ANÁLISIS DE FENÓMENOS RANSOMWARE, SU AFECTACIÓN EN LA CIBERSEGURIDAD Y HERRAMIENTAS DE CONTRAATAQUE EN MIPYMES.

PROPUESTA DE MONOGRAFÍA COMO OPCIÓN DE GRADO

AUTOR:

KARINA MARCELA DIAZ RHENALS

TUTOR:

JORGE ELIÉCER GÓMEZ GÓMEZ, Ph.D.

UNIVERSIDAD DE CÓRDOBA

FACULTAD DE INGENIERÍA

DEPARTAMENTO DE INGENIERÍA DE SISTEMAS Y TELECOMUNICACIONES INGENIERÍA DE SISTEMAS

Octubre 2021

MONTERÍA

ANÁLISIS DE FENÓMENOS RANSOMWARE, SU AFECTACIÓN EN LA CIBERSEGURIDAD Y HERRAMIENTAS DE CONTRAATAQUE EN MIPYMES.

KARINA MARCELA DIAZ RHENALS

Trabajo de grado presentado, en la modalidad de Monografía, como parte de los requisitos para optar al Título de Ingeniería de Sistemas

Director (es):

JORGE ELIÉCER GÓMEZ GÓMEZ, Ph.D.

UNIVERSIDAD DE CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERIA DE SISTEMAS

MONTERIA- CORDOBA

Nota de aceptación

_____

_____

_____

_____

_____

Firma del jurado

_____

Firma del jurado

AGRADECIMIENTO

Primero quiero agradecer a Dios por cada bendición a lo largo de este tiempo, por enviarme muchos ángeles que aportaron apoyo de diversas maneras, a mis padres (DORIS Y ORLANDO) que han sido mi pilar para llegar a cumplir cada proyecto que quiero a lo largo de mi vida, las gracias me quedan cortas cuando recuerdo cada sacrificio hechos por ellos a lo largo de estos años, a cada profesor que enriqueció mi conocimiento y me ayudó a crecer de manera profesional, al profesor JORGE GÓMEZ, quien estuvo guiando mi trabajo de grado y quien me ayudo a creer más en mis capacidades, a mis hermanos (DANNY, KATIA, KEYLA y DAYNER) que me empujaron a seguir y me inspiraron, resaltando a mi hermano mayor (DANNYS)quien siempre creyó en mi, me regaló su apoyo en todo momento, me abrió las puertas de su casa junto a su familia y estuvo para guiarme en cada decisión, a mis amigas de toda la vida porque de una u otra manera estuvieron conmigo (Andrea, Marina, Melisa, Dayana) y a las que me regalo esta hermosa universidad, quienes se hicieron mi familia (Neris, Tania, Diego). Y a muchas personas que estuvieron conmigo, solo me resta decir gracias,

Contenido

INTRODUCCION

El mundo está en constante expansión tecnológica, cada día la infraestructura de los edificios soporta de mejor forma los grandes terremotos, la explotación minera se especializa en búsqueda de generar un menor impacto ambiental, el hombre observa los confines del universo, lo comprendiéndolo aún más y así una larga lista de mejoras y crecimiento constante en casi todas las áreas o campos.

El mundo de la informática es un campo que tiende a generar grandes avances en poco tiempo si se compara con otros y su avance también determina cómo evolucionan muchos campos relacionados, por ende actualmente es un pilar de la civilización humana muy importante. Esta rápida evolución también conlleva algunos riesgos debido a la dependencia que se genera en torno a esta hasta en las acciones más cotidianas que realiza el ser humano.

Internet es una herramienta llena de infinitas posibilidades para los cibernautas, desde la adquisición de conocimientos, hasta el generar un beneficio económico sólo a través de este, claro, no es algo que sea demasiado fácil, pero esto ha permitido que muchas personas puedan mejorar su calidad de vida sin salir de casa en muchos casos.

El gran océano de la web, es un lugar que se mueve gracias a la información, sin ella, no existiría. Teniendo en cuenta esto, se puede determinar que la información es un recurso muy importante y sobre todo valioso y no solo en términos coloquiales, sino en términos monetarios, debido a que esta permite generar más conocimientos o inclusive, conocer los patrones de comportamiento de una población dependiendo de su ubicación geográfica, sus gustos, actividades frecuentes, etc. Toda esa información es útil para generar anuncios enfocados en por ejemplo esa población en específico, así igualmente esa información puede ser utilizada para generar dinero de forma ilegal, como por ejemplo, obteniendo información de cuentas bancarias o de tarjetas de crédito o débito, por lo cual se evidencia que siendo un valioso recurso, la información

puede ser algo beneficioso o puede ser utilizado como arma o instrumento para lograr fines criminales.

En el ámbito de la web, desde casi sus inicios, la trasmisión de información ha sido utilizada para múltiples finalidades, aunque también para otras actividades, es por ello que nacen los virus (o una de las múltiples teorías de donde provienen).

En el constante tiempo de evolución de la internet y la tecnología en general (manteniendo una mayor dependencia), la importancia de la información en la web fue aumentando, tal así que luego de una larga lista de virus informáticos creados para dañar ordenadores o desestabilizar sistemas operativos, se dio lugar a virus para obtener datos sobre cualquier cosa del interés del atacante, esa nueva frontera, convirtió a estos programas maliciosos en herramientas para generar dinero de manera ilegal y prácticamente en el anonimato. Teniendo en cuenta esto, se pueden distinguir muchos tipos de virus o programas maliciosos enfocados en el mismo punto, pero existe un tipo en especial que desde hace unos pocos años hasta la actualidad ha concentrado casi toda la atención y son los ransomware, del cual existen muchas variedades, las cuales tienen como objetivo encriptar datos que puedan significar un valor económico para su dueño y así pedir un tipo de "rescate" por dicha información. El ransomware al ser una serie de instrucciones encaminadas en el robo o secuestro de la información, también tiene sus puntos que podría decirse débiles, en otras palabras, un "talón de Aquiles", respecto a las respectivas configuraciones de seguridad que se pueden realizar para que la información no esté demasiado expuesta, e inclusive para recuperar la información si esta ha sido destruida, por tanto, en este documento se abordará una investigación que genere como resultado una serie de normas, configuraciones y/o recomendaciones que permitan mitigar el robo de la información en pequeñas y medianas empresas.

DESCRIPCIÓN DEL PROBLEMA

El mundo gira entorno a la tecnología, esta se ha vuelto parte fundamental de la vida como se conoce hoy día, es por ello que existe una dependencia de estas en el sector empresarial donde se utilizan para realizar sus actividades principales de negocio en general de manera virtual a través de la red, esto ha conllevado a que la preocupación por la ciberseguridad sea aún más grande, con el fin de poder tomar las medidas necesarias y/o adecuadas para la protección de la información.

En términos informáticos, una vulnerabilidad es un fallo o una debilidad de un sistema, este presenta un riesgo para la seguridad del mismo y puede ser provocado por un error de configuración. El ciberatacante analiza dicha vulnerabilidad, con el fin de robar información de carácter sensible o de interrumpir el funcionamiento normal de un sistema. Estas vulnerabilidades, son la principal causa por la que una empresa llega a ser atacada, por tal motivo, se recomienda mantener actualizados los sistemas de protección, sistemas operativos y las aplicaciones utilizadas, debido a que esto minimiza (no quiere decir que estarán exentos de un ataque) la posibilidad de pérdida de datos puesto que una actualización, contiene correcciones basadas en la corrección de las vulnerabilidades descubiertas.

Existen vulnerabilidades en los sistemas que van ligados a factores antes mencionados como errores de configuración, errores en la gestión de recursos o errores de validación entre otros. Otro tipo de amenaza proviene del llamado ataque de denegación de servicio, lo que se conoce como ataque DDoS, el cual se produce cuando el servidor recibe demasiadas peticiones de acceso, el sistema se sobrecarga y esto provoca que el servidor funcione de forma incorrecta o definitivamente se cuelgue.

Todos los factores de vulnerabilidad mencionados, se utilizan con el único fin de robar y/o secuestrar información, debido a que esta es actualmente un "activo" valioso de cualquier empresa y de igual forma hace parte importante de cualquier usuario, ya que con esta se pueden definir muchas características del mismo en la red, es decir, perfilar a un usuario a través de la información robada. Existen varios tipos de amenazas informáticas, algunas de ellas hacen parte del espectro del malware, tales como los virus, gusanos, troyanos o el ransomware, el cual ha sido aprovechado por los ciberdelincuentes para realizar ataques a muchas empresas, centros de salud y organismos del estado.

El Ransomware es un Malware que restringe permisos, evitando que el usuario pueda ingresar al sistema operativo o navegador de un usuario hasta hacer pagar por un rescate moderado a través de mensajes de textos o transferencias electrónicas; estas actividades ilegales decaen cuando se empezó a regular los pagos electrónicos. A pesar de esto, a partir del 2015 la cantidad de ataques de ransomware se extiende a gran paso que según resultados de varios estudios y basado en las estadísticas de Kaspersky Security Network, en un año el número de ataques se quintuplicó de 131.111 intentos de infección entre 2014 y 2015 a 718.536 entre 2015 y 2016.

Este fenómeno ha afectado a muchas personas y empresas a nivel mundial dejando pérdidas en lo económico e informático, hay distintos tipos de Ransomwares y cada uno afecta de forma diferente a los dispositivos.

Aunque los países donde más se logra identificar ataques globales más activos están India, Vietnam, Argelia, Brasil, Rusia, Vietnam, Argelia, Brasil, Kazajistán, Italia, Alemania, Ucrania y Estados Unidos.

Colombia registra noticias de casos desde junio de 2017 donde doce (12) empresas fueron afectadas por el ciberataque mundial, tratándose de empresas de telecomunicaciones, un banco y empresas industriales. Durante todo el año, han sido

nuevamente descubiertas muchas amenazas que han causado graves problemas tanto a empresas como usuarios finales. Entre todas ellas, el ransomware ha vuelto a ser el tipo de amenaza más utilizada y el que ha llegado a infectar más ordenadores. A continuación, se conocerá el análisis de este fenómeno, partiendo desde su base: el malware, evolución del malware hasta llegar a lo que es ransomware, tipos de ransomware, etc.

Como casos relevantes se conoce lo sucedido en el Centro Cardio-Infantil del municipio de Lorica, donde se detectó un intento de ataque en el cual se vieron comprometidos 2 ordenadores de la red interna, que posteriormente fueron intervenidos para evitar la propagación del ransomware.

La ESE Camu Santa Teresita de Lorica, fue atacada y la información de las bases de datos fue "secuestrada" por piratas informáticos a través del virus de tipo ransomware conocido como "WannaCry", adicionalmente se pedía una suma monetaria como rescate en "Bitcoin" (cripto moneda de alta demanda) para que la información fuese liberada. El ataque se produjo el 16 de mayo del año 2017 y provocó de igual forma un colapso en algunos de los procedimientos internos de la entidad.

ÁREA DE TEMÁTICA

El área de la temática es Análisis de fenómenos RANSOMWARE en la Ciberseguridad: técnicas para análisis de datos, su afectación a los mismos y herramientas podemos tener a mano para contrarrestar estos ataques.

OBJETIVOS

OBJETIVO GENERAL

Analizar los efectos que producen el ransomware y su afectación directa en la ciberseguridad dentro de las mi pymes y recomendaciones para el uso de herramientas para posibles ataques y recuperación de información

OBJETIVOS ESPECÍFICOS

- Analizar los efectos producidos por los ransomware y cómo afecta la ciberseguridad en pequeñas y medianas empresas.
- Estudiar las estrategias para contrarrestar los ataques con Ransomware en pequeñas y medianas empresas.
- Recomendar alternativas de solución ante posibles ataques con Ransomware, que permitan mitigar la pérdida de información de las pequeñas y medianas empresas.

