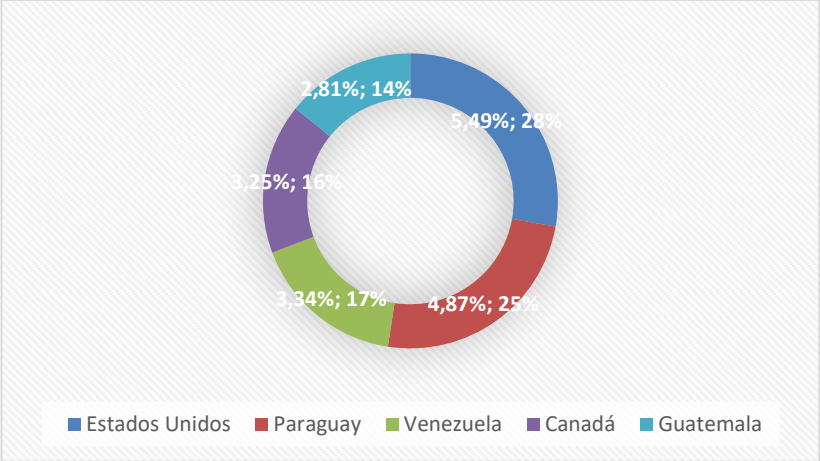
Figura 13 Índice de Ransomware afectando a las Mipymes



Fuente:" Kaspersky [Sitio Web] [Consultado el 14 de abril de 2022] Disponible en https://securelist.lat/ransomware-by-the-numbers-reassessing-the-threats-global-impact/93569/"

En el siguiente índice muestra que estados unidos tiene un 28% de afectación y Guatemala tiene el 14 % de afectación.

Figura 14 Índice de afectación ransomware en América



Fuente:" Kaspersky [Sitio Web] [Consultado el 14 de abril de 2022] Disponible en https://securelist.lat/ransomware-by-the-numbers-reassessing-the-threats-global-impact/93569/"

7.7 MEJORES PRÁCTICAS DE PREVENCIÓN DE RANSOMWARE

Revisando las mejores prácticas y referencias para minimizar el riesgo que representa el malware ransomware de debe realizar de forma coordinada y eficiente en la empresa de Mipymes ante un incidente del ransomware, se debe aplicar en lo posible estas prácticas en función de defender los recursos de la organización.

1. Los respaldos de la información se deben cifrar, estar fuera de línea de la red y probar periódicamente las copias de seguridad, estas copias de seguridad se deben llevar con frecuencia y tener una copia en la empresa y fuera de ella. Ya que las variantes del ransomware intentan encontrar y eliminar las copias de seguridad accesibles ejemplo una NAS. Mantener las copias de seguridad evita pagar un rescate por los datos y pueda iniciar su operación rápidamente.

2. Mantener las copias de los sistemas operativos virtualizados es decir backup de las máquinas virtuales y de los sistemas operativos para que puedan ser reconstruidos rápidamente para iniciar operación.

3. Conservar le hardware de respaldo para reconstruir los sistemas en el caso que no se pueda iniciar operación con la infraestructura primaria, ya que al tener incompatibilidad en las versiones de los sistemas operativos puede llevar a no funcionar correctamente.

4. Tener unas copias de respaldo del software o código fuente aplicable o ejecutables deben estar disponibles, entre otras guardar las licencias y demás llaves o keys para poderlos restaurar rápidamente.

5. Realizar un plan de acción de respuesta a incidentes cibernéticos, ante un incidente de un malware de tipos ransomware, con un plan de comunicación y notificación en una organización[23].

7.7.1 VECTORES DE INFECCION DEL RANSONWARE

Para el tipo de incidente del ransomware es importante conocer los tipos de vectores que utilizan los ciberdelincuentes y poder minimizar el riesgo.

7.7.1.1 VULNERABILIDADES DE INTERNET Y CONFIGURACIONES INCORRECTAS

1. Realice análisis de vulnerabilidades regulares para identificarlas y realizar un plan de acción, en los dispositivos que tienen salida de internet, para limitar el ataque[24] como:

    - Valoración Evaluación y Normalización
    - Escaneo de vulnerabilidades
    - Evaluación de campañas de phishing

[23] ESCC Playbook: A Crises Management Framework for the ESCC (Available to ESCC members. Contact secretariat@electricitysubsector.org or visit www.electricitysubsector.org to learn more.)
[24] Centro de recursos cibernéticos. [2022]. [online]. Disponible en: https://www.cisa.gov/cyber-resource-hub

- Evaluación de riesgos y vulnerabilidades
- Revisión de resiliencia cibernética
- Recursos descargables de CRR
- Evaluación de la Gestión de Dependencias Externas

2. Parchee y actualice periódicamente el software y los sistemas operativos a las últimas versiones disponibles.

3. Deshabilite SMBv1 y v2 en su red interna después de trabajar para mitigar cualquier, por ejemplo, deshabilite los puertos y protocolos que no se utilizan para fines comerciales (p. ej., Protocolo de escritorio remoto [RDP] – Protocolo de control de transmisión [TCP] Puerto 3389).

4. Emplear las mejores prácticas para el uso de RDP y otros servicios de escritorio remoto. Los actores de amenazas a menudo obtienen acceso inicial a una red a través de servicios remotos expuestos y mal asegurados, y luego propagan ransomware[25].

5. Audite la red en busca de sistemas que utilicen RDP, cierre los puertos RDP no utilizados, aplique bloqueos de cuentas después de un número específico de intentos, aplique la autenticación multifactor (MFA) y registre los intentos de inicio de sesión de RDP.

6. Deshabilite o bloquee la salida del protocolo del bloque de mensajes del servidor (SMB) y elimine o deshabilite las versiones obsoletas de SMB. Los actores de amenazas usan SMB para propagar malware entre organizaciones. En función de esta amenaza específica, las organizaciones deben considerar las siguientes acciones para proteger sus redes:

    - Bloquee todas las versiones de SMB para que no sean accesibles externamente a su red bloqueando el puerto TCP 445 con protocolos relacionados en los puertos 137–138 del Protocolo de datagramas de usuario y el puerto TCP 139.

[25] CISA AA20-073A, Enterprise VPN Security. [2022]. [online]. Disponible en: https://us-cert.cisa.gov/ncas/alerts/aa20-073a

- Eliminar las dependencias a través de actualizaciones y reconfiguraciones, es importante actualiza a la versión más reciente de SMB_V3 junto con la firma SMB.

7.7.1.2 VECTOR PHISHING

1. Con recursos humanos realizar capacitaciones de concientización de usuarios de en ciberseguridad como evitar y reportar actividades sospechosas y muy importante realizar pruebas de phishing controlados para reforzar la importancia de las capacitaciones.
2. Implementar filtros de puerta de enlace de emails para filtrar los correos electrónicos con indicadores maliciosos, como líneas de asunto maliciosas conocidas, y bloqueo indicadores maliciosos, como líneas de asunto maliciosas conocidas, y bloqueo.
3. Considere deshabilitar macro scripts para archivos de Microsoft Office transmitidos a través de Email. Estas macros se pueden usar para entregar ransomware.
4. Para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos, implementar autenticación de mensajes basada en dominio, generación de informes y Verificación y política de conformidad (DMARC)

7.7.1.3 VECTOR INFECCIÓN DE MALWARE PRECURSOR Y RANSOMWARE

1. Asegúrese de que las firmas y el software antivirus y antimalware estén actualizados fecha. Además, active las actualizaciones automáticas para ambas soluciones. CISA recomienda utilizar una solución antivirus gestionada de forma centralizada. Esto permite detección de malware "precursor" y ransomware.

2. Una infección de ransomware puede ser evidencia de una infección anterior no resuelta compromiso de la red. Por ejemplo, muchas infecciones de ransomware son el resultado de infecciones de malware existentes, como TrickBot, Dridex o Emotet.

3. En algunos casos, la implementación de ransomware es solo el último paso en un compromiso de la red y se descarta como una forma de ofuscar anteriores actividades posteriores al compromiso.

4. Utilice la lista de permitidos del directorio de aplicaciones en todos los activos para asegurarse de que solo el software autorizado puede ejecutarse y todo el software no autorizado se bloquea de ejecutar:

    - Habilite la lista de permitidos del directorio de aplicaciones a través del software de Microsoft Política de restricción o AppLocker.

    - Use la lista blanca de directorios en lugar de intentar enumerar cada posible permutación de aplicaciones en un entorno de red.

    - Los valores predeterminados seguros permiten que las aplicaciones se ejecuten desde PROGRAMFILES, ARCHIVOS DE PROGRAMA (X86) y SISTEMA32. No permitir todas las demás ubicaciones ARCHIVOS DE PROGRAMA (X86) y SISTEMA32. No permitir todas las demás ubicaciones

5. Considere implementar un sistema de detección de intrusos (IDS) para detectar actividad de comando y control y otra red potencialmente maliciosa actividad que ocurre antes de la implementación del ransomware.

