ESTUDIO MONOGRÁFICO SOBRE LA AMENAZA RANSOMWARE, SU IMPACTO EN LAS ORGANIZACIONES Y BUENAS PRÁCTICAS PARA SU PREVENCIÓN Y MANEJO

JOSE CARLOS PEREZ CASTRO

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

ESTUDIO MONOGRÁFICO SOBRE LA AMENAZA RANSOMWARE, SU IMPACTO EN LAS ORGANIZACIONES Y BUENAS PRÁCTICAS PARA SU PREVENCIÓN Y MANEJO

JOSE CARLOS PEREZ CASTRO

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

Tutor
ING. CÉSAR SILVA

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

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C., 26 de mayo de 2021

DEDICATORIA

A Dios mi Creador y a quien debo todo, a mi esposa María Claudia y mis hijos Samuel y Santiago por soportar mis días de ausencia y ocupación académica y ser el motor de mi vida. Pero de forma especial a mi padre, quien luchó hasta sus límites humanos para que lograra un día alcanzar mis propósitos y quien alguna vez me dijo "haz las cosas a lo bien hecho y la historia te absolverá".

Gracias Papá. Esto es para ti.

AGRADECIMIENTOS

Agradecimientos principalmente a la Universidad Nacional Abierta y a Distancia que me brindó la oportunidad de ser parte de su comunidad y formarme para ser un mejor profesional y tener las herramientas para brindar un mejor servicio al empresariado colombiano y a la sociedad en general.

A los tutores que guiaron mi proceso académico con mucha disposición y colocaron su experiencia y conocimientos al servicio de un aprendizaje primordialmente autónomo, pero con un acompañamiento oportuno y acorde con las expectativas de un ciclo de posgrado.

A los Ingenieros Luis Fernando Zambrano y César Silva por las sugerencias realizadas y por su acompañamiento en el proceso.

Al ingeniero Frey de Jesús Castro, por su guía y apoyo durante la consolidación del documento final del proyecto de grado que permitió lograr los objetivos planteados desde un comienzo con sus apreciaciones puntuales y valiosas para el perfeccionamiento del estudio monográfico presente.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

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.

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 del mismo. 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 inutilizables para su propietario. El objeto común de este ciberataque es extorsionar a la víctima con un mensaje en el que exigen un pago a cambio de permitirle recuperar su información.

VULNERABILIDAD: En seguridad informática se denomina vulnerabilidad a toda aquella debilidad o agujero de seguridad que eventualmente permitiría a un ciberdelincuente tomar el control de un sistema informático y realizar actividades delictivas como el robo, alteración de datos o dejar inoperable un sistema. Estas vulnerabilidades pueden ser corregidas por los llamados parches de seguridad.

0-DAY: Son vulnerabilidades de sistemas de información que no son conocidos por sus fabricantes, pero sí por algunos ciberdelincuentes. Al ser desconocidos estos fallos, no se desarrollan actualizaciones de seguridad y por tanto permanecen a la merced de quienes tengan conocimiento de esta debilidad. Son muy peligrosos y podrían ser aprovechados por largo tiempo de forma inadvertida para la víctima.

RESUMEN

Ransomware es el término acuñado para definir una clase de software malicioso o “malware” que se ha convertido en una auténtica pesadilla para los administradores de TI. Es una palabra compuesta por “ransom” y “software” que traduce "software de rescate", en otras palabras, una aplicación diseñada y diseminada por ciberdelincuentes capaz de infectar un sistema y cifrar sus ficheros por medio de un algoritmo robusto de encriptación, con el fin de extorsionar a su administrador exigiéndole un pago a cambio de poder recuperar su información.

Sin embargo, esta definición no hace justicia al nivel de daño que esta amenaza puede provocar en los servicios económicos, políticos, sanitarios o de seguridad, que afectan sensiblemente a los ciudadanos del común que tienen aspectos de su vida vinculados a dichos sistemas de información.

Por lo tanto, la finalidad de este documento es analizar en detalle las características de los criptovirus, su arquitectura, sus variantes, algoritmos de cifrado más utilizados, métodos de ataque, perfil de los atacantes, métodos de detección y especialmente generar un protocolo de buenas prácticas para preparar los sistemas objetivos del malware y proporcionarles un blindaje multicapa ante la posible incidencia del ataque; además de una guía de manejo ante una eventual infección y métodos de recuperación para mantener ante todo la disponibilidad de los servicios ofertados en la compañía.

Palabras clave: amenaza, controles, cibercriminalidad, criptomoneda, criptovirus, contingencia, disponibilidad, ransomware, rescate, seguridad, prevención,

ABSTRACT

Ransomware is the term coined to define a class of malicious software or "malware" that has become a real nightmare for IT administrators. It is a word composed of "ransom" and "software" that translates "rescue software", in other words, an application designed and disseminated by cybercriminals capable of infecting a system and encrypting its files by means of a robust encryption algorithm, with the purpose of extorting your manager by demanding a payment in exchange for being able to retrieve your information.

However, this definition does not do justice to the level of damage that this threat can cause in economic, political, health or security services, which significantly affect ordinary citizens who have aspects of their lives linked to such information systems.