ALCANCE

El proyecto contemplado en esta investigación, de manera concreta lo que busca es estrategias, planes y metodologías, que estén relacionadas con el análisis de fenómenos y herramientas de ataque sobre Ransomware, que contribuyan al fortalecimiento de la ciberseguridad de la información, por lo cual se recurre a la exploración de estudios relacionados sobre el tráfico de datos y la forma de analizar los mismos y las defensas que alberga la red.

JUSTIFICACIÓN

Este trabajo se realiza con el objetivo de estudiar a fondo al Ransomware para aportar conocimiento sobre este virus de tipo malware que está en expansión y que va dirigido a atacar principalmente empresas y áreas gubernamentales, información importante. Buscando entender cómo se infiltra y burla las medidas de seguridad informáticas con que estos entes cuentan.

Teniendo en cuenta lo anterior, se evidencia la necesidad de realizar una identificación que permita evidenciar cual es el tipo de vulnerabilidad que se está usando con mayor frecuencia para realizar los ataques (es decir no se ataca al ransomware como el problema, sino a la vulnerabilidad que es la que permite que el virus cumpla su propósito), con ello, se puede crear una ruta a seguir que permita poder mitigar los efectos de un futuro ataque con este tipo de virus.

En primer lugar se deben recolectar datos sobre la seguridad en las empresas, esto con el fin de realizar una comparación que permita identificar en primera instancia cuales son las posibles vulnerabilidades que se pueden presentar de acuerdo a los datos obtenidos.

Es necesario tener en cuenta que la capacidad tecnológica de las pequeñas y medianas empresas puede variar dependiendo del tipo de sector comercial en el que se destaque dentro de la región. Algunos detalles adicionales como la utilización de tecnologías de protección de la información o apartados como la capacitación del personal que labora en dicha empresa, se deben tener en cuenta con el fin de poder trazar una ruta que permita demostrar la tendencia a ser vulnerables ante un ataque de tipo

ransomware. La intención es que las recomendaciones sean lo más certera posible y que permitan en la medida de lo posible cumplir con el objetivo de mitigar el problema que convierte a las pequeñas y medianas empresas de la región en objetivo para este tipo de ataques, verificando los posibles brechas en la seguridad, basándose en las formas más conocidas en las que se han realizado ataques a otras empresas anteriormente.

MARCO CONCEPTUAL

SEGURIDAD INFORMÁTICA

Tiene como objetivo en esencia salvaguardar la información y los sistemas de información de cualquier amenaza que busque manipular el acceso, uso, circulación y/o destrucción no autorizada de la información, utilizando modelos, técnicas, instrucciones, estrategias, recursos informáticos, recursos educativos y recursos humanos de manera conjunta para cumplir dicho objetivo.

El autor Álvaro Gómez en la Enciclopedia de la Seguridad Informática, define la seguridad informática como, “toda medida preventiva o restrictiva que evite en cualquier medida la ejecución de instrucciones no autorizadas que puedan inhabilitar el acceso de los usuarios, generar inestabilidad en el sistema o que comprometan la confidencialidad, integridad o autenticidad de la información dentro de un sistema o red”.

MALWARE

Malware es la forma corta de decir “malicious software”, este encierra todo tipo de código, aplicación o programa malicioso que busca atentar contra la estabilidad de un sistema para provocar un mal funcionamiento. Algunos de estos se les conoce como: Virus, Troyanos (Trojans), Gusanos (Worm), Botnets, Ransomwares, Spyware, Adware, Hijackers, Keyloggers, Fakeavs, Rootkits, Bootkits, Rogues, etc. [1]

La principal finalidad de un malware se centra en el robo o destrucción de información, principalmente son diseñados por ciberdelincuentes, de este modo pueden tomar control del sistema o alterarlo para sus propósitos particulares. [2]

VIRUS INFORMÁTICO

Un virus es una extensión de código generalmente malicioso, cuya finalidad es transmitir funciones que permitan al atacante ocasionar daños en un sistema, estos en algunos casos suelen ser irreparables, en algunos casos el usuario no logra percatarse de que está siendo atacado hasta que ya es demasiado tarde. [3] Un virus informático un fragmento de código que se carga en su equipo sin su conocimiento o permiso. [4]

GUSANO

Este hace referencia a un tipo especial de programa que logra copiarse a sí mismo muchísimas veces y en ubicaciones diferentes del disco duro o el medio de almacenamiento del sistema, por lo general su función es desestabilizar el sistema mediante la saturación del mismo, con ello logra que el usuario no pueda realizar sus labores. A diferencia de los virus, estos no infectan archivos. [5]

RANSOMWARE

El ransomware es un tipo de virus muy poderoso que le permite al atacante apoderarse de sistemas completos o de la información contenida en bases de datos de empresas, centros de salud, etc. Este por lo general se utiliza mediante la modalidad de la ingeniería social para su propagación exitosa y, una vez dentro, puede permitirle al ciberdelincuente “secuestrar” la información de la entidad y pedir un rescate por la misma con el agravante de eliminar la misma si el pago no se hace efectivo en el tiempo estipulado. [6] La información secuestrada pasa por un proceso de cifrado muy complicado en algunos casos (depende en gran medida de la habilidad del atacante), inclusive, pueden alterar archivos de forma irreversible. En el último tiempo, el ransomware ha cobrado una mayor relevancia en el panorama de la seguridad de la información y ha infectado tanto a usuarios como empresas [7]

¿COMO INFECTA UN RANSOMWARE? [7]

1. EXPLOTACIÓN DEL SISTEMA: Capacidad de propagación a través de unidades magnéticas, páginas web e inclusive a través del correo electrónico.
2. INSTALACIÓN: A través de archivos infectados a través del correo electrónico, programas “craqueados” o similares.
3. Identificación de archivos a cifrar
4. CIFRADO DE DATOS: Las ultimas variantes de Filecoder usan RSA de 2048 bits
5. NOTIFICACIÓN A USUARIO: Tácticas de ingeniería social para confundir a la víctima y que esta realice acciones que conlleven al despliegue del virus.

6. ESPERAR POR PAGO: Los métodos aceptados van desde tarjetas prepagadas hasta bitcoins o cupones de MoneyPak, Ukash y cashU para otorgar anonimato.
7. ENTREGA DE LAS CLAVES DE DESCIFRADO: NADA asegura que el atacante devuelva el control del equipo infectado. [7]

PROTOCOLOS DE PROPAGACIÓN DE RANSOMWARE

DNS: Los cuentagotas de ransomware modernos utilizan el sistema de nombres de dominio para resolver los nombres de dominio que el atacante informático cambia con frecuencia, ocultándose así de los investigadores. [8]

HTTP y HTTPS: La mayoría de los ransomware se aprovechan de puertos comunes como el 80 y el 443, utilizados por los protocolos HTTP y HTTPS de manera que se aseguran tener una forma de conectarse a los ordenadores de las víctimas. [9]

RDP: The Remote Desktop Protocol proporciona visualización remota y capacidades de entrada sobre conexiones de red para aplicaciones basadas en Windows que se ejecutan en un servidor. [10] El ransomware de igual forma puede ser implantado a través de los famosos ataques DOS o de fuerza bruta a servicios de Escritorio remoto (RDP - Remote Desktop Protocol) expuestos. [11]

SMB: (Server Message Block), es un protocolo de uso compartido de archivos de red que permite que las aplicaciones de un equipo puedan leer y escribir archivos y solicitar servicios desde los programas de un servidor en una red de equipos. El protocolo SMB puede usarse sobre el protocolo TCP/IP u otros protocolos de red. Con el uso de un protocolo SMB, una aplicación (o el usuario de una aplicación) puede acceder a los archivos u otros recursos de un servidor remoto. Esto permite que las aplicaciones puedan leer, crear y actualizar archivos en un servidor remoto. [12]

ALGORITMOS QUE UTILIZA UN RANSOMWARE

ALGORITMO RSA: El algoritmo de clave pública RSA fue creado en 1978 por Rivest, Shamir y Adlman, y es el sistema criptográfico asimétrico más conocido y usado. Es el algoritmo de cifrado comúnmente utilizado por los Ransomwares para cifrar archivos. [13]

ALGORITMO RIJNDAEL: El algoritmo Rijndael permite una variedad de tamaños de bloque y clave y no solo los 64 y 56 bits del bloque DES y el tamaño de clave. De hecho, el bloque y la clave pueden ser elegidos independientemente si son de 128, 160, 192, 224, 256 bits y no es necesario que sean de igual tamaño. Sin embargo, el estándar AES establece que el algoritmo solo puede aceptar un tamaño de bloque de 128 bits y una elección de tres claves: 128, 192, 256 bits. [14]

TIPOS DE RANSOMWARE [15]

1. Ransomware Cifra archivos
    - CryptoLocker
    - CTB-Locker
    - TorrentLocker
    - CryptoMix
    - Mamba
    - Chimera
2. Ransomware Pantalla de Bloqueo
    - Reventon
    - CTB Locker
    - WannaCryptor
    - WinLock
3. Ransomware de Dispositivos Móviles
    - Simplocker
    - WireLurker

APATEDNS: Es una herramienta para controlar las respuestas DNS a través de una GUI fácil de usar. Como un servidor DNS falso, ApateDNS engaña las respuestas de DNS a una dirección IP especificada por el usuario escuchando en el puerto UDP 53 en la máquina local. ApateDNS también establece automáticamente el DNS local en localhost. Al salir de la herramienta, restablece la configuración DNS local original**.** [16]

FAKENET: FakeNet-NG esta herramienta permite realizar análisis de red dinámica de próxima generación, está enfocada para analistas de malware y probadores de penetración. Es de código abierto y puede desplegarse en las últimas versiones de

Windows y Linux (Linux tiene algunas restricciones). FakeNet-NG se basa en la herramienta FakeNet desarrollada por Andrew Honig y Michael Sikorski.