7.7.1.4 VECTOR DE TERCEROS Y PROVEEDORES DE SERVICIOS

1. Tener en cuenta la gestión de riesgos y cibernética prácticas de higiene de terceros o proveedores de servicios gestionados (MSP) en los que se basa su organización para cumplir su misión. Los MSP han sido un vector de infección para el ransomware que afecta a las organizaciones de los clientes.

2. Si un tercero o MSP es responsable de mantener y asegurar las copias de seguridad de su organización, asegúrese de que estén siguiendo las mejores prácticas aplicables descritas anteriormente. Usar el lenguaje del contrato para formalizar sus requisitos de seguridad es una buena práctica.

3. Comprender que los adversarios pueden explotar la confianza relaciones que tienen la organización con terceros y MSP[26]

4. Los adversarios pueden falsificar la identidad de entidades con las que su organización tiene una relación de confianza, o usar cuentas de correo electrónico comprometidas, para phishing a sus usuarios, lo que permite el compromiso de la red y la divulgación de información.

7.7.2 MEJORES PRACTICAS DE LOS SISTEMAS DE INFORMACION

Emplear MFA para todos los servicios en la medida de lo posible, particularmente para correo web, redes privadas virtuales y cuentas que acceden a sistemas críticos.

1. Si usas contraseñas, utilizar contraseñas seguras para varias cuentas. Cambiar las contraseñas predeterminadas. Aplicar bloqueos de cuenta después de un número específico de intentos de inicio de sesión. Los administradores de contraseñas pueden ayudarlo a desarrollar y administrar contraseñas seguras. ÿ Si un tercero o MSP es responsable de mantener.

2. Aplicar el principio de privilegio mínimo a todos los sistemas y servicios para que los usuarios solo tengan el acceso que necesitan para realizar su trabajo. Los actores de amenazas a menudo buscan cuentas privilegiadas para aprovechar y ayudar a saturar las redes con ransomware.

3. Restrinja los permisos de los usuarios para instalar y ejecutar aplicaciones de software.

4. Limitar la capacidad de una cuenta de administrador local para iniciar sesión desde una sesión interactiva local por ejemplo "Denegar el acceso a esta computadora desde la red" y evitar el acceso a través de una sesión RDP.

[26] APT´s en la seguridad. [2022][online] Disponible en: https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers

5. Elimine cuentas y grupos innecesarios y restrinja el acceso raíz.

6. Controlar y limitar la administración local.

7. Utilice el grupo Active Directory de usuarios protegidos en Windows en dominios para proteger aún más las cuentas de usuarios privilegiados contra los ataques passthe-hash.

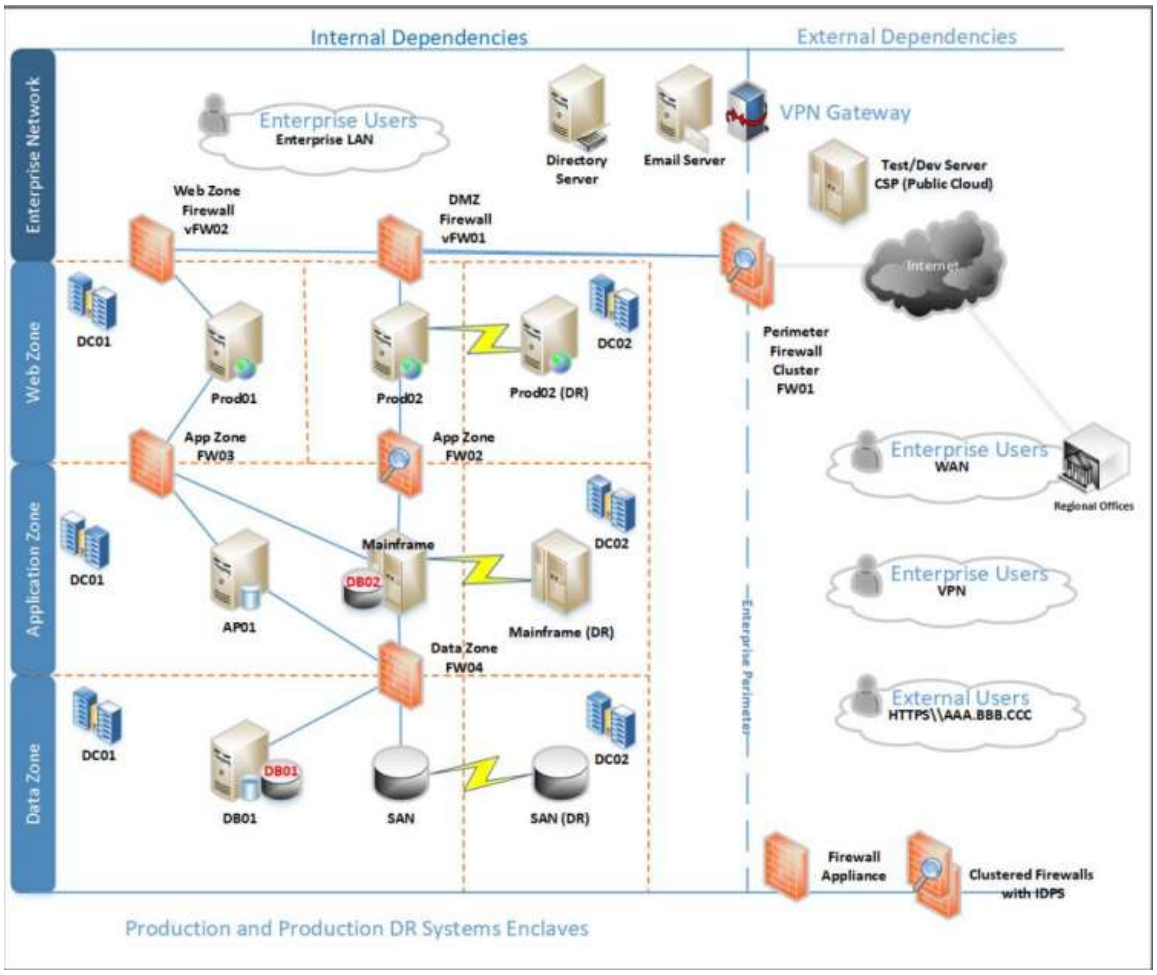
8. Auditar las cuentas de los usuarios con regularidad, en particular el monitoreo remoto y Cuentas de administración que son de acceso público: esto incluye auditorías de acceso de terceros otorgado a los MSP.

9. Aprovechar las mejores prácticas y habilitar configuraciones de seguridad en asociación con entornos de nube, como Microsoft Office 365[27]

10. Desarrollar y actualizar regularmente un diagrama de red integral que describe los sistemas y los flujos de datos dentro de la red de su organización.

[27] Microsoft Office 365 [2022][ONLINE]. Disponible en: https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a

Figura 15 Infraestructura ideal



Fuente: https://www.cisa.gov/cyber-resource-hub

- Esto es útil en estado estable y puede ayudar a los respondedores de incidentes a comprender dónde enfocar sus esfuerzos.

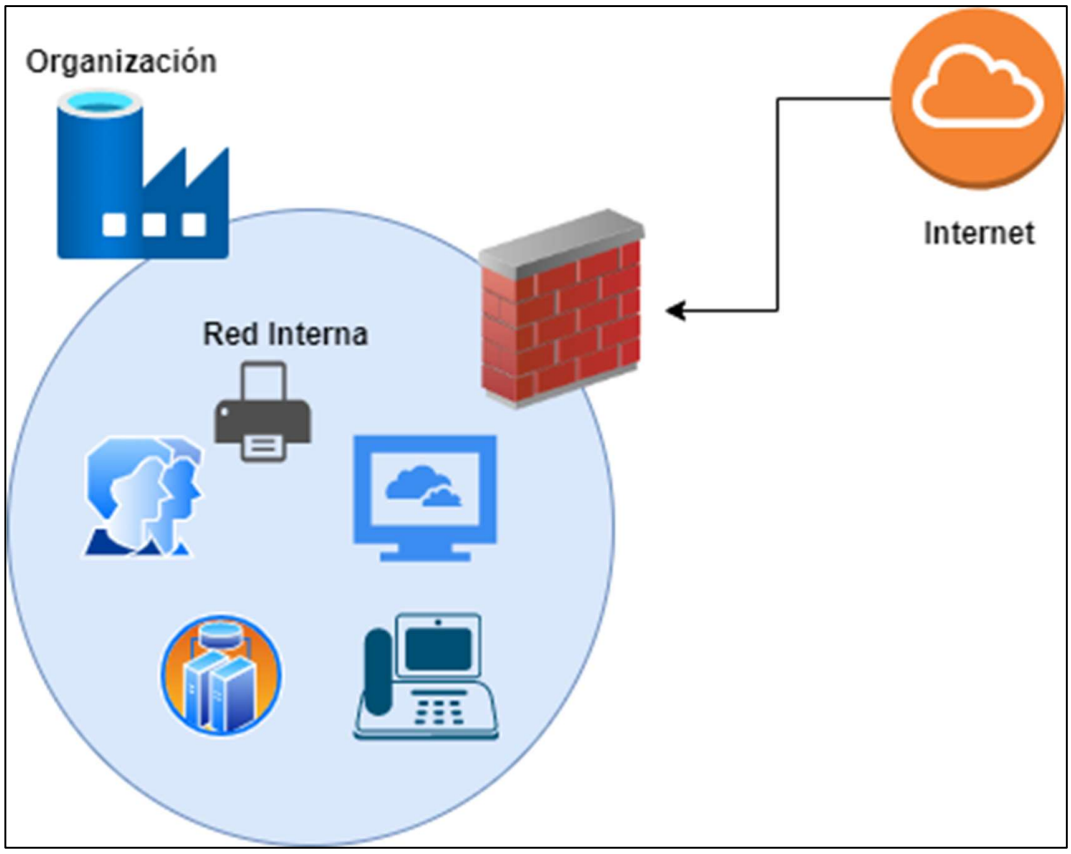
- El diagrama debe incluir representaciones de las principales redes cubiertas, cualquier esquema de direccionamiento IP específico y la topología general de la red (incluidas las conexiones de red, las interdependencias y el acceso otorgado a terceros o MSP).