Therefore, the purpose of this document is to analyze in detail the characteristics of cryptoviruses, their architecture, their variants, most commonly used encryption algorithms, attack methods, profile of attackers, detection methods and specially to generate a good protocol. practices to prepare the objective systems of the malware and provide them with a multilayer shield before the possible incidence of the attack; in addition to a management guide in the event of an infection and recovery methods to maintain the availability of the services offered in the company.

Keywords: availability, contingency, controls, cybercrime, ransomware, cryptocurrency, cryptovirus, rescue, prevention, security, threat

INTRODUCCIÓN

La concepción de seguridad, independientemente del aspecto humano al que se aplique, ha evolucionado de la mano de eventos adversos que interrumpieron el curso normal de las operaciones cotidianas de una entidad que se vio obligada a observar cómo se afectaban de distintas formas sus activos, al ser vulnerados sus sistemas con variables y recursos nunca previstos o por medio de herramientas que comúnmente eran utilizadas con fines benignos.

De forma especial la producción, almacenamiento, procesamiento y transmisión de la información digital, se ha convertido en el escenario de la guerra posmoderna: la guerra por la seguridad de la información. Y en este entendido debe suponerse que no existen presupuestos éticos ni límites establecidos para el accionar de los cibercriminales que están haciendo uso de herramientas muy poderosas como la criptografía, la vulneración de sistemas con exploits “0-days” o las redes anónimas para atacar con propósitos políticos, económicos o frívolos, los sistemas de información de compañías y personas del común en todo el mundo.

Es en este incierto e inquietante panorama que se desarrolla la amenaza Ransomware, conocida por ser la versión informática de un secuestro extorsivo en la que, de manera subrepticia, un malware se infiltra e instala en el sistema operativo de una máquina, cifrando de manera prácticamente irreversible su información o bloqueando la pantalla del sistema de modo que la deja inaccesible para su propietario o administrador. Este ataque va acompañado de mensajes extorsivo en los que se informa de la situación y se exige un pago anónimo para poder recuperar sus datos.

Desde los tiempos del Dr. Joseph Popp, hace casi 40 años cuando cifró los archivos de los asistentes a una de sus conferencias por medio de un diskette infectado, la idea ha evolucionado de forma sobresaliente, incorporando algoritmos avanzados de encriptación, métodos de penetración por exploits o tácticas de ingeniería social que logran aprovechar la falta de experticia y la ausencia de controles informáticos para infligir daños cuantiosos en términos financieros, operacionales, documentales y de imagen de los que pueden tardarse meses o años en recuperarse por completo.

El objetivo que se propone esta monografía es proporcionar una fuente de información confiable y relevante para organizaciones de cualquier tamaño o actividad económica, sobre la naturaleza de la amenaza Ransomware, los riesgos que entraña ser víctima de ella y proponer un protocolo de prevención de ataques y una guía de manejo de desastres que coadyuve a prevenir o en todo caso mitigar

los efectos de un ataque de este tipo a la infraestructura informática crítica con la que se cuente.

Para lograr este cometido, se realizará un investigación descriptivo-analítica que se apoyará inicialmente en un recorrido histórico evidencie la sofisticación que ha ido adquiriendo la amenaza bajo estudio, además de sus variados vectores de ataques, antecedentes recientes de ataques, tipos de objetivos e impacto generado. Todo lo anterior, como fundamento para elaborar una guía práctica que concentre las lecciones adquiridas y ofrecer así una hoja de ruta que guíe a los responsables de seguridad en la tarea de preservar la confidencialidad, integridad y sobre todo la disponibilidad de la información bajo su poder.

El enfoque metodológico parte de una amplia base documental de incidentes registrados y analizados por importantes empresas de seguridad, reportes de prensa, estadísticas oficiales y opiniones de expertos en seguridad que ponen sobre la apoyan la necesidad de implementar estrategias efectivas en el aseguramiento de la información. El análisis de esta masa documental objetiva permite reconocer y entender por qué ocurren este tipo de ataques, cómo se desarrollan y cómo encuentran a sus víctimas potenciales; además de soportar el diseño de procedimientos de prevención y defensa valiosos para aquellas organizaciones que aún no están seguras de cómo proceder ante la posibilidad de ser tocado por el Ransomware.

Se hace especial énfasis en la importancia de la prevención como mejor estrategia de defensa, teniendo como premisa que “la mejor pelea es la que no se da”. Es importante concienciar a los administradores de TI sobre la urgencia de conocer sus sistemas y de realizar pruebas permanentes que midan la fortaleza de sus mecanismos de seguridad, y especialmente que identifiquen los eslabones débiles en la estrategia de seguridad que gran parte de las veces son los usuarios que, al no seguir las recomendaciones propuestas por expertos, convierten sus equipos en portales de entrada para aplicaciones inseguras.

Si bien, nunca se podrá hablar de una seguridad invencible, resulta muy conveniente que se cuente con planes de contingencia que fijen protocolos probados para responder de forma inmediata a un ataque de secuestro informático y garantice que, aunque se deje inoperante un sistema o se pierda el acceso a los datos, estos podrán ser recuperados y puestos en servicio en el menor tiempo posible. Este protocolo de respuesta es otro de los propósitos de este tratado monográfico.