La herramienta le permite interceptar y redirigir todo o tráfico de red específico mientras simula servicios de red legítimos. Al utilizar FakeNet-NG, los analistas de malware pueden identificar rápidamente la funcionalidad del malware y capturar firmas de red. Los probadores de penetración y los cazadores de errores encontrarán que el motor de interceptación configurable y el marco modular de FakeNet-NG son muy útiles al probar la funcionalidad específica de la aplicación y crear prototipos de PoC. [17]

DEPENDENCY WALKER: Dependency Walker permite realizar un escaneo a los módulos de Windows en sus versiones de 32 y 64 bits, de igual modo, permite crear un árbol jerárquico de todos los módulos dependientes. Enumera módulo a módulo las funciones que exporta dicho módulo y también cuales de estas están siendo llamadas por otros módulos, también logra reunir información detallada de cada archivo mínimo necesario y la ruta completa, dirección base, números de versión tipo de máquina, información de depuración y más. [18]

PESTUDIO: PeStudio es una asombrosa herramienta de análisis de superficies todo en uno para portable ejecutables, esta aplicación contiene una base de datos de virus que utiliza VirusTotal para realizar sus análisis. PeStudio es una aplicación de Windows. [19]

ESTADO DEL ARTE

EVOLUCION DEL MALWARE

Teniendo en cuenta la teoría de Von Neumann (1949) y del juego que diez años después desarrollaron Robert Morris, Douglas McIlroy y Víctor Vysottsky el cual fue el precursor de la creación de los primeros virus informáticos y de la primera aparición del virus Brain en 1986, cada año es característico con la aparición de una amenaza, y tomando como base el documento una noticia publicada por Sabrina Pagnotta en la comunidad de seguridad de ESET, los siguientes son las amenazas características de cada año:

Para el año de1949, "*Von Neumann estableció la idea de programa almacenado y expuso La Teoría y Organización de Autómatas Complejos, donde presentaba por primera vez la posibilidad de desarrollar pequeños programas replicantes y capaces de tomar el control de otros programas de similar estructura. Si bien el concepto tiene miles de aplicaciones en la ciencia, es fácil apreciar una aplicación negativa de la teoría expuesta por Von Neumann: los virus informáticos, programas que se reproducen a sí mismos el mayor número de veces posible y aumentan su población de forma exponencial*". [20]

En el año 1959, *"Robert Thomas Morris, Douglas Mcllroy y Victor Vysottsky crean un juego denominado CoreWar basado en la teoría de Von Neumann y en el que el objetivo es que programas combatan entre sí tratando de ocupar toda la memoria de la máquina eliminando así a los oponentes. Este juego es considerado el precursor de los virus informáticos".* [20]

Robert T. Morris crea el Creeper en el año 1972, este es considerado como el primer virus reconocido en la historia, este era capaz de infectar las máquinas de IBM 360 en

la ARPANET (predecesora de internet). Este presentaba un mensaje al usuario que decía: “Soy una enredadera, atrápame si puedes”. Para eliminarlo, se creó otro virus llamado Reaper que estaba programado para buscarlo y eliminarlo.

Pakistani Brain, fue el primer virus para plataformas IBM PC y el primero en utilizar mecanismos de ocultamiento al año 1986. [21]

El virus Stoned, se conoció como el primero de su clase al atacar el sector de arranque. Algunos de los mensajes precargados eran alusivos al uso de drogas, este virus fue muy común a inicio de los 90’s. [21]

Robert T. Morris Jr para el año de1988, desarrolló el primer gusano de la historia, este fue capaz de propagarse en miles de computadores y estacones de trabajo con VMS (Virtual Memory System), BSD (Berkeley Software Distribution) y SunOS. [21]

En el año1989, Disk Killer o Computer Ogre, uno de los primeros virus destructivos, infecta el sector de arranque, el disco se va dañando lentamente.

En el año 1989 se conoce el primer caso de ransomware, con la llegada del virus troyano PC Cyborg, este reemplazaba el archivo AUTOEXEC.BAT, lo cual le permitía ocultar los archivos de la unidad primaria del disco, logrando que el sistema quedase inutilizable. Para poder quitar el cifrado al usuario se le pedía “renovar su licencia” con un pago de 189 dólares a PC Cyborg Corporation. [22] El cifrado de este troyano resultó ser débil dado que utilizaba un cifrado monoalfabético.

Whale en el año de 1990, fue el pionero en tecnología anti-debugging, los creadores de malware aprendieron mucho de este llamado virus ineficiente.

Michelangelo, más trascendente por el pánico mediático desencadenado a medida que se acercaba su época de activación, el 6 de marzo, esta variante de Stoned infectaba al sector de arranque de los disquetes floppy y al sector Mbr de los discos duros. Como

permanecía la mayor parte de periodo latente, podía sobrevenir años sin ser descubierto si no se reiniciaba el dispositivo el 6 de marzo en el año de 1991.

Para el año de 1994, OneHalf, el primer virus tipo ransomware, a diferencia del actual este no pedía rescate ni tampoco había un código de desactivación. Cifraba la primera serie de sectores del disco rígido; si se usaba FDISK/MBR, el sector MBR infectado se reemplazaba por uno vacío y el sistema ya no era capaz de arrancar.

WM/Concept fue el primer macro virus que utilizó Microsoft Word como medio de propagación en el año1995.

Larouxen fue el primer macro virus propagado a través de Excel, este lograba propagarse entre los dispositivos infectados sin control en el año de 1996. Se utilizaron macros para su realización tales como “Auto_Open” y “Check_Files” ocultas en una hoja de cálculo llamada “laroux”.

AOL Trojans, se empieza a utilizar a los troyanos como nuevo método para infectar equipos, este tipo de virus robaba las credenciales AOL, esto adoptó diferentes formas y a partir de allí tuvo lugar el phishing un fenómeno que ha sido base para la creación de nuevos malwares en el año de 1997.

Para el año de1998, Autostart, era más conocido como un gusano debido a su comportamiento de replicarse sobre algún programa host.

En el año de1999, Melissa, fue un gusano el cual enviaba correos electrónicos a través del cliente MS Outlook, infectaba las redes de Microsoft e Intel. El virus atacaba a través de un archivo adjunto MS Word y se reenviaba a los primeros 50 contactos de Outlook a partir de que el usuario hacía clic sobre él.

LoveLetter o ILOVEYOU en el año 2000, conocido como el virus del amor, este afectó muchos usuarios del sistema operativo Windows, llegaba al correo haciéndose

pasar por una supuesta carta de amor y era capaz de acceder al sistema operativo, al almacenamiento secundario, al sistema y a los datos de usuario de la víctima.

Para el año de 2001, Nimda, es un gusano que se caracteriza por usar varios métodos de ataque, entre los que se encuentran: correo electrónico, recursos compartidos de red abiertos y sitios comprometidos.

2002

KLEZ, en el año de 2002, era un gusano para el envío intensivo de correos electrónicos que se propagaba como un virus polimórfico. Una vez el dispositivo se infecta éste se enviaba a sí mismo a las direcciones de mensajería encontradas en el sistema, de igual forma utilizaba falsificación de remitente, es decir, sustituía la dirección de origen por una aleatoria pero existente.

SQL Slammer, fue un gusano que aprovechó una vulnerabilidad en Microsoft SQL Server, básicamente este gusano era un paquete de red que se propagó de forma rápida infectando a la mayoría de víctimas en diez minutos en el año 2003.

Después en 2004, MYDOOM, un gusano que se caracterizaba por realizar ataques DoS, el grupo SCO y Microsoft fueron los principales afectados, además como muchos este también hacia envío masivo de correos electrónicos lo que permitió su rápida propagación.

Para el año de 2005, Commwarrior, fue el primer virus que atacó la telefonía móvil, era capaz de propagarse vía mensajes MMS y Bluetooth. Atacó la línea de smartphones Symbian Series 60.

En el año de 2006, VB.NEI, también conocido como Nyxem, Blackmal o Mywife, utilizaba un contador que permitía rastrear la cantidad de host infectados, además borraba archivos de forma aleatoria.

En ese mismo año se lanzó WINLOCK ransomware para usuarios de PC. WinLock muestra imágenes pornográficas hasta que las víctimas envían un SMS de tarifa premium de 10 dólares para recibir un código de desbloqueo. [23]

El ransomware GPCODE se lanzó en junio de ese mismo año infectando PC a través de fraudes de spear phishing. El GPCode se extendió a través de archivos adjuntos de correo electrónico que parecían ser una aplicación de trabajo. [24]

ARCHIVEUS TROJAN fue uno de los primeros virus ransomware creados. Archiveus se desató en el mundo en 2006, afectando principalmente a los usuarios de PC. Además, Archiveus Trojan fue el primer hechizo ransomware en utilizar el cifrado RSA. El cifrado RSA es un criptosistema de clave pública y se usa ampliamente para la transmisión segura de datos y es extremadamente difícil de descodificar. Para descifrar o desbloquear un archivo encriptado RSA se necesita una cadena alfanumérica específica de dígitos. Archiveus Trojan cifró todo en el directorio Mis Documentos y exigió a las víctimas que compren artículos de una farmacia en línea para recibir la contraseña de 30 dígitos o el código de clave para desbloquear sus archivos. [25]

Para el año 2007, STORM detectado por ESET como Nuwar propagándose a través de correos electrónicos en Europa y Estados Unidos, luego se detectó en correos falsos con temas de Saddam Hussein a Fidel Castro. Los equipos infectados se convertían en parte de una botnet.

En el año 2008 GPCODE.AK una variante del GPCode se desató y comenzó a propagarse de PC a PC. Cada computadora infectada con GPCode.AK, bloquearía o encriptaría los archivos de la víctima y requeriría que el usuario pague un rescate o una tarifa para obtener un código que desbloquee sus archivos. La diferencia entre el primer GPCode y GPCode.AK fue el uso de una clave RSA de 1024 bits utilizada para

bloquear o encriptar los archivos de la víctima, lo que hizo que esta versión fuese más molesta y más difícil de descifrar. [26]

CONFICKER en el año 2008 botnet se propagó tanto que atrajo la atención de los medios, aun así, su uso de algoritmos variables para impedir su rastreo fue un indicador para desarrollos futuros.

En el año 2009, TDL3 rootkit innovador y adaptable dando nuevos giros a antiguas ideas como las redes P2P y otros códigos maliciosos aprovechando sectores marcados como defectuosos, utilizando efectivamente los archivos ocultos del sistema.

STUXNET el primer gusano de uso militar que llegó a las noticias, atacaba los sistemas de control industrial y se utilizó contra instalaciones nucleares iraníes en el año 2010.

A mediados de 2011, el primer brote de ransomware a gran escala, y el ransomware se mueve a la gran altura debido al uso de servicios de pago anónimos, lo que hizo que a los autores les resultara mucho más fácil recolectar dinero de sus víctimas. Se detectaron alrededor de 30,000 nuevas muestras en cada uno de los primeros dos trimestres de 2011. [27]

Durante el tercer trimestre de 2011, las nuevas detecciones de ransomware se duplicaron a 60,000. [27]

HELIHOS en el año 2011 un probable sucesor del gusano Storm utilizado para llevar a cabo campañas de SPAM y robar información.

En enero de 2012 el entorno del cibercrimen alcanza la madurez con CITADEL, un conjunto de herramientas para distribuir malware y administrar botnets que apareció por primera vez en enero de 2012. Citadel hace simple la producción de ransomware e infecta sistemas al por mayor con programas de pago por instalación que permiten a los ciberdelincuentes pagar una tarifa mínima para instalar sus virus ransomware en

computadoras que ya están infectadas por otro malware. Debido a la introducción de Citadel, las infecciones totales superaron las 100.000 en el primer trimestre de 2012. [28]

En marzo de ese mismo año, Citadel y Lyposit conllevan al gusano REVETON, un intento de obtener dinero a través de una multa fraudulenta. Reveton apareció por primera vez en los países europeos a principios de 2012. El "delito" y la "agencia de cumplimiento de la ley" exacto se adaptan a la ubicación del usuario. Las amenazas son "software pirateado" o "pornografía infantil". [27]

Entre abril y julio de 2012, se empiezan infectar usuarios con el URAUSY POLICE Ransomware, este ransomware es responsable de las estafas que se extendieron por toda América. Cabe resaltar que las detecciones de ransomware aumentaron a mas de 200.000 y habían más de 2000 víctimas por día. [27]

En noviembre de 2012, se lanza otra versión de REVENTON en está ocasión haciéndose pasar por el Centro de Quejas contra el Cibercrimen del FBI (IC3). [27]

Para el año 2013 HESPERBOT troyano que atacó usuarios bancarios imitando organizaciones confiables obteniendo credenciales de inicios de sesión.