- Emplear medios lógicos o físicos de segmentación de red para separar varias unidades de negocios o recursos de TI departamentales dentro de su organización, así como para mantener la separación entre TI y la tecnología operativa.

Esto ayudará a contener el impacto de cualquier intrusión que afecte a su organización y evitará o limitará el movimiento lateral por parte de los malintencionados.

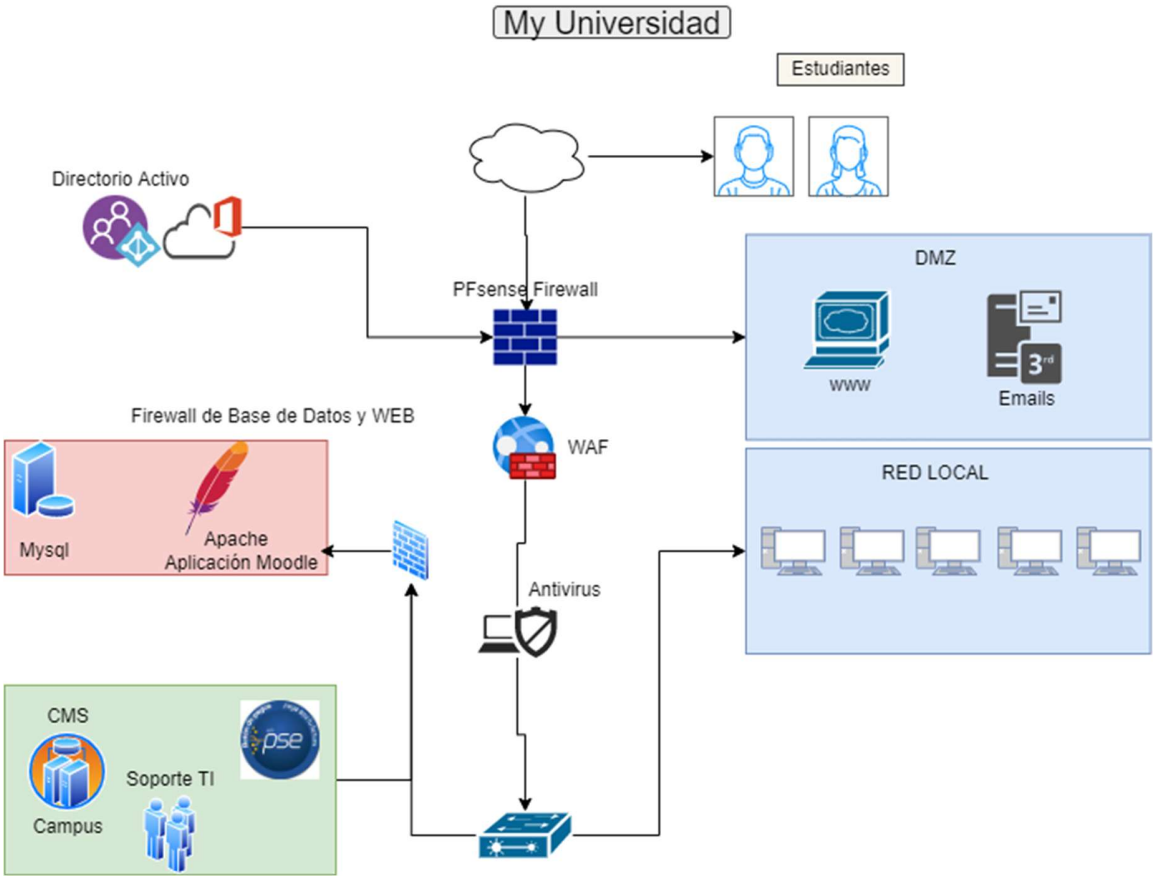
A continuación, las figuras 10 y 11, muestran la red fragmentada segura y no segura.

Figura 16 Red no segmentada No segura



Fuente:" https://www.cisecurity.org/insights/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet"

Figura 17 Infraestructura Segmentada ideal



Fuente: https://www.cisecurity.org/insights/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet

11. Asegúrese de que su organización tenga un enfoque integral de gestión de activos, es decir deben tener la administración y gestión de activos.

12. Restrinja el uso de PowerShell, mediante la directiva de grupo, a usuarios específicos caso por caso.

13. Asegúrese de que las instancias de PowerShell (utilice la versión más actual) tengan módulo, bloque de script y registro de transcripción habilitado (registro mejorado).

14. Los dos registros que registran la actividad de PowerShell son los de Windows "PowerShell"

Registro de eventos y el registro "Operativo de PowerShell". CISA recomienda activar estos dos registros de eventos de Windows con un período de retención de 180 días. Estos registros deben verificarse periódicamente para confirmar si los datos de registro se han eliminado o si se ha desactivado el registro. Establezca el tamaño de almacenamiento permitido para ambos registros lo más grande posible.

15. Controladores de dominio seguros (DC). Los actores de amenazas a menudo apuntan y usan los DC como punto de partida para propagar el ransomware en toda la red.

La siguiente lista contiene sugerencias de alto nivel sobre la mejor manera de asegurar un Controlador de Dominio:

- Asegúrese de que los controladores de dominio se actualicen con regularidad. Esto incluye la aplicación de críticas.
- Asegúrese de que se esté utilizando la versión más reciente del sistema operativo Windows Server en los DC.
- Asegúrese de que no haya ningún software o agente adicional instalado en los DC, ya que estos se pueden aprovechar para ejecutar código arbitrario en el sistema.
- El acceso a los DC debe estar restringido al grupo Administradores. Usuarios dentro este grupo debe ser limitado y tener cuentas separadas utilizadas para el día a día operaciones con permisos no administrativos.
- Los firewalls de host de DC deben configurarse para evitar el acceso a Internet. Por lo general, estos los sistemas no tienen una necesidad válida de acceso directo a Internet. Actualizar servidores con la conectividad a Internet se puede utilizar para extraer las actualizaciones necesarias en lugar de permitir acceso a internet para DC.

7.8 LISTADO DE VERIFICACION DE PREVENCION DEL RANSOMWARE

Si su organización es víctima de ransomware, CISA recomienda enfáticamente responder utilizando la siguiente lista de verificación. Asegúrese de pasar por los siguientes pasos:

7.8.1 DETECCION Y ANALISIS DEL RANSOMWARE

1. Determinar qué sistemas se vieron afectados e inmediatamente aislarlos.

    - Si varios sistemas o subredes parecen afectados, desconecte la red en el nivel del conmutador. Puede que no sea factible desconectar sistemas individuales durante un incidente.

    - Si no es posible desconectar la red temporalmente de inmediato, ubique el cable de red (por ejemplo, Ethernet) y desconecte los dispositivos afectados de la red o elimínelos de WiFi para contener la infección.

    - Después de un compromiso inicial, los actores maliciosos pueden monitorear la actividad o las comunicaciones de su organización para comprender si se han detectado sus acciones. Asegúrese de aislar los sistemas de manera coordinada y utilice métodos de comunicación fuera de banda, como llamadas telefónicas u otros medios, para evitar avisar a los actores que han sido descubiertos y que se están tomando medidas de mitigación. No hacerlo podría hacer que los actores se muevan lateralmente para preservar su acceso, ya una táctica común, o implementar ransomware ampliamente antes de que las redes se desconecten.

2. Solo en caso de que no pueda desconectar los dispositivos de la red, apáguelos para evitar una mayor propagación de la infección de ransomware.

3. Clasificar los sistemas afectados para su restauración y recuperación.

4. Consulte con su equipo para desarrollar y documentar una comprensión inicial de lo que ha ocurrido en base al análisis inicial.