1. PLANTEAMIENTO DEL PROBLEMA

Colombia, según el vicepresidente de Planeación Estratégica de la Sociedad Internacional de Automatización, "… ha desarrollado una serie de prácticas para la seguridad de los gobiernos y de la prestación de servicios públicos. Las Fuerzas Militares y la Policía están preparadas, pero el país en general se ha ratificado en un nivel de riesgo intermedio. Un estudio de ciberseguridad industrial muestra que alrededor del 40% de las empresas que fabrican algún tipo de producto en el sector real, no han hecho una evaluación de riesgos por ciberataques" [1].

Sin embargo, el problema puede ser aún mayor. Según fuentes consultadas por el periódico El Tiempo, "Colombia fue el país de la región en el que más se detectaron infecciones de malware del tipo ransomware durante 2018, según un informe de la compañía de ciberseguridad ESET." [2] Lo que pone de manifiesto la compleja situación de inseguridad informática que se extiende a lo largo y ancho de un país que se esmera por alcanzar máximos históricos de desarrollo industrial y tecnológico, pero que al parecer no va acompañado de una cultura de ciberseguridad que soporte su crecimiento empresarial.

Este mismo reporte provisto por la empresa tecnológica ESET, informa que del total de eventos de infecciones por Ransomware en Latinoamérica "el 30 por ciento de los casos se presentaron en Colombia, seguido de Perú con un 16 por ciento, México (14 por ciento), Brasil (11 por ciento) y Argentina con el 9 por ciento" con la particularidad que en Colombia se detectó el mayor número de casos de ataque de la variante de criptovirus "Crysis" [3] que, valiéndose de técnicas de ingeniería social, se propaga por medio de correos electrónicos conteniendo archivos infectados y alertando a la víctima de supuestas deudas comerciales.

Cabe resaltar de igual forma, que el sector financiero es el sector más sensible o vulnerable a las ciber amenazas en general incluyendo desde luego los criptovirus. Así lo demuestra la Encuesta Global de Seguridad de la Información 2018 – 2019 de EY, informando que "Tan solo el 6% de las compañías de servicios financieros

[1] Noticias Caracol. 2017. Colombia es muy débil en materia de ciberseguridad: expertos. Disponible en: http://caracol.com.co/radio/2017/06/09/nacional/1497042960_148590.html

[2] TECNÓSFERA, El Tiempo. 2019. Colombia, el país de Latinoamérica más afectado por ransomware en 2018. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/los-paises-mas-afectados-por-ransomware-en-2018-313224

[3] Ibid.

aseguró que su función de seguridad de la información satisface las necesidades de la organización; sin embargo, el 65% tiene planes de realizar mejoras y el 31% advirtió que la escasez de habilidades es un obstáculo potencial.” [4]

Las consecuencias de un ataque ransomware pueden ser realmente devastadoras. El secuestro de activos de información de una entidad financiera, estatal o incluso de una PYME tiene el potencial de generar pérdidas económicas cuantiosas, indisponibilidad de los servicios, traumatismos operacionales, afectaciones a terceros, daño reputacional y/o retrasos importantes e irrecuperables en el desarrollo de toda clase de proyectos empresariales.

Estas afectaciones se ven acentuadas si las víctimas no cuentan con la infraestructura o preparación estratégica para enfrentar una contingencia de este tipo, si no cuentan con sistemas de respaldo o con tecnologías de protección que prevengan la propagación de los ciberataques hacia sistemas críticos o neurálgicos.

1.1 FORMULACIÓN DEL PROBLEMA

¿De qué maneras puede prepararse una organización para evitar la ocurrencia de un ataque ransomware y para mantener la disponibilidad de sus sistemas en caso de ser víctimas de un ataque?

[4] Ernst & Young, EY. 2019. Encuesta Global de Seguridad de la Información 2018-19. Disponible en: https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf

2. JUSTIFICACIÓN

La amenaza Ransomware se propone derribar la integridad y la disponibilidad de la información, que son dos de los tres ejes fundamentales de la seguridad de la información. Ninguna organización responsable puede operar efectivamente sin garantizar un servicio informático confiable, oportuno y con tolerancia a fallos. Por ello es indispensable contar con un sistema de prevención de desastres informáticos que involucren tecnologías convergentes de detección de malware, gestión permanente de actualizaciones de software y plan robusto de respuesta ante un ataque de secuestro de datos en el indeseable caso de su ocurrencia.

Una razón de peso para tomar con seriedad el riesgo de un ciber secuestro es el hecho de contar con herramientas de cómputo que ya no solo son los computadores de escritorio sino todo el ecosistema de tecnologías móviles como laptops, tablets o smartphones que se usan en el día a día por empleados de todos los niveles en los que ya está comprobado que también hay un considerable riesgo de ser infectados tanto en sistemas Android como en iOS que son los plataformas móviles más populares de la actualidad y para las que no se toma casi ninguna medida especial de protección, aun cuando son terminales con cada vez más protagonismo en la operación cotidiana de organizaciones de todos los tipos.