En julio de 2013 la empresa de seguridad informática Kaspersky descubre el troyano SVPENG el cual infecta a dispositivos Android. Originalmente fue creado para robar información de tarjetas de los clientes del banco ruso. Para comienzos de 2014 se le empezó a reconocer como un ransomware, bloqueando los teléfonos celulares desplegando un mensaje acusando al usuario de acceder a pornografía infantil. [27]

En septiembre de 2013, es lanzado el CRYPTOLOCKER, el primer malware criptográfico que se propaga a través de descargas provenientes de sitios comprometedores (software pirata, banners, etc.) y/o que son enviados a empresas,

negocios, entre otros, mediante correos electrónicos haciéndose pasar por algún proveedor de servicios de software. [27]

En noviembre de 2013 hay cambios en el rescate. El pago por el rescate en ese momento es de 2 Bitcoins o alrededor de 460 dólares, si no cumplían con el plazo del rescate original, debían pagar 10 Bitcoins (2300 dólares aproximadamente) para usar un servicio que se conectaba a los servidores de comando y control. Después de pagar por ese servicio, los primeros 1024 bytes de un archivo cifrado se cargarían en el servidor y el servidor buscaría la clave privada asociada. [27]

A principios de diciembre de 2013 se llegó a 250.000 máquinas infectadas. Cuatro cuentas de Bitcoin asociadas con CryptoLocker descubrieron que 41,928 Bitcoins se movieron a través de esas cuatro cuentas entre el 15 de octubre y el 18 de diciembre. Dado el precio actual de 661 dólares, eso representaría más de $ 27 millones en pagos recibidos, sin contar todos los demás métodos de pago. [27]

A finales de diciembre de 2013 se conoce el CryptoLocker 2.0, a pesar del nombre similar, CryptoLocker 2.0 se desarrolló en C#, mientras que el original estaba en C ++, por lo que probablemente lo hizo un equipo de programación diferente. Entre otras diferencias, el 2.0 solo aceptaría Bitcoins y encriptaría archivos de imágenes, música y video que el original omitió. Y, aunque decía usar RSA-4096, realmente usaba RSA-1024. Sin embargo, los métodos de infección fueron los mismos y la imagen de la pantalla muy similar a la original. [27]

También durante este período de tiempo, CryptorBit salió a la luz. A diferencia de CryptoLocker y CryptoDefense, que solo se enfoca en extensiones específicas de archivos, CryptorBit corrompe los primeros 212 o 1024 bytes de cualquier archivo de datos que encuentre [27]

En 2014, WINDIGO tomó el control de más de 25.000 servidores Unix en todo el mundo y envío millones de mensajes spam diarios, se diseñó para secuestrar servidores, infectar equipos que luego los visitaban a robar información.

A partir de mayo de ese mismo año, varios usuarios de dispositivos Apple en Australia y EE. UU., Así como algunos de EE. UU. Y Nueva Zelanda, se han tropezado con algunos problemas cuando sus dispositivos se bloquearon inesperadamente y se guardaron para pedir un rescate. Estas víctimas encontraron una pantalla de bloqueo inusual en sus dispositivos que les informó que alguien llamado "Oleg Pliss" había bloqueado sus dispositivos. Según el mensaje, Oleg Pliss exigió un pago de entre $ 50 y $ 100 (o de 50 a 100 euros) a través de PayPal, MoneyPak o Ukash para que el dispositivo se desbloquee. [27]

A mediados del 2014 alrededor de 900.000 celulares fueron infectados por el ransomware SVPENG. [27]

Finales de 2014, se propaga el TorrentLocker: según iSight Partners, TorrentLocker "utiliza componentes de CryptoLocker y CryptoWall, pero con un código completamente diferente de estas otras dos familias de ransomware". Se propaga a través del correo no deseado y utiliza el algoritmo Rijndael para el cifrado de archivos en lugar de RSA-2048. el rescate se paga mediante la compra de Bitcoins de sitios web específicos de Bitcoin de Australia. [27]

A principios de 2015, CryptoWall despega y reemplaza a CryptoLocker como la principal infección de ransomware.

Abril de 2015: CryptoLocker ahora está siendo localizado para países asiáticos. Hay ataques en Corea, Malasia y Japón. [27]

Mayo de 2015 nace el ransomware como servicio. En resumen, se podía ir a este sitio web de TOR "para criminales por criminales", lanzar su propio ransomware de forma

gratuita, y el sitio recibía un 20% de comisión de cada pago de rescate de Bitcoin. También en mayo de 2015 aparece una nueva versión que se llama Locker y ha estado infectando las estaciones de trabajo de los empleados, pero permaneció allí silenciosamente hasta la medianoche del 25 de mayo de 2015 cuando se despertó. Locker comenzó a causar estragos de manera masiva. [27]

BLACKENERGY es un troyano usado para ejecutar tareas específicas como ciber espionaje con D DoS, ataques de destrucción y daño a mercados de energía, muestra señales de habilidades por encima de administradores de botnets D DoS tradicionales, en el año 2015.

En junio de 2015 el foro SANS InfoSec señala que una nueva versión de CryptoWall 3.0 está en rondando, utilizando currículos de mujeres jóvenes como señuelo de la ingeniería social: "reanudar el ransomware". A su vez el FBI, a través de su Internet Crime Complaint Center (IC3), emitió una alerta el 23 de junio de 2015 que, entre abril de 2014 y junio de 2015, el IC3 recibió 992 quejas relacionadas con CryptoWall, y las víctimas informaron pérdidas por un total de más de $ 18 millones. Ransomware les da a los cibercriminales casi un 1.500% del dinero de sus victimas. [27]

En julio de 2015, el investigador de seguridad Fedor Sinitsyn informó sobre el nuevo TESLACRYPT V2.0. Esta familia de ransomware es relativamente nueva, se detectó por primera vez en febrero de 2015. Se ha denominado la "maldición" de los jugadores de computadora porque se dirige a muchos tipos de archivos relacionados con juegos.

En septiembre de 2015, una agresiva variedad de ransomware de Android se está extendiendo en Estados Unidos. Los investigadores de seguridad de ESET descubrieron el primer ejemplo real de malware capaz de restablecer el PIN de su teléfono para bloquearlo permanentemente en su propio dispositivo. Lo llamaron LOCKERPIN, y cambia el código PIN de la pantalla de bloqueo del dispositivo

infectado y deja a las víctimas con una pantalla móvil bloqueada, exigiendo un rescate de $ 500. [27]

Para febrero del año 2016 aparece LOCKY, es un ransomware es un método popular de atacantes para buscar dinero, recibiendo ese nombre del Dios nórdico embaucador Loki y capaz de cifrar archivos en unidades de red, fijas y removibles, para descifrar los archivos el usuario debe aceptar ciertas condiciones a cambio de instrucciones o una contraseña.

En abril 2016 aparecen nuevos casos de ransomware, uno de los casos se presenta debido al ransomware CRYPTOHOST, este ransomware tiene la particularidad de que hace creer a la victima que sus archivos están encriptados y por eso pide un rescate, pero en realidad lo que hace es comprimirlos en un archivo RAR protegido con contraseña. También se conoció el caso del ransomware JIGSAW, su nombre se proviene del personaje de la saga de películas El Juego del Miedo, éste ransomware actuaba cifrando los archivos de las víctimas, colocando el papel tapiz con la imagen del personaje y mostraba un mensaje a sus víctimas diciendo que quería jugar un juego, sus archivos estaban encriptados y si no hacia el pago por el rescate en la primera hora un archivo sería borrado, pasado el día cien archivos y así sucesivamente, si el usuario intentaba apagar el equipo o quitar el ransomware como castigo borraba mil archivos.

En mayo de 2017 aparece una variante del ransomware NotPetya llamado WANNACRY consiguió atacar en países como España, Francia, Ucrania, Rusia y muchos otros países éste ransomware cifra los archivos de la víctima y pide un pago por el rescate dicho pago se realiza en Bitcoins, este fue uno de los mayores ciberataques vistos en 2017 ya que logró paralizar al servicio nacional de salud de Reino Unido, y a compañías como Telefónica, FedEx o Deutsche Bahn.

BAD RABBIT apareció por primera vez en octubre de 2017 y está dirigido a organizaciones en Rusia, Ucrania y los EE. UU. Con un ataque que básicamente era

nuevo y mejorado NotPetya ransomware. Las autoridades ucranianas atribuyen Bad Rabbit a Black Energy, el grupo de amenazas que también creen que estaba detrás de NotPetya. Muchos expertos en seguridad creen que Black Energy opera en interés y bajo la dirección del gobierno ruso. El ataque no duró mucho tiempo, lo que indica que los controladores lo cerraron ellos mismos. El ataque comenzó a través de archivos en sitios web de medios rusos pirateados, utilizando el popular truco de ingeniería social de pretender ser un instalador de Adobe Flash. El ransomware exige un pago de 0,05 bitcoins, o alrededor de 275 dólares, dando a las víctimas 40 horas para pagar antes de que aumente el rescate.

En febrero de 2018, se descubrió una nueva variante llamada Annabelle, que parece haber sido diseñada para "mostrar las habilidades" del desarrollador que la creó, al ser tan difícil de tratar como sea posible. Finaliza numerosos programas de seguridad, deshabilita Windows Defender, desactiva el firewall, cifra archivos, intenta propagarse a través de unidades USB, por lo que no puede ejecutar una variedad de programas y sobrescribe el registro de inicio maestro de la computadora infectada con un cargador de arranque, es decir, cuando inicie el sistema operativo cargue el ransomware. [27]

A mediados de marzo de 2018 se conoce un nuevo ransomware como servicio llamado GANDCRAB. Este es el ransomware más prominente de 2018, infectando aproximadamente 50,000 computadoras, la mayoría de ellas en Europa, en menos de un mes pidiendo a cada víctima rescates entre 400 y 700,000 dólares en criptomoneda DASH. Yaniv Balmas, un investigador de seguridad de Check Point, compara a GandCrab con la notoria familia Cerber, y el experto también agregó que los autores de GandCrab están adoptando un enfoque ágil de desarrollo de software, la primera vez en la historia del ransomware. [27]

METODOLOGÍA

Para la realización de este proyecto se llevó a cabo tres tipos de investigación (la exploratoria y la descriptiva) es exploratoria ya que se hizo una recolección de información sobre el tema abordado para la realización de este proyecto, y la descriptiva porque permite describir de forma global la situación presentada por los Ransomware y sus posibles causas.

Se tendrá en cuenta para el desarrollo metodológico del trabajo la obtención de material bibliográfico referente al tema en cuestión, teniendo en cuenta el contexto, de este modo también se tendrá en cuenta las experiencias y o datos que se recopilen sobre casos de ataques que puedan relacionarse a la región, esto serviría para poder realizar una comparación que posibilite la creación de la ruta de sugerencias de seguridad que se planea con base en la recopilación y análisis de los datos.

El proceso de creación de la ruta de sugerencias dispondrá de las siguientes fases:

Fase I: Se centrará en la recopilación de la información que concierne a los ataques a empresas, es decir la información con base en la experiencia en cuanto a ataques a otras empresas y las vulnerabilidades reportadas (esto con el fin de enriquecer la siguiente fase), cabe aclarar que se iniciará centrado en los puntos clave o vías de ataque de acuerdo al tipo de ransomware, etc.

Fase II: Se realizará un análisis que permita poder encontrar dichas vulnerabilidades en la seguridad de las empresas, esto con el fin de generar indicadores que permitan contrarrestar las mismas.

Fase III: Se diseñará a partir de los conocimientos generados en las fases uno y dos, la ruta que permita a las empresas poder mitigar el riesgo de ser atacadas a través del ransomware.