5. Usando la información de contacto a continuación, involucre a sus equipos internos y externos y a las partes interesadas con una comprensión de lo que pueden proporcionar para ayudarlo a mitigar, responder y recuperarse del incidente.

7.8.2 CONTENCION Y ERRADICACION

1. Tome una imagen del sistema y una captura de memoria de una muestra de los dispositivos afectados (p. ej., estaciones de trabajo y servidores). Además, recopile todos los registros relevantes, así como muestras de cualquier archivo binario de malware "precursor" y observables o indicadores asociados de compromiso (por ejemplo, direcciones IP de comando y control sospechosas, entradas de registro sospechosas u otros archivos relevantes detectados). Los contactos a continuación pueden ayudarlo a realizar estas tareas.

2. Consulte a la policía federal sobre los posibles descifradores disponibles, ya que los investigadores de seguridad ya han descifrado los algoritmos de cifrado para algunas variantes de ransomware.

3. Investigue la guía confiable (es decir, publicada por fuentes como el gobierno, MSISAC, un proveedor de seguridad acreditado, etc.) para la variante de ransomware en particular y siga los pasos adicionales recomendados para identificar y contener sistemas o redes que se confirmen que ser impactado.

4. Identifique los sistemas y cuentas involucrados en el incumplimiento inicial. Esto puede incluir cuentas de correo electrónico.

5. Acciones adicionales sugeridas: pasos de identificación rápida del cifrado de datos del lado del servidor:

    - En caso de que se entere de que una estación de trabajo infectada está cifrando los datos del lado del servidor, los pasos de identificación rápida son:

a) Revise Administración de equipos > Sesiones y Abrir Listas de archivos en servidores asociados para determinar el usuario o sistema accediendo a esos archivos.

b) Revise las propiedades de los archivos cifrados o las notas de rescate para identificar usuarios específicos que pueden estar asociados con el archivo propiedad.

a) Revise el registro de eventos de TerminalServices-RemoteConnectionManager para verificar si hay conexiones de red RDP exitosas.

b) Revise el registro de seguridad de Windows, los registros de eventos SMB y cualquier registro relacionado que pueda identificar una autenticación importante o acceder a eventos.

a) Ejecute Wireshark en el servidor afectado con un filtro para identifique las direcciones IP involucradas en la escritura activa o el cambio de nombre de los archivos por ejemplo "smb2.filename contiene cryptxxx").

6. Realizar un examen de los sistemas existentes de detección o prevención de la organización (antivirus, Detección y respuesta de punto final, IDS, Sistema de prevención de intrusiones, etc.) y registros. Si lo hace, puede resaltar la evidencia de sistemas adicionales o malware involucrado en etapas anteriores del ataque.

7. Realice un análisis extenso para identificar los mecanismos de persistencia de afuera hacia adentro y de adentro hacia afuera.

8. Reconstruir sistemas basados en una priorización de servicios críticos (p. ej., salud y seguridad o servicios generadores de ingresos), utilizando imágenes estándar preconfiguradas, si es posible.

9. Una vez que el entorno se haya limpiado y reconstruido por completo (incluidas las cuentas afectadas asociadas y la eliminación o corrección de los mecanismos de persistencia maliciosos), restablezca las contraseñas de todos los sistemas afectados y aborde las vulnerabilidades asociadas y las lagunas en la seguridad o la visibilidad. Esto puede incluir la aplicación de parches, la

actualización del software y la adopción de otras precauciones de seguridad que no se hayan tomado previamente.

10. Según los criterios establecidos, que pueden incluir seguir los pasos anteriores o buscar ayuda externa, la TI designada o la autoridad de seguridad de TI declara que el incidente de ransomware ha terminado

7.8.3 RECUPERACION Y POSTINCIDENTE

En los siguientes pasos realizar para recuperación de la información ante el ataque del ransomware.

1. Vuelva a conectar los sistemas y restaure los datos de las copias de seguridad encriptadas fuera de línea en función de la priorización de los servicios críticos.

2. Documentar las lecciones aprendidas del incidente y las actividades de respuesta asociadas para informar las actualizaciones y refinar las políticas, los planes y los procedimientos organizacionales y guiar los ejercicios futuros de los mismos.

3. Tenga cuidado de no volver a infectar los sistemas limpios durante la recuperación. Por ejemplo, si se ha creado una nueva red de área local virtual con fines de recuperación, asegúrese de que solo se le agreguen sistemas limpios.

4. Considere compartir lecciones aprendidas e indicadores relevantes de compromiso con CISA o su sector ISAC/ISAO para compartir más y beneficiar a otros dentro de la comunidad.

5. Reportar el incidente a las autoridades de cada país.

7.9 HERRAMIENTAS RECOLECCION, EXPLOTACION Y POSTEXPLOTACION

7.9.1 RECOLECCIÓN PASIVA DE INFORMACIÓN

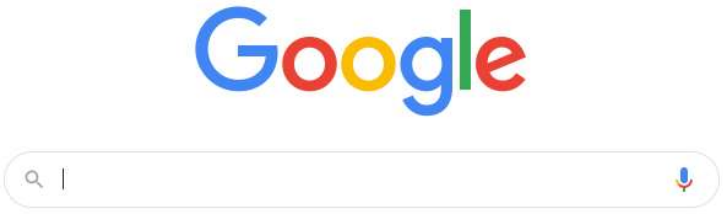
Esta fase el atacante realiza una investigación sobre un objetivo en este caso a una empresa u organización, sin que las diferentes formas de obtener información sean detectadas por el objetivo.

Los atacantes utilizan las bases públicas donde almacenan información y utilizan las siguientes herramientas para hacerlo:

GOOGLE HACKING

Técnica que utilizan los ciberdelincuentes para indexar páginas web, obtenido información que las mismas organizaciones publican, esta se divide en operadores lógicos y comandos[28].

Figura 18 Buscador Google

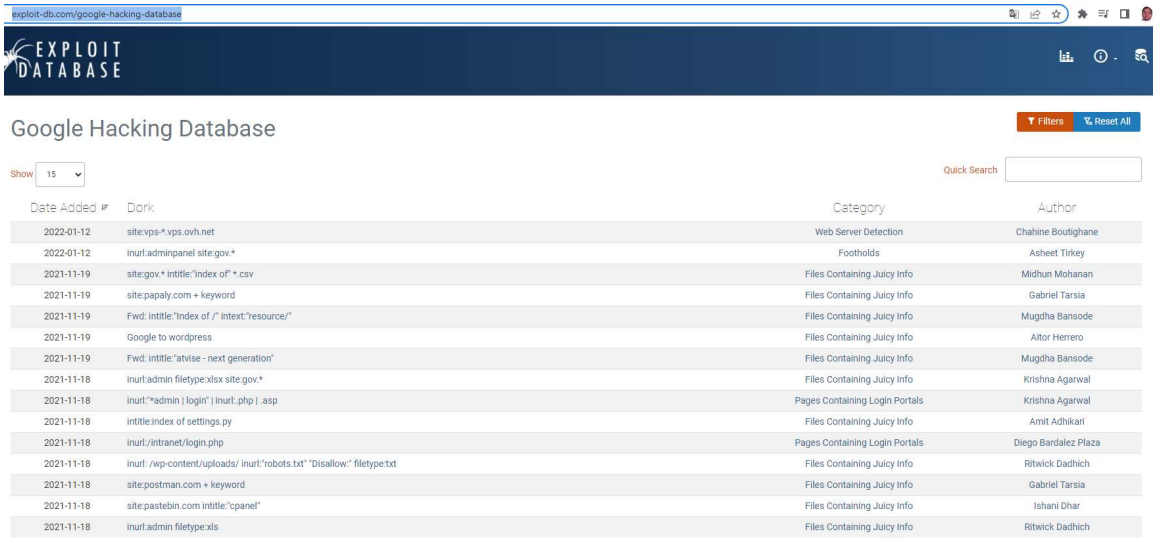


Fuente:" https://www.google.com/"

[28] Google Hacking. [Consultado el 28 de febrero 2022] Disponible en: https://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/3172-google-hacking-que-es-y-como-aprovecharlo

Existe muchos comandos que se encuentra en Exploit Databases[29] y actualizados a la fecha.