Contar con una base de conocimientos suficiente sobre la amenaza ransomware y con protocolos de acción detallados proveerá a los cuerpos técnicos responsables de la seguridad, de una útil herramienta de apoyo que dará precisión a sus sistemas de defensa pudiendo anticiparse a las fallas conocidas de los sistemas operativos que controlan los equipos, corrigiéndolas oportunamente sellando los agujeros por donde comúnmente penetran estos peligros.

La guía de procedimiento que se desarrollará en esta monografía se propone como un insumo estratégico para que las pequeñas y medianas empresas, eviten la improvisación al momento de responder a la crisis generada por un criptoataque, permitiéndoles priorizar acciones de contención y minimizando al máximo los daños provocados por la infección.

Entre otras ventajas del diseño y construcción de un guía de manejo de incidentes ransomware se presentan:

- Provee una base amplia de conocimiento sobre las características de la amenaza

- Conciencia a los responsables de decisiones sobre el riesgo al que se exponen de no tomar acciones
- Entrega una hoja de ruta para la preparación y el parcheo de los sistemas de información móviles o de escritorio
- Se integra al Sistema de Gestión de Seguridad de la Información con que cuente la compañía
- Provee un plan de manejo de desastres y de continuidad del negocio
- Disminuye ostensiblemente la probabilidad de ocurrencia de una infección y en consecuencia el impacto económico de la pérdida de la información privada o pública que se resguarde
- Posiciona a la organización en un nuevo nivel de competitividad frente a otras que opten por desconocer sus riesgos informáticos

Contar con un protocolo de prevención y respuesta antiransomware, afecta positivamente la operación de la empresa porque, por un lado, reduce las probabilidades de materialización del riesgo al identificar los vectores de ataques, las vulnerabilidades conocidas de las que se aprovecha y provee de una serie de mecanismos de control y protección probados alrededor del mundo para blindar los sistemas informáticos de ser secuestrados.

De igual forma, su componente de reacción disminuye sensiblemente los tiempos de respuesta y contención de la amenaza dotando a los responsables de seguridad de un plan de acción controlado que busca minimizar el tiempo de recuperación de los servicios afectados, garantizando al máximo posible la disponibilidad de estos.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar un protocolo de prevención de ataques del tipo Ransonware y guía de manejo de desastres para pequeñas y medianas empresas con infraestructura tecnológica de información.

3.2 OBJETIVOS ESPECÍFICOS

- Compilar información relacionada al ataque ransomware que permita comprender su arquitectura, metodología, motivaciones, variantes y alcance de su impacto en las organizaciones.

- Definir controles y planes de mejoramiento pertinentes para la prevención de ataques por criptovirus.

- Establecer una guía de manejo y recuperación de desastres en caso de ser víctimas de secuestro de datos.

4. MARCO REFERENCIAL

Para el desarrollo de este documento, se tomará como referencia la “Guía Contra Ataques Ransomware” desarrollada por Christopher M. Frenz & Christian L. Diaz y publicada por OWASP, en la que se abordan los mecanismos más eficaces para protegerse de este tipo de amenazas, así como un Plan de Respuesta ante incidentes como guía de recuperación luego de un criptoataque informático.

Otro referente es la guía “Ransomware: una guía de aproximación para el empresario” desarrollada por INCIBE (Instituto de Ciberseguridad de España) la cual hace un recorrido a través de los conceptos generales sobre las características del Ransomware, sus métodos de infección, sus variedades métodos de prevención y también consejos sobre cómo responder ante un ataque efectuado.

4.1 MARCO TEÓRICO - CONCEPTUAL

4.1.1 RANSOMWARE

El ransomware es un software malicioso de la familia de los criptovirus utilizado por ciberdelincuentes para secuestrar los archivos de un sistema o en ocasiones el sistema por completo, encriptándolos para hacerlos inaccesibles por el usuario de modo que los deja inutilizables, al tiempo que deja mensajes en las ubicaciones infectadas informando que se ha sido víctima de un cifrado de ficheros y que se deberá hacer un pago al atacante a cambio de poder recuperar su información.

Es en esencia un secuestro extorsivo de datos y está pensado para recaudar dinero alrededor del mundo utilizando medios de pago de difícil rastreo como las criptomonedas, por ejemplo, el Bitcoin. Tal como lo dirían Scaifer, Carter, Traynor y Butler: “Si bien esta clase de malware ha existido durante más de una década, su uso cada vez más extendido ahora causa decenas de millones de dólares en pérdidas a los consumidores anualmente. Siendo esto ya un problema, un número creciente de agencias de aplicación de la ley también han sido víctimas de ransomware, perdiendo valiosos archivos de casos y obligando a estas organizaciones a ignorar sus propios consejos y pagar a los atacantes.” [5]

[5] SCAIFE, N., CARTER, H., TRAYNOR, P., & BUTLER, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS).

4.1.2 CRIPTOVIROLOGÍA

Es la disciplina informática que se encarga de estudiar el uso de criptografía como ciencia para la construcción de softwares maliciosos. Entendida la criptografía como el conjunto de mecanismos para enmascarar la información y hacerla ilegible a terceros no autorizados. Es una poderosa herramienta que puede y ha sido usada con propósitos benignos como el procesamiento de datos y cifrado de comunicaciones civiles o militares alrededor del mundo. Pero tal como la energía atómica que ha otorgado sendos beneficios a la humanidad también puede ser usada con fines perjudiciales como es el caso del ransomware.