DESARROLLO

Las fases desglosadas a continuación buscan resolver algunos interrogantes importantes que se plantean a la hora de generar un documento, recomendaciones o ruta de acción de acuerdo a las medidas que se deben tomar para evitar y/o mitigar los ataques de ransomware en pequeñas y medianas empresas, por lo tanto, es necesario que se verifique en cierta medida cómo están protegidas dichas empresas en materia de seguridad informática y/o protección de datos, para resolver los interrogantes y completar los objetivos, se ha desarrollado una serie de fases que permitirán manipular de manera óptima la información, con el fin de generar los resultados esperados.

Fase I:

RANSOMWARE Y POSIBLES VÍAS VULNERABLES

Uno de los puntos más vulnerables a la hora de hablar de ciberseguridad, se le conoce como "ingeniería social", esta es un practica que en esencia busca que la víctima se sienta en total confianza con los contenidos enviados a través de correo electrónico, esto con el fin de que este ingrese a los links o descargue los archivos adjuntos, regularmente este proceso contiene de forma no autorizada, material de tipo bancario (lo cual es un indicador de que algunas víctimas son elegidas luego de un pequeño estudio), gubernamental o similares, algunos bastante creíbles a tal punto de emular de manera casi precisa los correos, páginas web y demás herramientas usadas por dichas entidades, esto logra que la víctima baje la guardia y en esencia permite que el atacante logre su cometido. Ya sea robar información para cometer fraude o con el fin de pedir rescate por la misma.

En el caso de las pequeñas y medianas empresas, la forma habitual de "infectar" los servidores es la del envío de archivos adjuntos a la oficina de recursos humanos debido a una

vacante, pero en realidad o que sucede es totalmente distinto al proceso, esta área es fundamentalmente vulnerable por este tipo de acciones, podría decirse que es la zona con mayor porcentaje de vulnerabilidad, debido al manejo constante de información adjunta en entrada y salida constante; un ejemplo claro se da debido a que Windows de forma predeterminada oculta las extensiones de los archivos, por lo tanto un archivo con nombre y extensión "hoja_de_vida.pdf.exe", puede fácilmente camuflarse y ser ejecutado, debido a que el usuario sólo podrá ver el nombre del archivo (el cual sería hoja_de_vida.pdf) y de esta forma se desencadenaría la ejecución del mismo, el cual puede secuestrar la información (encriptación) y pedir una suma para liberarla nuevamente (por lo general en Bitcoin); cabe aclarar que en la totalidad de ataques, se estima un conteo regresivo para la entrega del rescate (por lo general un plazo no mayor a 5 días), amenazando con destruir la información de acabarse el conteo.

Fig. 1. Cryptolocker exigiendo el pago por el rescate de la información [30]

Otro tipo de vulnerabilidades se evidencia cuando se le brinda acceso al sistema a consultores externos (con el fin de implementar mejoras de negocio, para alcance, etc.), estos accesos son vulnerabilidades en potencia que se pueden dar si por ejemplo el dispositivo desde el que se accede está infectado.

Una vulnerabilidad muy particular se evidencia en el hecho del desconocimiento por parte del personal que mantienen contacto estrecho con sistemas informáticos, es que algunas opciones pueden no ser lo que parecen, tal es el caso de los documentos que "no se visualizan de manera correcta", los cuales piden al usuario activar ciertas opciones como "macros", para poder visualizar el contenido del documento, esto el usuario lo toma como una medida necesaria y segura, debido a que está utilizando software licenciado y seguro para la

visualización de los documentos, he ahí el principal problema por el cual "Locky" se ha convertido en la pesadilla de los hospitales y/o centros de salud, este se aprovecha de cada vulnerabilidad que pueda provenir del usuario y en realidad usa los programas "seguros" como pequeños señuelos para ejecutar instrucciones sin que el usuario se percate, esto le permite alojar de forma local y posiblemente dentro de la red interconectada para servicios del centro de salud, un archivo que encripta la red, esté mapeada o no, convirtiendo a este virus en un arma poderosa.

Como se puede evidenciar, el ransomware utiliza los vectores de infección más comunes (es muy similar en dicho sentido a un troyano o virus común), este se acopla a lo que se conoce como ingeniería social, a través de la cual el ciberdelincuente logra engañar a un usuario para que este intervenga sin saberlo de forma que el virus se propague satisfactoriamente. Otros vectores de infección comunes son:

E-mails maliciosos

Actualmente de los más usados por su probabilidad de éxito para infectar, como se expuso anteriormente, la ingeniería social es una herramienta que usada de forma correcta, permite hacer grandes cosas o en el tema en cuestión hace mucho más peligroso al ransomware, permitiéndole al atacante poder suplantar entidades oficiales de cualquier índole y obtener datos de la víctima sin mayor esfuerzo.

Webs infectadas

Iniciando por la descarga de archivos maliciosos a través de un payload, hasta la utilización de un exploit kit, que permite encontrar vulnerabilidades en el sistema que permitan la instalación del ransomware, este es otro vector de infección muy utilizado por la facilidad con la que puede lograrse que el usuario acceda a dichos sitios, haciéndose pasar por páginas de contenidos deportivos, educacionales, etc, esto con el único fin de lograr la infección del equipo y robar datos.

Dispositivos extraíbles

Utilizado desde hace mucho tiempo para infectar sistemas, la forma de propagación más rápida conocida antes de que la web se volviera popular. Los medios extraíbles eran la forma más rápida y efectiva de infectar equipos, debido a que poca importancia se le brindaba a su seguridad, esto permitía que en archivos simples como presentaciones de power point, se pudiese transmitir un virus de forma sencilla, aprovechando la reproducción automática de dispositivos de Windows.

Un caso muy particular del que se habla por la web (más exactamente en reddit), dice que un ciberdelincuente intentaba apoderarse de información de una determinada empresa, para lo cual agotó todos los vectores de infección disponibles para lograr su cometido, pero este omitió el uso de dispositivos extraíbles, por alguna razón desconocida. Al percatarse de esto, ideó un nuevo plan para poder lograr su propósito, este fue infectar una cantidad considerable de memorias USB y ubicarlas en la recepción de la empresa víctima, básicamente como una "muestra gratis", es decir utilizó la ingeniería social, para convencer a las personas de tomar una debido a que era un regalo y bueno, completó dicho propósito de la manera menos esperada.

Modelo de negocios

Aquí básicamente se convierte en un negocio lucrativo el infectar las redes y secuestrar los datos de entidades de cualquier índole, con el fin de obtener una remuneración económica, esta es la esencia actual de los ataques con ransomware, debido a que representan un beneficio muy grande a costos relativamente bajos, debido a que principalmente, se reduce la posibilidad de los ciberdelincuentes sean capturados.

Estrategia de negocios

El mundo de los negocios es para personas voraces, esta frase se materializa al utilizar el ransomware como estrategia de negocio, es muy común encontrar todo tipo de servicios para empresas, que permiten que estas puedan obtener información de la competencia, así como

realizar ataques orquestados con el fin de desestabilizarlos y, aunque es una práctica nada legal, no está exenta de ser utilizada para beneficio de algunos y desgracia de otros.

Herramientas de trabajo colaborativo

Las herramientas de trabajo colaborativo se han convertido actualmente en la forma de trabajo más usada debido a la pandemia a causa del covid-19, por tanto, también se han convertido en un blanco para los ciberataques, por su vulnerabilidad de factor humano, su utilización desde estaciones de trabajo de empresas hacia puntos de conexión particulares (como tablets, smarphones, etc.), es decir, de uso no oficial de la empresa. Esto supone un gran punto de convergencia en el cual puede liberarse un virus para infectar a dicha empresa haciendo uso de las conexiones establecidas por los usuarios al interior de dichas plataformas, esto gracias nuevamente a la ingeniería social.

Fase II:

Los datos de cabecera sobre la encuesta realizada se encuentran en la siguiente ficha técnica:

FICHA TÉCNICA	
Persona natural o jurídica que realizó la encuesta	Karina Díaz Rhenals, estudiante de ingeniería de sistemas universidad de Córdoba sede Lorica.
Nombre	Encuesta sobre seguridad informática.
Fuente de financiación	No aplica.
Objetivo general	Obtener información general acerca del estado de las empresas en materia de seguridad informática.
Universo de estudio	Pequeñas y medianas empresas del departamento de Córdoba (Con infraestructura tecnológica definida).
Diseño de la muestra	A conveniencia. Respuesta voluntaria de los participantes en la encuesta.
Tamaño de la muestra	20 encuestas.
Método de muestra	Auto-administrada.
Técnica de recolección	Encuesta virtual a través de "Google Forms".
Fecha de aplicación	29 de Julio de 2021 hasta 15 de Agosto de 2021 (18 días aproximadamente).

Tabla 1. Ficha técnica encuesta sobre seguridad informática

A continuación se presentará la información obtenida a través de la encuesta aplicada a pequeñas y medianas empresas del departamento de Córdoba (Mi Pymes), dicha información gira en torno a las posibles vulnerabilidades que puede presentarse en materia de seguridad de la información.

Algunas de las preguntas se tendrán en cuenta para realizar una exploración inicial sobre el estado de las empresas encuestadas en materia de seguridad, las cuales serán presentadas a continuación:

A- ¿Con cuál/es de los siguientes métodos está protegida la información que utiliza?

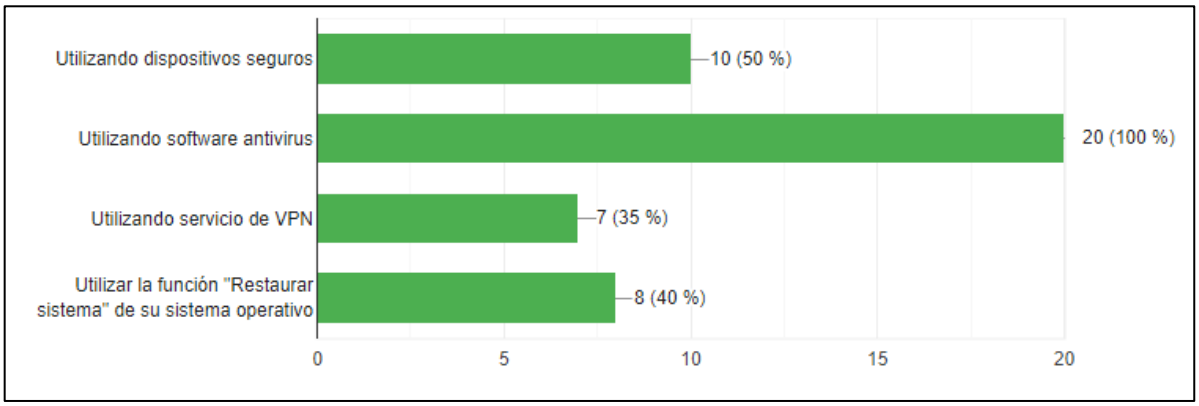

Gráfico A.. Métodos de protección de información

B- ¿Realiza periódicamente una copia de seguridad de sus datos?

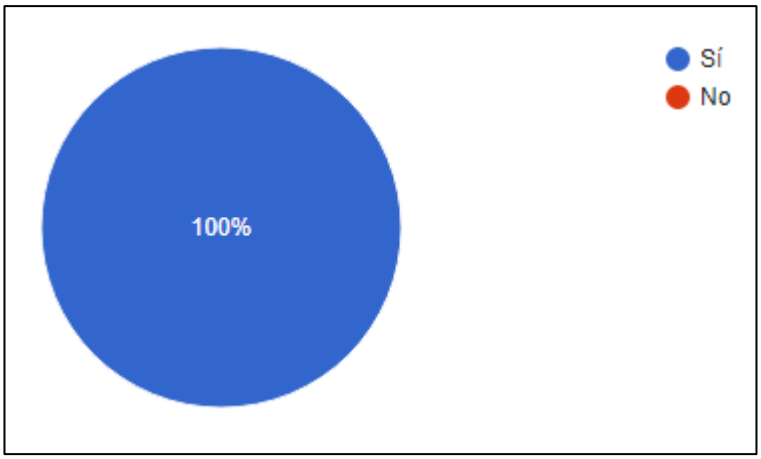

Gráfico B. Uso de backups (gráfico tarta)

C- ¿Cuáles de los siguientes aspectos considera más importantes para la ciberseguridad de las empresas? Seleccione todas las opciones que correspondan.