Figura 19 Exploit Database GOOGLE HACKING

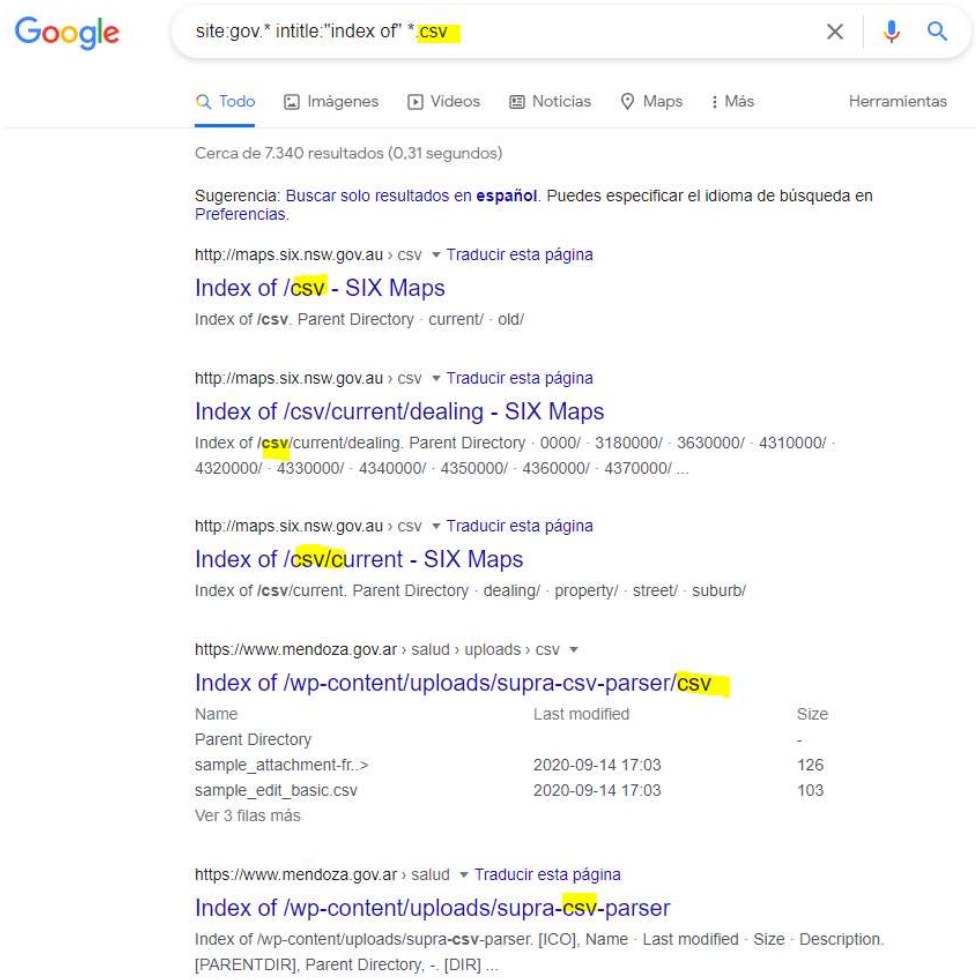


Fuente: "HACKING GOOGLE. [2022][ONLINE]. Disponible en: https://www.exploit-db.com/google-hacking-database"

Un ejemplo de comando **site:gov.* intitle:"index of" *.csv** el cual filtra todas la paginas index y que contengan archivos con extensión .csv separado por comas en páginas que terminen en gov es decir gobierno.

[29] HACKING GOOGLE. [2022][ONLINE]. Disponible en: https://www.exploit-db.com/google-hacking-database

Figura 20 Comando Google hacking



Fuente: "Elaboración propia"

COMANDOS PRINCIPALES GOOGLE HACKING

A continuación, se muestran los comandos principales que podemos utilizar con Google. Hay que tener en cuenta que todos ellos deben ir seguidos (sin espacios) de la consulta que quiere realizarse:

define: término: se muestra la definición del sitio para el término de búsqueda.

filetype: término: la búsqueda se limita a las páginas cuyo nombre termina con el término especificado. Se utiliza principalmente para determinar la extensión de los archivos requeridos. Nota: comando

ext: término usado de manera equivalente.

Site:sitio/dominio: los resultados están restringidos al contenido del sitio o dominio específico. Muy útil para encontrar sitios que no tienen su propio motor de búsqueda interno.

Link:url - Muestra páginas que apuntan a la página identificada por dicha url. El número (y la calidad) de los enlaces a una página determina su relevancia para los motores de búsqueda. Nota: solo muestra páginas con un rango de página de 5 o superior.

Cache: url - La versión de la página determinada por la url que Google tiene en su memoria para mostrar, es decir, la copia que Googlebot creó la última vez que visitó esta página.

info:url: Google mostrará información sobre el sitio que coincide con la URL.

Related: url - Google mostrará páginas similares a la especificada por la url. Nota: Es difícil entender qué tipo de relación tiene en cuenta Google para mostrar estas páginas. Muchas veces no ayuda.

allinanchor: términos: Google limita las búsquedas a páginas a las que apuntan enlaces cuyo texto contiene términos de búsqueda.

inanchor: término: Las búsquedas se limitan a aquellas a las que apuntan los enlaces cuyo texto contiene el término especificado. A diferencia de allinanchor, se puede combinar con misiones regulares.

allintext: término: la búsqueda se limita a los resultados que contienen términos en el texto de la página.

intext: término - Limite los resultados a los textos que contienen el término en el texto. A diferencia de allintext, se puede combinar con términos de búsqueda habituales. allinurl: términos: solo se devolverán los resultados que contengan los términos de búsqueda en la URL.

inurl: término: los resultados se limitan a aquellos que contienen palabras clave en la URL. A diferencia de allinurl, se puede combinar con términos de búsqueda regulares.

allintitle: término: limita los resultados a aquellos que contienen los términos en el título.

intitle: término: limita los resultados a los documentos que contienen el término en el título. A diferencia de allintitle, se puede combinar con términos de búsqueda habituales.

OPERADORES BOOLEANOS GOOGLE HACKING

Google hace uso de los operadores booleanos para realizar búsquedas combinadas de varios términos. Esos operadores son una serie de símbolos que Google reconoce y modifican la búsqueda realizada:

" " – en el buscado busca las palabras exactas

\- Excluye todas las palabas en el input de navegador de búsqueda de Google.

OR (o |) – Busca en diferentes páginas una opción u otra.

\+ - Permite incluir varias palabras en el buscado de Google.

* - Se utiliza como comodín para complementar una palabra.

7.9.2 RECOLECCIÓN SEMIPASIVA DE INFORMACIÓN

Es la recolección de información sobre un objetivo o victima determinado utilizando métodos que se asimilen al tráfico de red y un comportamiento normal que suele recibir cualquier organización.

Lo que más utilizan los ciberdelincuentes se centran en lo siguiente:

- Consulta de servidores DNS
- Acceso de recursos internos de las aplicaciones WEB, ejemplo .pdf o .txt
- Análisis de metadatos.
-

Las consultas se realizan en bases de datos públicas.

¿Qué es un DNS?

- **DNS** es un acrónimo de Domain Name System
- Realizan una traducción de nombres de los dominios a direcciones Ip´
- Corresponde a unos de los protocolos más importante del internet.

¿Porque los ciberdelincuentes les interesa estos DNS?

- Obtiene la dirección publica sobre un dominio u organización.
- Puede descubrir relaciones entre dominios y hosts internos de las empresas.
- Puede utilizar herramientas de explotación para ganar o acceder a los sistemas de las organizaciones.

7.9.3 RECOLECCIÓN ACTIVA DE LA INFORMACIÓN

Esta técnica de recolección activa de la información consiste en obtener información sobre el objetivo determinado utilizando métodos que interactúan directamente con la organización.

Dentro de las actividades que utilizan los ciberdelincuentes son:

- Escaneo de puertos.
- Escaneo de Hosts
- Escaneo de servicios

Si las empresas tienen un sistema de detención a intrusiones es fácil de detectar si no está expuesto a un ataque.

Las herramientas que más utilizan.

- **NMAP:** Es una utilidad para la exploración de redes o la auditoría de seguridad. Admite escaneo de ping (determina qué hosts están activos), muchas técnicas de escaneo de puertos, detección de versiones (determina protocolos de servicio y versiones de aplicaciones que escuchan.

- **METASPLOIT:** Con esta herramienta tiene una dirección ip objetivo, buscan el servicio o vulnerabilidades y les regresa un exploit que puede vulnerar un sistema con un payload.

- **NESSUS:** Programa de escaneo de vulnerabilidades muy utilizando por las profesiones en seguridad informática tiene una licencia free y de pago.

- **OPENVAS:** Escaneo de varias máquinas a la vez por su segmentación. Soporte de SSL para OTP gestión de notas para los resultados de escaneos.

7.9.4 EXPLOTACION Y HACKING DE VULNERABILIDADES

En esta técnica ya teniendo la información de las fases anteriores se procede a realizar la explotación de vulnerabilidades, para ello ya tenemos información importante como son los hosts, puerto abierto y los servicios y además el sistema operativo con sus vulnerabilidades.