La criptovirología surge en el ambiente académico producto de la observación del mecanismo utilizado por los creadores de virus que empleaban el cifrado asimétrico por lo que el antivirus sólo puede ver la llave pública, pero desconoce la privada que es indispensable para descifrar los ficheros y que está en poder virus o de su creador. A medida que se avanzó el tiempo se fueron perfeccionando los algoritmos de cifrado a una variedad bastante amplia y compleja que ha convertido esta rama de la informática en un laboratorio para la gestación de virus que son "… herramientas para la extorsión, actividad criminal potencial, y como municiones en el contexto de la guerra de la información, en lugar de su reputación tradicional de ser simplemente una fuente de perturbación y molestia." [6]

4.1.3 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. [7]

"La Criptografía en términos generales es el arte y la ciencia que estudia las comunicaciones secretas. Específicamente, se ocupa de estudiar los métodos más apropiados para proteger la confidencialidad de la información. Por otra parte, el Criptoanálisis es la rama que se ocupa de descifrar los mensajes ocultos. Los mensajes secretos, creados a través de la criptografía, son llamados Criptograma o

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

texto cifrado (ciphertext). Su principal característica es que éstos terminan siendo un conjunto de caracteres (pueden ser dígitos o símbolos), que a ojos de un tercero parecieran no tener ningún sentido, ni orden lógico.” [8]

La criptografía puede ayudar a resolver varios problemas relacionados a la integridad, confidencialidad y la disponibilidad de la información, entendiendo por ejemplo al transmitir datos de forma que sea ilegible para terceros, se garantiza que exista alteración de la información envida, al tiempo que puede emplearse para asegurarse que solo las personas o sistemas autorizados puedan descifrar los ficheros y hacer uso de ellos si se cuenta con las llaves criptográficas necesarias.

4.1.4 SISTEMAS DE CIFRADO ASIMÉTRICO

“Un sistema de cifrado de clave pública usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.” [9]

El texto anterior explica la razón por la que los creadores de criptovirus utilizan los sistemas de cifrado asimétricos. Pueden utilizar la misma clave pública para encriptar a sus víctimas y no tienen necesidad de intercambiar su llave privada por lo que se hace imposible interceptarla en la comunicación. Los principales algoritmos de cifrado de clave pública y privada son: Diffie-Hellman, RSA, DSA, ElGamal, Criptografía de curva elíptica, Criptosistema de Merkle-Hellman, Goldwasser-Micali, Goldwasser-Micali-Rivesto el Cifrado extremo a extremo.

4.1.5 CIBERTERRORISMO

Podría definirse como: “El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de

[8] Ecured. Criptografía. Disponible en: https://www.ecured.cu/Criptografía.

[9] GNUPG. Sistemas de cifrado asimétrico. Disponible en: https://www.gnupg.org/gph/es/manual/x212.html

computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos." [10]

"El ciberterrorismo, también denominado terrorismo electrónico, podemos definirlo como la forma de terrorismo que utiliza las tecnologías de información para intimidar, coaccionar o para causar daños a grupos sociales, con objeto de lograr una serie de fines políticos o religiosos." [11.]

En el escenario planteado, es indudable que toda persona u organización que utiliza un sistema de información puede ser una víctima directa o colateral de cibercriminales que actúen en nombre propio o a nombre servicios de inteligencia de algún país en particular.

El comportamiento de grupos extremistas o radicales alrededor del mundo ya no es comparable a sus homólogos del pasado, puesto que ahora están provistos de talento humano reclutado de distintas naciones, con sendas habilidades en temas de seguridad informática, desarrollo de software, hacking y saboteo industrial.

En vez de campos de batalla, uniformes o fusiles, el teatro de la guerra se ha traslado al ciberespacio y las armas son las tecnologías de la información y las comunicaciones, que pueden ser usadas para el espionaje, robo de información o ciberataques de saboteo que pueden incluso poner en riesgo la vida humana si se dirigen a sectores críticos para la sociedad como instituciones de salud o los servicios públicos.

Ésta ha resultado ser una mezcla peligrosa para la institucionalidad de las naciones a las que se oponen pues pueden comprometer seriamente su infraestructura tecnológica.

[10] Pollitt, M, Mark. "Cyberterrorism - Fact or Fancy?" FBI Laboratory. Internet. Disponible en: http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

[11] Urueña Centeno, Francisco J. 2015. Ciberataques, La Mayor Amenaza Actual. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

5. MARCO HISTÓRICO

5.1 ANTECEDENTES

A continuación, se muestra una línea histórica de la evolución que ha tenido el modelo de criptovirus Ransomware a través del tiempo, pudiendo visualizar el perfeccionamiento de sus métodos de ataque y variantes de la amenaza.

Le empresa vpnMentor, que desarrolla soluciones de seguridad informática, publicó un artículo en donde realiza un recorrido por los principales incidentes asociados al ransomware, sus características y la forma que como logró convertirse en una de las mayores amenazas del presente siglo.