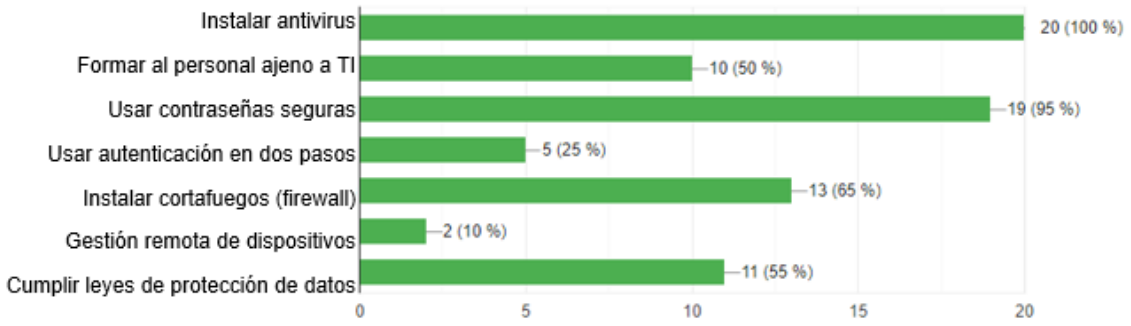

Gráfico C. Aspectos importantes de la seguridad informática

Tomando como base estas sencillas preguntas, se pueden deducir algunos aspectos importantes de la seguridad de las empresas encuestadas (basándose en la estadística).

Primero: Iniciando con la primer línea de defensa, todas las empresas encuestadas poseen un software antivirus protegiendo sus equipos informáticos según los resultados de la pregunta A, respuesta que asumen como importante y la ratifican en las respuestas de la pregunta C.

Segundo: La realización periódica de copias de seguridad es un aspecto que nuevamente es utilizado por todas las empresas encuestadas para mantener más segura su información, lo cual indica que tienen conocimiento de los riesgos a los que está sometida su información.

Tercero: Algunos aspectos como el uso de dispositivos seguros, contraseñas seguras y redes virtuales privadas (VPN), permite evidenciar que al menos el 50% de las empresas encuestadas, protegen su información con métodos acertados.

En materia de seguridad informática, las empresas están realizando el trabajo pertinente a la hora de proteger la información de las mismas, como mínimo a nivel básico en lo que a este apartado se refiere, con las siguientes preguntas, se pondrá en observación la o las posibles causas de las vulnerabilidades de las empresas encuestadas.

A la pregunta:

1- **¿En su empresa han existido accidentes a nivel de seguridad informática? Los resultados fueron:**

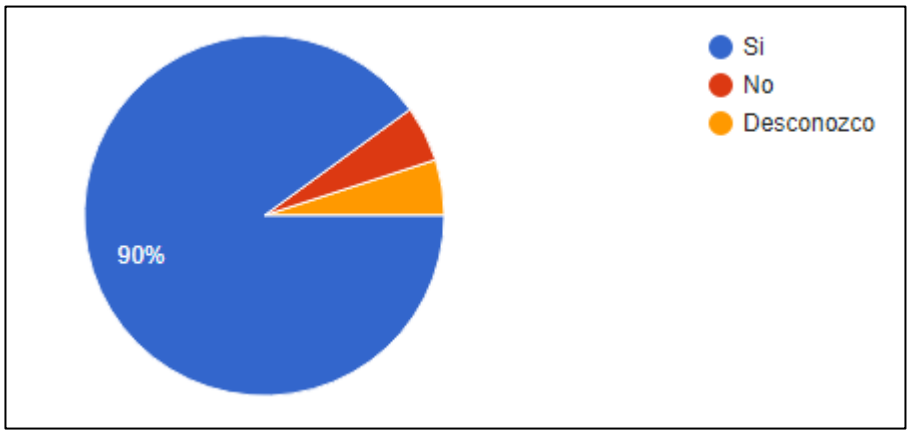

Gráfico 1. Accidentes a nivel de seguridad informática (gráfico tarta)

Como se aprecia en el gráfico 1, Las pequeñas y medianas empresas (por lo menos en el territorio del departamento de Córdoba), son un blanco habitual de los ciberdelincuentes, esto puede decirse que se debe tal vez a la implementación de seguridad no acorde al tipo de negocio y/o al manejo de los datos que estos poseen. Se evidencia de manera muy clara, que por lo menos el 90% de los encuestados, manifestó haber sido blanco de al menos un ciberataque, esto es muy habitual dada la tasa de ataques que ha estado con tendencia alta desde el 2017 hasta la actualidad en Colombia, no obstante, cabe aclarar que los ataques a los cuales fueron sometidos dichas empresas son variados e algunos casos, es claro afirmar que algunos virus comunes siempre están moviéndose por la red, lo cual deja un espectro

visible de "ataques inocentes", los cuales no poseen el mismo nivel de complejidad o de importancia a la hora de mantener la integridad de los datos, debido a que son como la gripe, se pueden eliminar del sistema con un simple escaneo y las afectaciones en el peor de los casos son muy mínimas.

A la pregunta:

2- En caso de responder afirmativamente a la pregunta anterior, por favor indique ¿Qué tipo(s) de ataque(s) informáticos ha recibido?

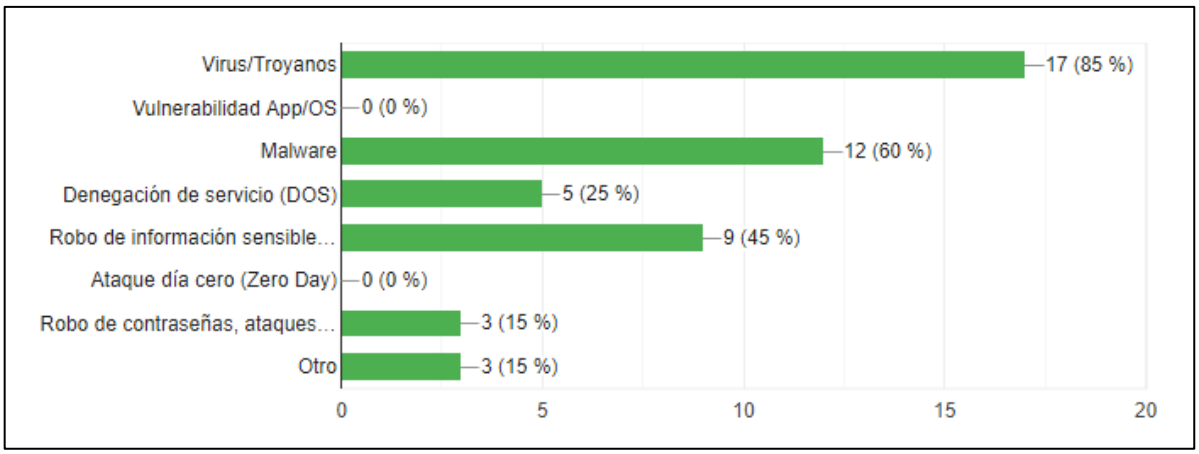

Gráfico 2. Accidentes a nivel de seguridad informática (gráfico barras laterales)

Según la información plasmada en el gráfico 2. Se evidencia que las pequeñas y medianas empresas son puntos convergentes regulares para ataques con variación de tipo. Es claro que algunas de estas al no poseer una estructura tecnológica compleja, como por ejemplo el uso de aplicaciones internas de tipo móvil, pues claramente la concentración de los ataques no inicia por ese punto. Se debe tener en cuenta que todas las empresas se encuestaron en igualdad de condiciones (es decir independientemente de su estructura tecnológica), para

analizar un espectro amplio que permita obtener información más clara acerca de la forma de ataque de los ciberdelincuentes.

A partir de la información dada, se puede deducir que teniendo en cuenta que los tipos de ataque más utilizados por los ciberdelincuentes son los virus/troyanos 85%, malware 60% y robo de información sensible 45%, asumiendo que cada ataque con el malware ransomware tiene una finalidad clara la cual es secuestrar, robar y/o destruir información sensible de las víctimas, es posible evidenciar que el porcentaje de ataques con Malware es alto siendo consecuente teniendo en cuenta que los ataques con ransomware aumentaron en al menos 300% desde marzo de 2020 [31].

A la pregunta:

3- ¿Su empresa invierte presupuesto en ciberseguridad?

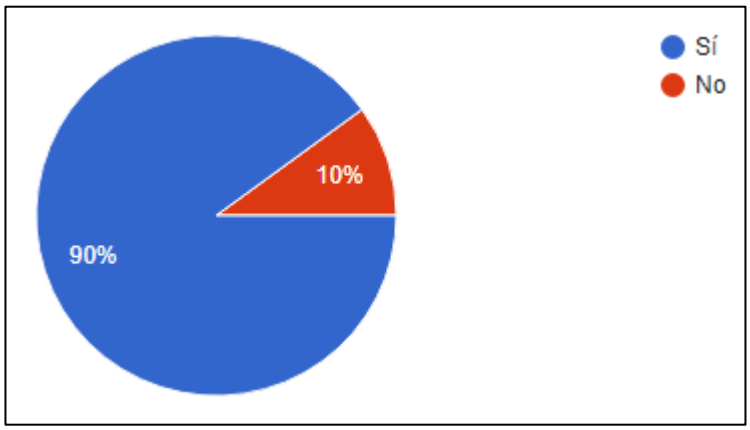

Gráfico 3. Inversión de presupuesto en seguridad informática (gráfico tarta)

Este 90% permite deducir que las pequeñas y medianas empresas, están protegiendo sus datos al menos a nivel básico en lo que a seguridad informática se refiere, este cambio proviene muy seguramente de ataques pasados, lo cual literalmente obligó a dichas empresas a modernizar su infraestructura de seguridad informática o a utilizar otros mecanismos para

mantener segura su información.

Aunque exista un mayor porcentaje de pequeñas y medianas empresas que estén invirtiendo en seguridad informática, no implica que ahora estén exentos de ser blancos para los ciberdelincuentes, por lo cual adquirir un buen servicio en torno al tema en cuestión es vital para evitar el robo o la pérdida de datos.

El 10% restante de pequeñas y medianas empresas en algunos casos es posible que la falta de seguridad en materia tecnológica, puede deberse a temas económicos o a infraestructuras antiguas que para la finalidad del negocio no requieren una inversión adicional como pueden concluir que el uso de un antivirus convencional gratuito o una licencia básica del mismo es suficiente para mantener protegidos sus datos y así puede haber una larga lista de razones que son poco relevantes teniendo en cuenta el mínimo porcentaje de empresas que no invierte dinero en seguridad, teniendo en cuenta que al mencionar dicha inversión, se debe entender que esta se hace periódicamente.

A la pregunta:

4- ¿Conoce usted si su empresa trabaja con herramientas tipo SIEM?