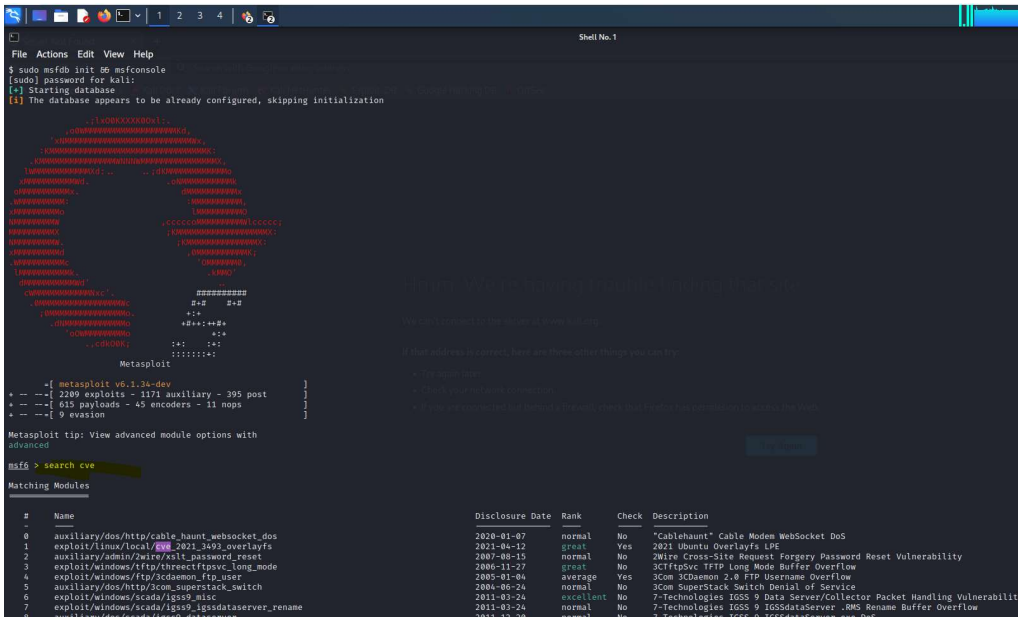
Con esta información los ciberdelincuentes utilizan los exploit y los payload, para poder comprometer un sistema, buscando su vulnerabilidad.

Figura 21 Metasploit-framwork

Fuente: “Measploit-Framwwork [Sitio web] [Consultado el 03 de marzo 2022] Disponible en: https://www.kali.org/tools/metasploit-framework/”

Con el framework Metasploit con la información del objetivo, buscan el servicio o vulnerabilidades y les regresa un exploit que puede vulnerar un sistema con un payload.

Figura 22 Explotar vulnerabilidades con Framework Metasploit



Fuente: “Elaboración propia”

7.9.5 TECNICAS DE POST EXPLOTACION

La fase de post explotación consiste en determinar el valor de los recursos que han sido comprometidos en las fases anteriores de los procesos de recolección de información.

El valor se puede medir en la importancia y de la sensibilidad de la información que almacenan o por la capacidad de un ciberdelincuente para comprometer recursos dentro de la organización.

Debe garantizarse que los procesos de negociación del cliente no se vean expuestos a un nivel mayor de riesgo debido a la realización del hacking.

8 LAS VULNERABILIDADES INFORMÁTICAS QUE PUEDEN CONTRIBUIR A UN ATAQUE RANSOMWARE EN LAS MIPYMES

8.1 PROGRAMA CVE®

La misión del Programa CVE® es identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas públicamente. Hay un Registro CVE para cada vulnerabilidad en el catálogo. Las vulnerabilidades son descubiertas, luego asignadas y publicadas por organizaciones de todo el mundo que se han asociado con el Programa CVE. Los socios publican registros CVE para comunicar descripciones consistentes de vulnerabilidades. Los profesionales de la tecnología de la información y la ciberseguridad utilizan CVE Records para asegurarse de que están discutiendo el mismo problema y para coordinar sus esfuerzos para priorizar y abordar las vulnerabilidades[30].

Tabla 4 Vulnerabilidades Ransomware CVE

VULNERABILIDAD	DETALLE
CVE-2021-42258	BQE BillQuick Web Suite 2018 a 2021 anterior a 22.0.9.1 permite la inyección SQL para la ejecución remota de código no autenticado, tal como se explotó en octubre de 2021 para la instalación de ransomware. La inyección de SQL puede, por ejemplo, usar el parámetro txtID (también conocido como nombre de usuario). La explotación exitosa puede incluir la capacidad de ejecutar código arbitrario como MSSQLSERVER$ a través de xp_cmdshell.
CVE-2020-9452	Se descubrió un problema en Acronis True Image 2020 24.5.22510. anti_ransomware_service.exe incluye la funcionalidad de poner en cuarentena los archivos al copiar un archivo sospechoso de ransomware de un directorio a otro usando los privilegios del SISTEMA. Debido a que los usuarios sin privilegios tienen permisos de escritura en la carpeta de cuarentena, es posible controlar esta escritura privilegiada con un enlace fijo. Esto

[30] Programa CVE. [Consultado 08 de marzo 2022]. [ONLINE]. Disponible en: https://www.cve.org/About/Overview

	significa que un usuario sin privilegios puede escribir/sobrescribir archivos arbitrarios en carpetas arbitrarias. La escalada de privilegios a SYSTEM es trivial con escrituras arbitrarias. Si bien la función de cuarentena no está habilitada de forma predeterminada, se puede obligar a copiar el archivo a la cuarentena comunicándose con anti_ransomware_service.exe a través de su API REST.
CVE-2020-9451	Se descubrió un problema en Acronis True Image 2020 24.5.22510. anti_ransomware_service.exe mantiene un registro en una carpeta donde los usuarios sin privilegios tienen permisos de escritura. Los registros se generan en un patrón predecible, lo que permite que un usuario sin privilegios cree un enlace fijo desde un archivo de registro (aún no creado) a anti_ransomware_service.exe. Al reiniciar, esto obliga al servicio anti_ransomware a intentar escribir su registro en su propio proceso, lo que genera una VIOLACIÓN DE COMPARTIR. Este bloqueo se produce en cada reinicio.
CVE-2020-9450	Se descubrió un problema en Acronis True Image 2020 24.5.22510. anti_ransomware_service.exe expone una API REST que todos pueden usar, incluso los usuarios sin privilegios. Esta API se utiliza para comunicarse desde la GUI con anti_ransomware_service.exe. Esto se puede explotar para agregar un ejecutable malicioso arbitrario a la lista blanca, o incluso excluir una unidad completa de la supervisión de anti_ransomware_service.exe.
CVE-2020-6023	Check Point ZoneAlarm anterior a la versión 15.8.139.18543 permite que un actor local aumente los privilegios mientras restaura archivos en Anti-Ransomware.
CVE-2020-6022	Check Point ZoneAlarm anterior a la versión 15.8.139.18543 permite que un actor local elimine archivos arbitrarios mientras restaura archivos en Anti-Ransomware.

CVE-2020-6012	ZoneAlarm Anti-Ransomware anterior a la versión 1.0.713 copia archivos para el informe desde un directorio con pocos privilegios. Un atacante cronometrado sofisticado puede reemplazar esos archivos con contenido malicioso o vinculado, como explotar CVE-2020-0896 en sistemas sin parches o usar enlaces simbólicos. Esto permite que un usuario sin privilegios habilite la escalada de privilegios a través del acceso local.
CVE-2020-28950	El instalador de Kaspersky Anti-Ransomware Tool (KART) anterior a KART 4.0 Parche C era vulnerable a un ataque de secuestro de DLL que permitía a un atacante elevar los privilegios durante el proceso de instalación.
CVE-2018-6318	En Sophos Tester Tool 3.2.0.7 Beta, el controlador carga (en el contexto de la aplicación utilizada para probar un exploit o ransomware) la DLL mediante una carga útil que se ejecuta desde NTDLL.DLL (por lo tanto, se ejecuta en el espacio del usuario), pero el controlador no realiza ninguna validación de esta DLL (ni su firma, ni su hash, etc.). Una persona puede cambiar esta DLL de forma local, o con una conexión remota, a una DLL maliciosa con el mismo nombre, y cuando se usa el producto, se cargará esta DLL maliciosa, también conocida como un ataque de secuestro de DLL.
CVE-2018-19589	Los controles de acceso incorrectos del oficial de seguridad (SO) en el proveedor PKCS11 R2 que se envía con el paquete del producto Utimaco CryptoServer HSM permiten que un SO autenticado en una ranura recupere los atributos de las claves marcadas como claves privadas en el almacenamiento externo de claves y también elimine las claves marcadas como privadas. claves en el almacenamiento de claves externo. Esto compromete la disponibilidad de todas las claves configuradas con almacenamiento de claves externo y puede resultar en un ataque económico en el que el atacante niega a los usuarios legítimos el acceso a las claves mientras mantiene la posesión de una copia cifrada (blob) del almacén

	de claves externo a cambio de rescate. Este ataque se ha denominado ataque de ransomware inverso y puede ejecutarse a través de una conexión física al CryptoServer o una conexión remota si SSH o el acceso remoto al LAN CryptoServer se han visto comprometidos. La Confidencialidad e Integridad de las claves afectadas,
CVE-2017-18362	La integración de ConnectWise ManagedITSync hasta 2017 para Kaseya VSA es vulnerable a los comandos remotos no autenticados que permiten el acceso directo completo a la base de datos de Kaseya VSA. En febrero de 2019, los atacantes explotaron activamente esto para descargar y ejecutar cargas útiles de ransomware en todos los puntos finales administrados por el servidor VSA. Si la página ManagedIT.asmx está disponible a través de la interfaz web de Kaseya VSA, cualquier persona con acceso a la página puede ejecutar consultas SQL arbitrarias, tanto de lectura como de escritura, sin autenticación.