Para empezar, hay de trasladarse al año de 1989 cuando un académico de Harvard llamado Joseph Popp, distribuyó alrededor de 20.000 disquetes a varios países y en una conferencia sobre SIDA, con un archivo ejecutable que, una vez ejecutado se instalaba en el equipo y después de 90 reinicios realizaba un cifrado de archivos y ocultamiento de directorios, a cambio de enviar por correo postal un pago se $ 189 dólares.

En el año 2005 nace GPCoder, un criptovirus capaz de cifrar una gran cantidad de extensiones de sistemas Windows, además de eliminar los ficheros originales.

En 2009 se comienzan a ver los primeros vestigios de una estrategia económica detrás de la amenaza ransomware. “Vundo” fue un virus que coaccionaba a sus víctimas para que compraran un antídoto para desbloquear sus datos.

Por el año 2011, surge “WinLock” que se caracterizaba por ser un bloqueador de pantalla y no un cifrador de archivos. Este virus funcionaba bloqueando el acceso a la computadora con un falso mensaje indicando que se había detectado fraude y que se debía llamar a un número internacional para resolver el problema. El engaño estaba en que la llamada ocasionaba un alto cobro en la factura telefónica de la víctima a favor de atacante.

En el 2013, hay un antes y un después en la historia del ransomware con la aparición de Criptolocker, una variante que incorporaba una de las más avanzadas técnicas de cifrado que es RSA de 2048 bits con clave pública y privada para infectar distintas

extensiones de archivos. Esta fuerza de cifrado hace casi imposible pensar en una recuperación unilateral de los datos cifrados.

En 2014, el ransomware se traslada a dispositivos móviles con variantes como Sypeng que bloqueaba la pantalla del dispositivo con un mensaje falso del FBI pidiendo $200 dólares para el desbloqueo.

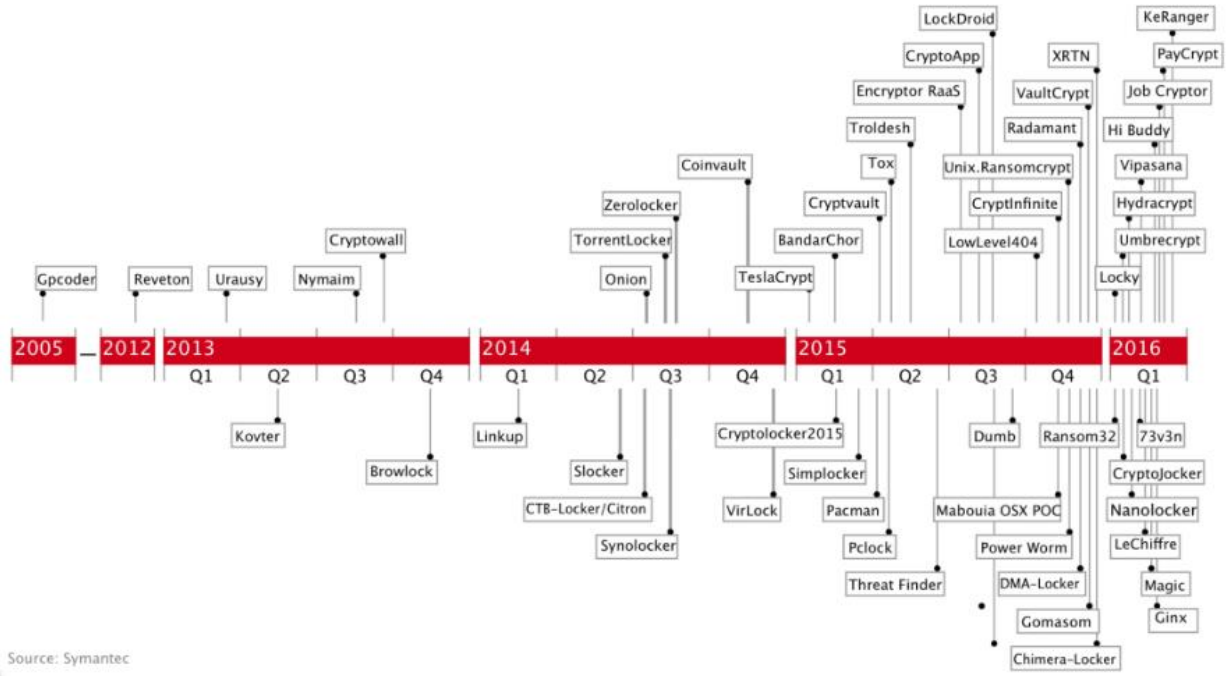
En el 2016, la amenaza sigue su evolución con virus como “Criptowall” que transformó una de sus antiguas versiones añadiéndole funcionalidades como la capacidad de registrarse en el inicio del sistema para ejecutarse con cada reinicio.

En el año 2017, surge el tristemente célebre “WannaCry” un gusano ransomware que inició infectando computadoras en España, expandiéndose en cuestión de horas a docenas de países desde los que pudo obtener alrededor de 500.000 dólares en ganancias por extorsión. Este ataque se convirtió en el peor de toda la historia. [12]

Cuando se observa esta línea temporal con gráficas como la publicada por la empresa de seguridad Symantec en la figura 1, se puede ver un crecimiento exponencial de las variantes de criptovirus diseminadas por la Internet con un nivel de sofisticación cada vez mayor, con ataques direccionados especialmente a la obtención de rédito económico que potencialmente esté financiando nuevas campañas de ciberataques u otras actividades ilícitas.