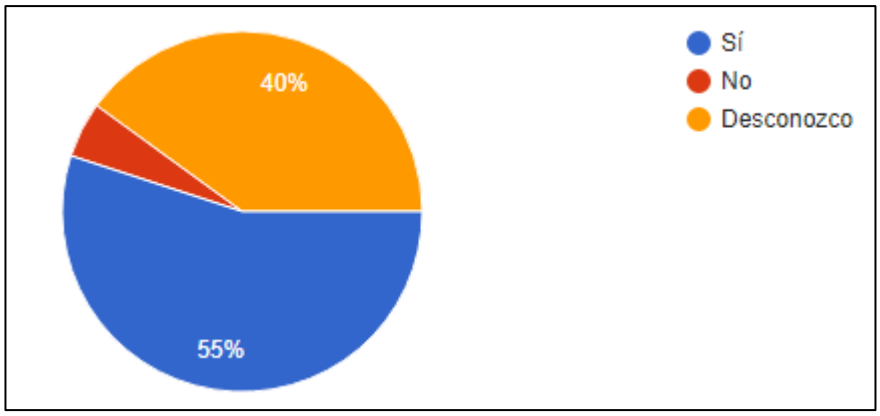

Gráfico 4. Utilización de herramientas SIEM (gráfico tarta)

Poco más del 50% de las empresas encuestadas utiliza herramientas tipo SIEM[1] para controlar la seguridad de los datos dentro la misma. La implementación de este tipo de herramienta se evidencia en mayor forma dentro de las empresas que puede presumirse que poseen un capital bruto mayor o puede que la cantidad de información manejada por la misma sea considerablemente grande (como centros de salud, clínicas, etc), en cualquiera de los casos, de igual forma existe aún un desconocimiento grande acerca de las herramientas para la protección de los datos de las empresas lo cual es un problema generalizado en materia de seguridad debido a que aunque no es un factor determinante el conocer cada tipo de herramienta que existe actualmente para la protección de datos de una empresa, la utilización de las mismas sí implica una disminución en la probabilidad de que un ataque pueda generar grandes pérdidas económicas.

A las preguntas:

5- ¿Los empleados (fuera del área de sistemas) tienen la formación que necesitan para prevenir errores de seguridad informática?

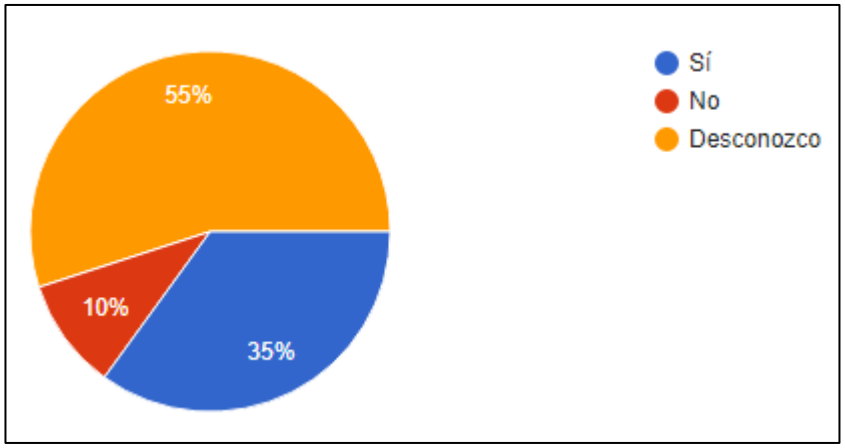

Gráfico 5. Prevención de errores humanos (gráfico tarta)

[1] La informática SIEM es un acrónimo que significa Security Information and Event Management y que se traduce como gestión de información y eventos de seguridad. Esta herramienta permite mejorar la seguridad global de una organización y/o compañía desde el punto de vista informático.

6- ¿Los empleados son capaces de identificar un intento de phishing?

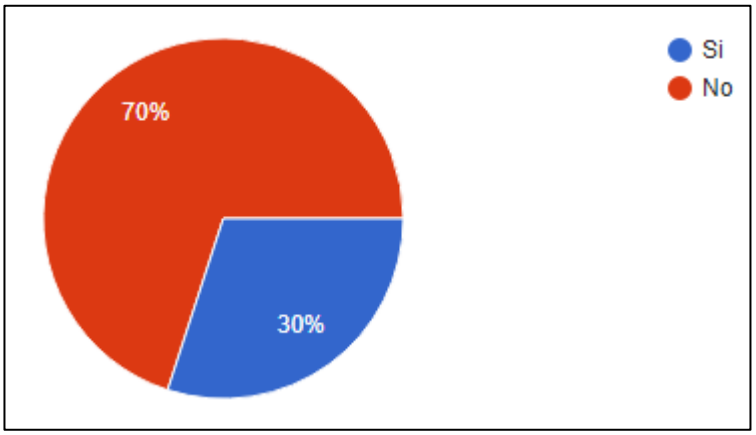

Gráfico 6. Prevención de phishing (gráfico tarta)

Las preguntas relacionadas con los gráficos 5 y 6, permitirán hacer un análisis de un punto clave de vulnerabilidad de una empresa, el cual es el factor humano.

Ahora, es claro tener en cuenta que en ambos casos el porcentaje de prevención de errores y de conocimiento sobre phishing es muy bajo y esto permite ver una ventana de posibilidad para un ciberatacante, debido a que este desconocimiento, que es una de las principales formas de ataque el cual se conoce como "ingeniería social", que no es más que la utilización de este desconocimiento de la víctima, para que esta realice lo que el ciberatacante quiere, es decir, son encaminados a presionar en un botón, ingresar a un link específico para recuperar una contraseña, etc.

Teniendo en cuenta los resultados de estas preguntas particulares, se puede ir trazando una alternativa de solución, al ser este un problema de gravedad, debido a que el error del factor humano, puede ser el paso para pérdidas económicas.

A las preguntas:

7- ¿Realiza periódicamente una copia de seguridad de sus datos?

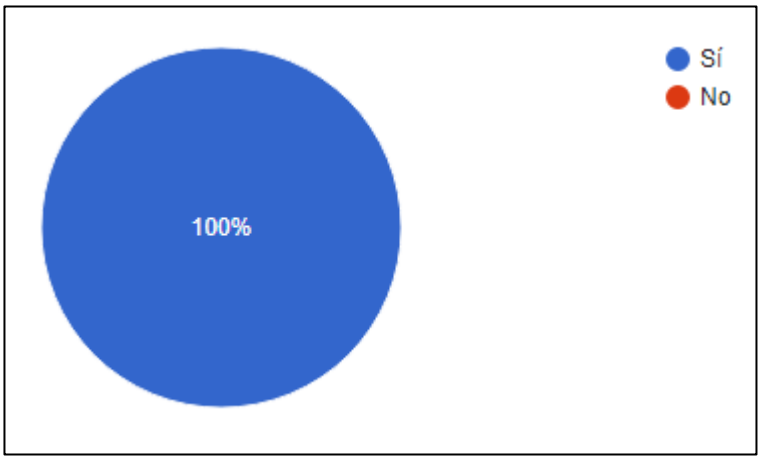

Gráfico 7. Uso de backups (gráfico tarta)

8- ¿Tiene idea de la repercusión real y las pérdidas que sufriría su organización si se ve afectada por un robo de información?

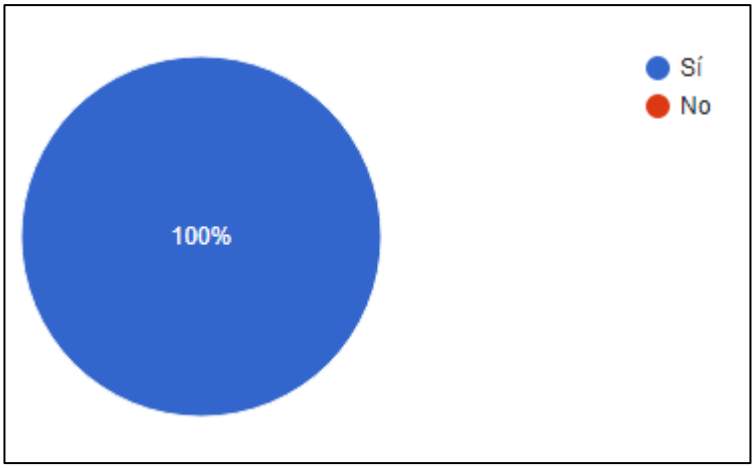

Gráfico 8. Importancia financiera de la información (gráfico tarta)

Como punto de convergencia vital para el funcionamiento de toda empresa con respecto a la información de sus bases de datos, es la realización de copias de seguridad, que si bien no en todos los casos poseen la misma capacidad para aislar dicha copia de un posible ataque, los propietarios de las empresas tienen muy claro que la información es vital para el desarrollo

de las actividades de las mismas.

La pérdida de información, está sujeta a pérdidas en materia financiera en cualquier empresa, debido a que, aunque manipulación de información no sea el generador de ingresos de la misma, sí lo son todos los registros almacenados en las bases de datos, datos de clientes, deudas, cuentas, etc.

En este aspecto, todas las empresas encuestadas saben que la información es vital para el correcto desarrollo de sus actividades esenciales, por ello las copias de seguridad bien organizadas de manera periódica (no importa lo antiguo del sistema siempre y cuando esté actualizado), es de vital importancia para mitigar la pérdida de datos al ser víctimas de ataques de tipo ransomware.

Análisis final de la fase II: Todo el material informativo obtenido de las encuestas, permite observar en primera instancia que existen múltiples problemas que propician que las empresas sean blanco de ataques informáticos de tipo ransomware, algunos por el uso de herramientas de seguridad muy básicas otros por lo antiguo de sus sistemas en uso, pero luego de realizar un análisis e interpretación de la información obtenida, es evidente que la herramienta de ataque más utilizada por el ciberdelincuente para infectar sistemas de pequeñas y medianas empresas es a través de la estrategia de la **ingeniería social**[2] debido a que esta se enfoca en el error y/o el desconocimiento humano sobre cómo pueden ser infectados los ordenadores de sus puestos de trabajo, por ende este es un pilar fundamental que toda empresa debe tener en cuenta para mitigar el impacto de un ataque. Esta estrategia es utilizada muy frecuentemente y es debido a su bajo costo para el ciberdelincuente y a la minimización del riesgo de ser identificado. La utilización del engaño como método de persuasión con el fin de que la víctima realice lo que el atacante desea y de esta forma poder lograr su objetivo.

[2] La ingeniería social es una estrategia usada por los ciberdelincuentes para engañar a sus víctimas con el fin de que estos revelen información sensible (a través de link engañosos, archivos maliciosos, etc) que les permita acceder a sus cuentas de usuario o infectar el ordenador en uso.

Fase III:

Con el fin de proporcionar información que permita mitigar la efectividad en cuanto a un inminente ataque de tipo ransomware (en general cualquier tipo de ataque que utilice la ingeniería social como medio), se proveen las siguientes recomendaciones como buenas prácticas que deben tomarse como medida de prevención.