Fuente: "https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=RANSOMWARE"

8.2 HERRAMIENTAS NMAP, NESSUS Y OPENVAS PARA BUSQUEDA DE VULNERABILIDADES.

Tabla 5 Herramientas para búsqueda de vulnerabilidades

HERRAMIENTA	DESCRIPCION	CARACTERISTICAS	LICENCIA	REQUERIMIENTO	DESCARGA
Nmap 	Nmap es una utilidad para la exploración de redes o la auditoría de seguridad. Admite escaneo de ping (determina qué hosts están activos), muchas técnicas de escaneo de puertos, detección de versiones (determina protocolos de servicio y versiones de aplicaciones que escuchan	Descubrimiento de sistemas operativos Identificación de puerto abiertos Identificación de servicios. Identifica vulnerabilidades Escaneo silencioso que no detecta el Firewall	GPL v2	Multiplataforma Procesador de 64 o 32 Disco duro mayor a 30 MB Memoria mayor a 512 MB	https://nmap.org/

	detrás de los puertos) y huellas dactilares de TCP/IP (sistema operativo de host remoto o identificación de dispositivo). Nmap también ofrece especificaciones flexibles de objetivos y puertos, escaneo señuelo/sigilo, escaneo sunRPC y más. La mayoría de las plataformas Unix y Windows son compatibles con los modos GUI y línea de comandos. También se admiten varios	

	dispositivos de mano populares, incluidos Sharp Zaurus y iPAQ.				
Openvas	Framework que integra varios servicios de escaneo y gestión de vulnerabilidades	Escaneo de varias máquinas a la vez por su segmentación. Soporte de SSL para OTP Gestión de notas para los resultados de escaneos. Gestión de falsos positivos en el escaneo. Gestión de administración de usuarios. Escaneos en programación de tareas	GNU General licencia publica	Mutiplataforma	https://www.openvas.org/

Nessus	Programa de escaneo de vulnerabilidad es muy utilizando por las profesiones en seguridad	Fácil de implementar y usar. Detección avanzada con más de 65000CVE Investigación de vulnerabilidad es día cero. Visibilidad precisa en redes. Reportes fáciles de entender Calificación de las vulnerabilidad es	BSD / Propietary	Multiplataform a	https://es-la.tenable.com/products/nessus/nessus-professional
WireShark	Analizador de protocolos o Snnifer	Verifica el tráfico de la red con diferentes protocolos. Verificación de redes LAN y WiFi. Filtrado de los paquetes.	BSD / Propietary	Multiplataform a, mínimo requerido básico	https://www.wireshark.org/

		Lee y escribe diferentes formatos de lectura.			
MetaSploit	Framework para pruebas de penetración,	Escanea diferentes importaciones de datos. Escaneo la red. Integración de escaneo con Nessus, Nmap y Openvas. Gestión de sesiones. Módulos de Postexplotación Payload Exploit Interfaz web	BSD / Proprietary	Multiplataforma	https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers

Fuente:” Elaboración propia”

9 CONCLUSIONES

- Se estableció los niveles de afectación que produce los diferentes tipos de ransomware a partir de su origen, características y funcionamiento, a partir de una investigación sobre el ransomware basado en su historia y en su afectación a las empresas colombianas.

- Se identificó el ciclo de vida y los diferentes tipos de ransomware, a partir de una investigación sobre el ransomware basado en su historia y en su afectación a las empresas colombianas.

- Se verificó en base a fuentes documentales los índices de ataques informáticos tipo Ransomware y su nivel de impacto en la infraestructura TI y en los procesos de transformación digital en las MiPymes, mediante se identifican factores importantes como su prevención, backup y mitigación y recuperación.

- Se analizó las diferentes medidas de que pueda hacer una organización, mediante los factores importantes como su prevención, backup y mitigación y recuperación.

- Se identificó las vulnerabilidades informáticas que pueden contribuir a un ataque ransomware en las MiPymes, con herramientas que ayudan a identificarlas para minimizar el riesgo de materialización ante un ataque tipo ransomware.

- Se revisó diferentes herramientas de escaneo de la red para encontrar vulnerabilidades y cerrar la brecha de seguridad con herramientas que ayudan a identificarlas para minimizar el riesgo de materialización ante un ataque tipo ransomware.

- Se propuso mecanismos de prevención y medidas de seguridad contra ataques de ransomware para las MiPymes colombianas realizando las mejores prácticas en su prevención, identificando los vectores de infección, el endurecimiento o hardening de los sistemas informáticos, un listando de verificación si fue atacado y finalmente una verificación de prevención, detección, contención, erradicación y recuperación ante un incidente de tipos ransomware.

10 RECOMENDACIONES

Realizar capacitaciones contantes al usuario final en ciberseguridad para minimizar los índices de ataques informáticos tipo ransomware.

Analizar la infraestructura con herramientas que puedan dar un diagnóstico de vulnerabilidades que contribuyen a materializar un ataque tipo ransomware, como Nessus, Nmap, OpenVas, etc.

Estructurar mecanismos de prevención y medidas de seguridad contra ataques de ransomware para las mipymes colombianas, para saber qué hacer ante un incidente.

Realizar un endurecimiento de los sistemas de información en su infraestructura con las mejores prácticas en cada activo que tienen en una compañía.

Planificar auditorías internas con expertos en seguridad informática de tipo de sobrero blanco, para minimizar las vulnerabilidades de una empresa colombiana.

Recolectar información pasiva, semipasiva y activa de la empresa, ya que con esta información podemos cerrar brechas de seguridad.

Realizar backup diarios de los sistemas de información, como máquinas virtuales, Bases de datos, ficheros, etc.., y demás activos importantes, los respaldos deben estar offline y online, para recuperar información rápidamente ante un ataque de tipo ransomware.

Implementar un Sistema de Gestión de los sistemas de información SGSI y una gestión de la administración del riesgo informáticos internos que minimicen la intrusión de un atacante.

Verificar constantemente las vulnerabilidades en el programa CVE, ya que existen programa maligno de día cero, es decir que no tiene parches de seguridad y no se sabe su afectación.

Reportar a las autorizades competentes o CIRT para reportar el tipo de ransomware y en la fiscalía, para la parte legal y estadísticas.

11 BIBLIOGRAFÍA

Ahmad O. Almashhadani, Mustafa Kaiiali, Sakir Sezer, and Philip O'Kane. 2019. A multi-classifier network-based crypto ransomware detection system: A case study of locky ransomware. IEEE Access 7 (2019), 47053–47067.

Akashdeep Bhardwaj, Vinay Avasthi, Hanumat Sastry, and G. V. B. Subrahmanyam. 2016. Ransomware digital extortion: A rising new age threat. Indian J. Sci. Technol. 9, 14 (2016), 1–5.

Al-rimy, Bander Ali Saleh and Maarof, Mohd Aizaini and Shaid, Syed Zainudeen Mohd. 2018. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Comput. Secur. 74 (2018), 144–166.

ÁLVARO URIBE VÉLEZ. Fabio Valencia Cossio. LEY 1273 DE 2009. [ON LINE]. 2009.[14 DE noviembre del 2021] Disponible en: https://www.enticconfio.gov.co/images/stories/normatividad/Ley_1273_de_2009%20.pdf

Alzahrani, Abdulrahman and Alshehri, Ali and Alshahrani, Hani and Fu, Huirong. 2020. Ransomware in Windows and Android platforms. arXiv preprint arXiv:2005.05571 (2020).

Amin Azmoodeh, Ali Dehghantanha, Mauro Conti, and Kim-Kwang Raymond Choo. 2018. Detecting cryptoransomware in IoT networks based on energy consumption footprint. J. Amb. Intell. Human. Comput. 9, 4 (2018), 1141–1152.

ATAQUES DE ACCESO REMOTO RDP. [Sitio Web] [Consultado el 14 de abril de 2022] Disponible en: https://prensariotila.com/32980-colombia-sufre-mas-de-91-millones-de-ataques-de-acceso-remoto-en-2020/
Ataques de ransomware: riesgos, medidas de protección y prevención. [ONLINE]. 2021.[14 noviembre 2021]. Disponible en: https://ieeexplore-ieee-org.bibliotecavirtual.unad.edu.co/document/9548507

Aurangzeb, Sana and Aleem, Muhammad and Iqbal, Muhammad Azhar and islam, Muhammad Arshad. 2017. Ransomware: A survey and trends. J. Inf. Assur. Secur. 6, 2 (2017).

Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainuddin Mohd Shaid. 2017. A 0-day aware cryptoransomware early behavioral detection framework. In International Conference of Reliable Information and Communication Technology. Springer, 758–766.

Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, and Syed Zainudeen Mohd Shaid. 2019. Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection. Fut. Gen. Comput.Syst. 1, 101 (2019), 476–491.

Bander Ali Saleh Al-rimy, Mohd Aizaini Maarof, Yuli Adam Prasetyo, Syed Zainudeen Mohd Shaid, and Asmawi Fadillah Mohd Ariffin. 2018. Zero-day aware decision fusion-based model for crypto-ransomware early detection. Int. J. Integ. Eng. 10, 6 (2018).

Berrueta, Eduardo and Morato, Daniel and Magaña, Eduardo and Izal, Mikel. 2019. A survey on detection techniques for cryptographic ransomware. IEEE Access 7 (2019), 144925–144944.

Centro de recursos cibernéticos. [2022]. [online]. Disponible en: https://www.cisa.gov/cyber-resource-hub
Centro de recursos cibernéticos. [2022]. [online]. Disponible en: https://www.cisa.gov/cyber-resource-hub

Chainanalysis Team. 2014. Building trust in blockchains. Disponible en: https://www.chainalysis.com/.

Chen, Ping and Desmet, Lieven and Huygens, Christophe. 2014. A study on advanced persistent threats. In IFIP International Conference on Communications and Multimedia Security. Springer, 63–72.

Chris Hoffman, "Windows Memory Dumps: ¿What Exactly Are They For?," Hot-To Geek, 2014. [Online]. Available: https://www.howtogeek.com/196672/windows-memory-dumps-what-exactly-are-they-for/. [Accessed: 08-Dic-2021].

Continella, Andrea and Guagnelli, Alessandro and Zingaro, Giovanni and De Pasquale, Giulio and Barenghi, Alessandro and Zanero, Stefano and Maggi, Federico. 2016. ShieldFS: A self-healing, ransomware-aware filesystem. In 32nd Conference on Computer Security Applications. 336–347.

Cuneyt Gurcan Akcora, Yitao Li, Yulia R. Gel, and Murat Kantarcioglu. 2019. BitcoinHeist: Topological data análisis for ransomware detection on the bitcoin blockchain. arXiv preprint arXiv:1906.07852 (2019).

Delgado Fernández, T. (2021). Taxonomía de Transformación Digital. Revista Cubana De Transformación Digital, 1(1), 4–23. Recuperado a partir de https://rctd.uic.cu/rctd/article/view/62 (Original work published 21 de abril de 2020)

DIAZ RHENALS, Karina. Análisis de fenómenos ransomware, su afectación en la ciberseguridad y herramientas de contraataque en mipymes. [en lí-nea] Montevideo: Facultad de Ingeniería, 2022-02-16. [Fecha consulta: 14 de abril 2022].

ESCC Playbook: A Crises Management Framework for the ESCC (Available to ESCC members. Contact secretariat@electricitysubsector.org or visit www.electricitysubsector.org to learn more.)

Formas de defenderse del ransomware. Wall Street Journal (en línea), [sl], pág. 1, 20 de agosto. 2016. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=asn&AN=117557612&lang=es&site=ehost-live. Acceso: 8 de diciembre. 2021.

Google Hacking. [Consultado el 28 de febrero 2022] Disponible en: https://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/3172-google-hacking-que-es-y-como-aprovecharlo IEEE, 3222–3226.

Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC'15). IEEE, 79–84.

Julian Bhardwaj, "Techniques in ransomware explained," Naked Security, 2012. [Online]. Available: https://nakedsecurity.sophos.com/2012/09/14/new-technique-in-ransomware-explained/. [Accessed: 08-Dic-2021].

K. Amari, K. A. Mil, and C. Cid, "Techniques and Tools for Recovering and Analyzing Data from Volatile Memory Techniques and Tools for Recovering and Analyzing Data from Volatile Memory GCFA Gold Certification Techniques and Tools for Recovering and Analyzing Data from Volatile Memory 3," SANS Inst., p. 61, 2009.

Manaar Alam, Sarani Bhattacharya, Debdeep Mukhopadhyay, and Anupam Chattopadhyay. 2018. Rapper: Ransomware prevention via performance counters. arXiv preprint arXiv:1802.03909 (2018).

Maxat Akbanov, Vassilios G. Vassilakis, and Michael D. Logothetis. 2019. Ransomware detection and mitigation using software-defined networking: The case of WannaCry. Comput. Electr. Eng. 76 (2019), 111–121.

Maxat Akbanov, Vassilios G. Vassilakis, and Michael D. Logothetis. 2019. WannaCry Ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications & Information Technology 1 (2019).

Microsoft Office 365 [2022][ONLINE]. Disponible en: https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a

Mohammad Mehdi Ahmadian, Hamid Reza Shahriari, and Seyed Mohammad Ghaffarian. 2015. Connection-monitor
Muhammet Baykara and Baran Sekin. 2018. A novel approach to ransomware: Designing a safe zone system. In 6th International Symposium on Digital Forensic and Security (ISDFS'18). IEEE, 1–5.

Nicoló Andronio, Stefano Zanero, and Federico Maggi. 2015. HelDroid: Dissecting and detecting mobile ransomware. In International Symposium on Recent Advances in Intrusion Detection. Springer, 382–404.

NO MÁS RANSOMWARE. [2021][ONLINE] [Consultado el 08 de diciembre] Disponibles en: https://www.nomoreransom.org/en/prevention-advice-for-businesses.html

OJEDA, J. E., RINCÓN, F., ARIAS, M. E., DAZA, L.A. "Delitos informáticos y entorno jurídico vigente en Colombia." [En línea]. 2010. [14 de noviembre de 2021} disponible en: (http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003).

Omar M. K. Alhawi, James Baldwin, and Ali Dehghantanha. 2018. Leveraging machine learning techniques for Windows ransomware network traffic detection. In Cyber Threat Intelligence. Springer, 93–106.

Pastor Franco, José, Sarasa López, Miguel Ángel, Salazar Riaño, José Luis, "Criptografía digital: fundamentos y aplicaciones", Ed. Prensas Universitarias de Zaragoza, 1998.

Porolli, M. (2021, junio 12). Operación Spalax: Ataques de malware dirigidos en Colombia. WeLiveSecurity. [Sitio Web] [Consultado 20 de mayo 2022] Disponible en: https://www.welivesecurity.com/la-es/2021/01/12/operacion-spalax-ataques-malware-dirigidos-colombia/

Programa CVE. [Consultado 08 de marzo 2022]. [ONLINE]. Disponible en: https://www.cve.org/About/Overview

Rakshit Agrawal, JackW. Stokes, Karthik Selvaraj, and Mady Marinescu. 2019. Attention in recurrent neural networks for ransomware detection. In IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'19).

Ransomware – Top 3 Vectores de Ataque 2021, [ONLINE]. 2021. Disponible en: https://m3security.mx/ransomware-top-3-vectores-de-ataque-2021/

RANSOMWARE [Sitio Web] [Consultado 14 de abril de 2022] Disponible en: https://latam.kaspersky.com/blog/el-ransomware-dirigido-a-empresas-aumenta-mas-de-un-200-en-latinoamerica/23784/#:~:text=Sin%20embargo%2C%20al%20comparar%20los,sanitaria%20%E2%80%93%20con%20una%20actividad%20m%C3%A1s

Ransomware [Sitio Web] [Consultado el 14 de abr. de 22] Disponible en: https://securelist.lat/ransomware-by-the-numbers-reassessing-the-threats-global-impact/93569

RANSOMWARE EN AMERICA [Sitio Web] [Consultado el 26 de mayo 2022] Disponible en: http://globalcyber.cl/

Seguridad Informática: virus ransomware, el Secuestro virtual de datos. Posible Medina Carranza, Facundo Martin. [Consultado 31 de marzo 2022]. [online]. Disponible en: https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/13925/MEDINA%20CARRANZA%20FACUNDO%20MARTIN.pdf?sequence=1&isAllowed=y

UNA MEDIDA DE LA INCERTIDUMBRE BASADA EN LA ENTROPÍA PARA CUANTIFICAR EL IMPACTO DE LA PÉRDIDA DE INFORMACIÓN DE LOS SISTEMAS DE GESTIÓN. [2021][online] Disponibles en: https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/4849/Schwarz_Diaz_Max.pdf?sequence=1&isAllowed=y

Victor Alvarez. 2014. YARA Rules. Disponible en: https://yara.readthedocs.io/en/latest/.
Zubaile Abdullah, Farah Waheeda Muhadi, Madihah Mohd Saudi, Isredza Rahmi A. Hamid, and Cik Feresa Mohd Foozy. 2020. Android ransomware detection based on dynamic obtained features. In International Conference on Soft Computing and Data Mining. Springer, 121–129.

(2019, febrero 18). APT-C-36: Continuous Attacks Targeting Colombian Government Institutions and Corporations. Centro de inteligencia de amenzas de Qi Anxin. [Sitio Web] [Consultado el 20 de mayo 2022] Disponible en: https://ti.qianxin.com/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government- institutions-and-corporations-en/