[12] VPNMENTOR**.** Historia de la amenaza conocida como Ransomware: pasado, presente y futuro. Disponible en: https://es.vpnmentor.com/blog/historia-de-la-amenaza-conocida-como-ransomware-pasado-presente-y-futuro

Figura 1. Línea temporal de surgimiento de Ransomwares hasta 2016



Fuente: Symantec

Hay varios factores determinantes en el éxito obtenido por esta amenaza. Uno de ellos es el surgimiento de las tecnologías de anonimato en la red como las redes Onion y TOR que, si bien han mejorado la privacidad de los usuarios, también ha servido de escondite para el accionar de los cibercriminales que las usan para evitar que se rastreen sus transacciones con criptomonedas y los orígenes de sus ataques.

Otro elemento es la automatización de los ataques que, por medio de botnets y sistemas inteligentes pueden buscar autónomamente a las potenciales víctimas y realizar el ataque sin intervención humana. La capacidad de autoreplicación de los criptovirus elevó su potencial destructivo por el amplio radio de acción que pueden alcanzar.

Resulta alarmante también la inconsciencia por parte de usuarios y empresas en temas de seguridad de sus sistemas aun a pesar de la contundencia de la ola de ataques de 2017 con WannaCry. No se instalaron los parches de seguridad ni se tomaron en serio la necesidad de implementar controles adicionales a sus redes para detectar la ocurrencia de un incidente.

Por lo visto, aún la sociedad está lejos de librarse de un posible secuestro de datos. Las técnicas siguen perfeccionándose para adaptarse a los nuevos dispositivos forzándolos a revelar sus vulnerabilidades, a la par del desarrollo de nuevos métodos de encriptación y de malwares con propiedades de ocultamiento que los hagan invisibles a los sistemas antivirus.

Las pequeñas, medianas y aún las grandes empresas deben acabar por completo con el uso de sistemas obsoletos que persisten en muchas de sus áreas de trabajo, sistemas operativos desactualizados y sin soporte y promover una cultura organizacional que se tome en serio la seguridad de sus datos como un activo que proteger y en el que deben invertir lo necesario.

6. MARCO LEGAL

El congreso de la república de Colombia realizó ajustes al código penal tipificando delitos informáticos en el año 2009. Para ello se creó un nuevo bien jurídico denominado “de la protección de la información y de los datos” en busca de preservar los sistemas basados en el uso de las tecnologías de información y de las comunicaciones.

La ley 1273 del 5 de enero de 2009 contempla una serie de penas privativas de la libertad y sanciones económicas para quienes sean hallados culpables de sabotear, dañar, obstaculizar o acceder ilegalmente un sistema informático además de contemplar algunos agravantes que aumentarían eventualmente la pena principal.

A continuación, se presenta el compendio de artículos de la mencionada ley que estarían relacionados en su mayoría a la comisión de un ataque por ransomware:

“De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático: El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269D: Daño Informático: El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso: El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales: El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito. Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.” [13]

[13] Congreso de Colombia. 2009. Ley 1273 de 2009. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

7. DISEÑO METODOLÓGICO

El presente trabajo se ha centrado en reunir evidencia documental de ámbito tecnológico y noticioso concerniente a la amenaza Ransomware con el objeto de realizar un análisis cualitativo y en base a este análisis producir un manual práctico de prevención y control que resulte de utilidad para la PYMES en nuestro país.

Se ha usado un método descriptivo y analítico del contenido recabado concerniente a la historia y evolución de las criptoamenazas, además de realizar un análisis de casos de distintos tipos de ciberataques a organizaciones en diversos lugares del mundo que ejemplifican el potencial destructivo de los ataques informáticos de este tipo. Gracias a esta conceptualización y referenciación se diseña una guía concreta de prevención, control y recuperación de ataques.

Se obtuvo material principalmente de fuentes electrónicas, sin embargo, también hay un aporte proveniente de la experiencia personal del autor en relación con el enfrentamiento al ransomware en un entorno de producción.

7.1 Fases del diseño metodológico

Figura 2. Fases del diseño metodológico

Fuente: Autor

8. VARIANTES DE RANSOMWARE

Existen al menos 3 variantes principales de esta clase de amenaza, descritos por la empresa de seguridad ESET que, en los últimos años ha hecho un esfuerzo importante por informar y capacitar a sus clientes y al público en general sobre el ransomware y sus formas de prevenirlo:

En su "Guía del Ransomware" exponen los principales tipos de criptovirus identificados hasta el momento:

8.1 LOCKSCREEN

"El ransomware de tipo lockscreen se caracteriza por impedir el acceso y el uso del equipo mediante una pantalla de bloqueo, imposibilitando cualquier acción para cerrarla, abrir el administrador de tareas, los navegadores web o cualquier otra parte del sistema. En esta pantalla típicamente se muestra un mensaje donde se explica lo ocurrido y se solicita el pago de un rescate.

Cryptolocker, CTB-Locker y TorrentLocker son los más resonantes. Estas variantes son detectadas por los productos de ESET bajo el nombre Win32/FileCoder.