Buenas prácticas (preventivas) para mitigar los ataques con malware ransomware

Los sistemas informáticos siempre estarán expuestos a vulnerabilidades, algunas más graves, otras con un mayor tiempo de exposición desde el momento en que se detecta hasta el momento en que se resuelven y otras de forma casi permanente en lo que se refiere al factor humano. Para fomentar el uso de buenas prácticas, este informe presenta los siguientes puntos críticos a tener en cuenta:

i. Proteger la red o redes internas de la empresa protegida, para ello existen herramientas conocidas como "SIEM", las cuales permiten proteger la información de ataques, e inclusive permiten combatirlos en la mayoría de los casos.
ii. Realizar copias de seguridad o backups es muy importante para poder contar con un respaldo que permita que el funcionamiento de la empresa no cese por pérdida o robo de datos.
iii. Comprender que en malo que a sistemas operativos se refiere, es necesario tener en cuenta que todo ambiente en el que se pueda ejecutar una serie de instrucciones, se puede ejecutar un virus, por lo tanto es necesario tener muy claro que en cualquier sistema puede ejecutarse un virus.
iv. Licenciar los equipos, programas y utilidades de terceros que sean utilizados por la empresa. En el ambiente empresarial, el software licenciado además de ser un requisito legal, es primordial a la hora de evitar exponer los datos de la empresa, por tanto, a partir del sistema operativo, hasta los programas utilizados de manera interna, deben evitar ser pirateados, debido a que esto genera vulnerabilidades que los

ciberdelincuentes pueden aprovechar.

v. Capacitar a los empleados en el uso de los sistemas de la empresa y en seguridad informática para que adquieran los conocimientos necesarios (por lo menos a nivel básico) que les permita detectar posibles fraudes como por ejemplo a través del correo electrónico evitando así ser víctimas de phishing u otras técnicas de ingeniería social.

vi. Evitar ejecutar archivos que contengan las extensiones EXE, COM, SCR, provenientes de correo electrónico, porque son una clara señal de que se intenta robar información.

vii. Evitar abrir documentos con extensiones DOCX (Word), PDF o XLSX (Excel) de dudosa procedencia o inclusive si el nombre del archivo está escrito en un idioma distinto.

viii. Evitar activar macros para archivos en Excel o Word que provengan de internet y/o correo electrónico, debido a que estos pueden ejecutar algoritmos que utilizan la ofimática como cortina para descargar archivos maliciosos o acceder a los registros del sistema.

ix. Navegar de forma segura en internet, es importante tener en cuenta que muchas webs también almacenan gran cantidad de archivos maliciosos, por ello se debe evitar visitar sitios poco conocidos.

x. Mantener actualizados los programas y sistemas operativos que se utilicen al interior de la empresa, al hacerlo se aumenta el nivel de seguridad gracias a los parches que la empresa prestadora del servicio envía con datos adicionales de seguridad o corrección de brechas en la misma.

xi. Considerar el uso de tecnologías en la nube en caso de no estar utilizando ninguna todavía. Toda la infraestructura basada en la nube posee un menor riesgo de ataque, debido a que sus vulnerabilidades son más difíciles de explotar.

xii. Analizar todo archivo descargado sin importar su procedencia, esto es vital teniendo en cuenta que el ataque puede ocurrir luego de una cadena de envío de archivos, aun cuando se confía en el emisor, este puede ser también una víctima de la ingeniería social y el confiar puede traer problemas.

xiii. Revisar las extensiones instaladas en el navegador, esto con el fin de no utilizar desconocidos que puedan generar brechas de seguridad.

xiv. Deshabilitar la ejecución de archivos desde las carpetas AppData y LocalAppData, Cryptolocker ejecuta su archivo .EXE desde alguna de estar carpetas, por lo tanto se pueden bloquear un comportamiento en particular que es típico del uso de este malware, adicionalmente se deben crear excepciones, en caso de que alguno de los programas utilizados se ejecute desde alguna de estas carpetas.

xv. Proteger el sistema utilizando antivirus y un firewall actualizados, debido a que el ciberatacante varía sus programas maliciosos para poder evadir la seguridad.

xvi. Utilizar filtro antispam, debido a que muchos de los ataques ransomware han sido distribuidos a través de campañas masivas de correo electrónico.

xvii. Utilizar cuentas con privilegios, es decir que los usuarios no posean permisos de administrador dentro del sistema, esto en el caso de Windows se puede utilizar para "esquivar" amenazas.

xviii. Utilizar máquinas virtuales es una técnica que permite aislar el sistema operativo y es idóneo porque el ransomware no suele consolidarse en entornos virtuales.

xix. Bloquear las ejecuciones de JavaScript, debido a que la ejecución de ventanas emergentes pueden infectar el ordenador durante la navegación.

CONCLUSIONES Y RECOMENDACIONES

Luego de realizar el análisis de toda la información obtenida, se puede concluir que el factor de vulnerabilidad más importante es el usuario, debido a que las acciones de este repercuten totalmente en el sistema y los archivos del mismo.

Los ataques con malware varían según la experiencia del atacante y de la vulnerabilidad del sistema o en tal caso, viendo a la empresa como un todo, utilizar el eslabón más débil, el cual es el usuario inexperto y sin ningún tipo de capacitación, por lo cual es necesario actuar con prudencia, esta es una medida clave para disminuir la posibilidad de que un ataque exitoso que comprometa información sensible de una empresa.

El ransomware es un tipo de malware sumamente peligroso para cualquier organización por su modo de operación al secuestrar información y solicitar rescate por la misma, e inclusive al destruirla al no ser efectuado el pago, por ello se hace necesario que las empresas se den a la tarea de capacitar a sus empleados en buenas prácticas para el uso de sistemas de información, con el fin de reducir la probabilidad de que el ciberatacante encuentre una vulnerabilidad a través de un usuario que ponga en peligro la información de la empresa.

Es importante que las empresas se adapten a las nuevas tecnologías en materia de ciberseguridad con el fin de no exponer sus datos ante posibles ataques, debido a que luego del análisis de la información, se pudo evidenciar que tan sólo el 35% de las empresas encuestadas se encuentran un paso por delante en lo que a seguridad se refiere, debido a que poseen sistemas tipo SIEM o porque hacen uso de buenas prácticas para evitar exponer su información.

Es importante sesgar el acceso de los usuarios en el sistema, debido a que esto impide

que el ransomware pueda ejecutarse libremente y encriptar archivos, debido que tendría que romper los privilegios o encontrar la clave de administrador para hacerlo. En situaciones donde parte de la información de una empresa o su totalidad se vea comprometidas, la primer recomendación es NO REALIZAR EL PAGO, debido a que en primera instancia se debe realizar un análisis de los equipos afectados y de la información que se encuentra encriptada, con ello, hacer un contraste con las copias de seguridad, para identificar hasta qué punto la información se guardó dentro de los archivos de copia de seguridad y así evaluar si restaurando las mismas, la pérdida de información es mínima o "despreciable".

Sesgar la red interna de la empresa también es un factor determinante a la hora de mitigar el avance de un ataque, debido a que realizando este procedimiento, la red de la empresa puede ser aislada, de manera que por ejemplo el almacenamiento de las copias de seguridad no se vea afectado por el ataque y así poder recuperar la información en caso de pérdida por el ataque.

Para finalizar, es de suma importancia recalcar que todas las recomendaciones aquí dadas, no son determinantes para no ser atacado con un malware como el ransomware, debido a que es imposible, en lugar de ello, como se ha descrito en este documento, la finalidad del mismo es ayudar a mitigar los efectos que dichos ataques pueden tener sobre las empresas, para ello es de suma importancia tener en cuenta las buenas prácticas para mitigar los ataques.

REFERENCIAS

[1] M. Rivero, «INFOSPYWARE,» INFOSPYWARE, 1 Octubre 2016. [En línea]. Available: https://www.infospyware.com/articulos/que-son-los-malwares/.

[2] Revista Semana, «¿Qué es un Malware y cómo se puede prevenir?,» Semana, 30 Enero 2014. [En línea]. Available: http://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3.

[3] Panda Security, «www.pandasecurity.com,» Panda Security, [En línea]. Available: https://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/virus/.

[4] AVAST, «www.avast.com,» [En línea]. Available: https://www.avast.com/es-es/c-computer-virus.

[5] P. Security, «Panda Security,» [En línea]. Available: https://www.pandasecurity.com/colombia/homeusers/security-info/classic-malware/worm/.

[6] INSTITUTO NACIONAL DE CIBERSEGURIDAD, Ransomware: una guía de aproximación para el empresario, Madrid, 2017.

[7] ESET, ESET-Ransomware-final, Ciudad de Mexico, 2017.

[8] ICANN, «www.icann.org,» 13 Marzo 2017. [En línea]. Available: https://www.icann.org/news/blog/que-es-un-ransomware.

[9] Test de Velocidad, «test de velocidad,» [En línea]. Available: https://www.testdevelocidad.es/test-de-puertos/vulnerabilidades-y-troyanos/ransomware/.

[10] «Remote Desktop Protocol,» [En línea]. Available: https://msdn.microsoft.com/en-us/library/aa383015(v=vs.85).aspx.

[11] Secretaría Nacional de Tecnologías de la Información y Comunicación, «Centro de Respuestas a Incidentes Cibernéticos,» [En línea]. Available: https://www.cert.gov.py/index.php/noticias/distribucion-de-ransomware-mediante-ataques-de-fuerza-bruta-rdp.

[12] Microsoft, «Server Message Block Overview,» [En línea]. Available: https://msdn.microsoft.com/es-es/library/hh831795(v=ws.11).aspx.

[13] University of Malaga, «neo.lcc.uma.es,» [En línea]. Available: http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/rsa.html.

[14] [En línea]. Available: http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf.

[15] ESET, «ESET Latinoamerica,» [En línea]. Available: https://empresas.eset-la.com/archivos/novedades/34/ESET-Ransomware-final.pdf.

[16] Fireeye, «ApateDNS,» 11 Septiembre 2011. [En línea]. Available: https://www.fireeye.com/services/freeware/apatedns.html. [Último acceso: 2018].

[17] Ffireeye, 24 Octubre 2017. [En línea]. Available: https://www.fireeye.com/services/freeware/fakenet-ng.html.

[18] Microsoft, «Dependency Walker,» [En línea]. Available: http://www.dependencywalker.com/.

[19] M. Aubert, 31 Agosto 2016. [En línea]. Available: https://medium.com/@aubsec/pestudio-standard-f2ada4e8564.

[20] Panda Security, «Classic Malware: su historia, su evolución.,» Panda Security, [En línea]. Available: https://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/.

[21] ESET Latinoamerica, «La historia del malware, actualizada: un breve repaso,» 24 Octubre 2016. [En línea]. Available: https://www.welivesecurity.com/la-es/2016/10/24/historia-del-malware-actualizada/.

[22] ESET , «La evolución del ransomware: del ochentero PC Cyborg a un servicio en venta,» [En línea]. Available: https://www.welivesecurity.com/la-es/2015/08/21/evolucion-del-ransomware/.

[23] KnowBe4, «Winlock Ransomware,» [En línea]. Available: https://www.knowbe4.com/winlock-ransomware.

[24] KnowBe4, «GPCode Ransomware,» [En línea]. Available: https://www.knowbe4.com/gpcode.

[25] KnowBe4, «Archiveus Trojan,» [En línea]. Available: https://www.knowbe4.com/archiveus-trojan.

[26] KnowBe4, «GPCode.AK Ransomware,» [En línea]. Available: https://www.knowbe4.com/gpcodeak-ransomware.

[27] KnowBe4, «Ransomware,» [En línea]. Available: https://www.knowbe4.com/ransomware.

[28] KnowBe4, «Citadel Trojan,» [En línea]. Available: https://www.knowbe4.com/citadel-trojan.

[29] ESET, TODO SOBRE EL RANSOMWARE, Cuidad de mexico, 2016.

[30] Piscitelli, E. (2015, 2 octubre). [Mensaje CryptoLocker]. El Ransomware Cryptolocker ha hecho de las suyas en nuestra PC. https://www.redusers.com/noticias/ransomware-que-es-y-como-funciona-el-secuestro-digital/

[31] Caracol, A. (2021, 2 septiembre). El ransomware asola a Colombia. Caracol Radio. https://caracol.com.co/radio/2021/09/02/tecnologia/1630613927_972376.html