8.2 CRYPTOLOCKERS

El ransomware de tipo criptográfico, por su parte, utiliza diversos algoritmos de cifrado para bloquear el acceso a los archivos del usuario. Una vez que se apodera de un sistema, se inicia el cambio en la estructura de los archivos y documentos, de manera tal que solo se podrán volver a leer o utilizar tras restaurarlos a su estado original, lo cual requiere del uso de una clave conocida únicamente por los ciberdelincuentes. En la mayoría de los casos, el ataque afecta solo a ciertos archivos, siendo los de ofimática los más comúnmente perjudicados." [14]

[14] ESET. Guía de Ransomware. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/10/guia-ransomware-eset.pdf

8.3 PARA DISPOSITIVOS MÓVILES

En los dispositivos móviles, se encuentra que los vectores de infección suelen provenir de sitios no oficiales de descarga y foros. Los virus se camuflan dentro de aplicaciones que simulan ser versiones gratuitas de otras apps reconocidas, con tal de llamar la atención. Estas apps prometen todo tipo de cosas como trucos, cambiar la apariencia del dispositivo o juegos ilimitados.

La clasificación que se ha visto es genérica y engloba las distintas modalidades de ataque del ransomware. Pero, en resumen, su objetivo final no es más que impedir a un usuario acceder a sus objetos digitales de valor sea que estos se encuentran en un PC, en un servidor local, en un celular o incluso en la nube.

Cada tipo de ataque está dirigido a un perfil específico de víctima para poder obtener el mayor beneficio posible en términos extorsivos. En el caos de las empresas se suelen ubicar los servidores donde están almacenadas bases de datos y en las computadoras personales se encriptan habitualmente los documentos y archivos multimedia.

Se ha descubierto también, que los propagadores de estos virus intentan esconder su código malicioso en la parte más profunda del código fuente la aplicación, de tal manera, que resulte indetectable para los controles de las tiendas de aplicaciones simulando por fuera ser una app inofensiva, para luego activarse el virus una vez se encuentre instalado en el dispositivo de la víctima.

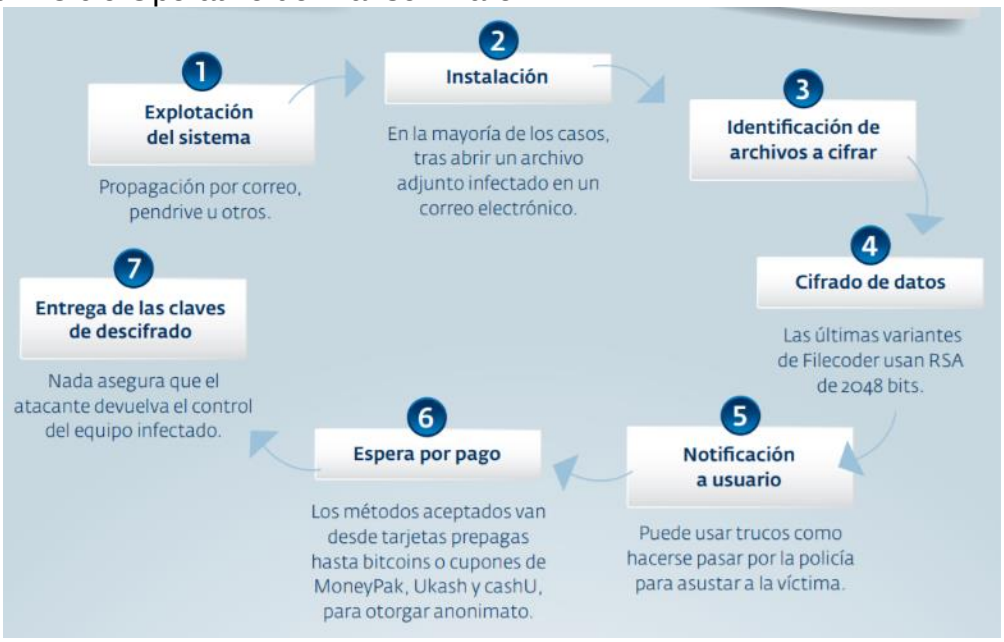
El código oculto pude estar incluso cifrado de forma que es muy difícil detectarlo por parte de sistemas automatizados o antivirus. Por ello es recomendable siempre, evitar utilizar aplicaciones que no sean necesarias y que no provengan de fuentes confiables aun cuando aparenten ser útiles al usuario.

9. MODUS OPERANDI

En este apartado se detallará el paso a paso del accionar del malware Ransomware iniciando con sus métodos de explotación de vulnerabilidades hasta su final incierto de desbloqueo de los datos.

Para empezar, se ilustra a continuación el ciclo de acción del malware:

Figura 2. Ciclo Operativo del Ransomware



Fuente: https://empresas.eset-la.com/archivos/novedades/34/ESET-Ransomware-final.pdf

9.1 EXPLOTACIÓN DEL SISTEMA

Es el paso inicial del ataque, que consiste en el aprovechamiento de las vulnerabilidades de un sistema para conseguir implantar el malware de forma que no se detectado por los sistemas de defensa y posteriormente su auto propagación por los demás equipos de la red de datos.

Es conocido que la plataforma con mayor número de ataques es el sistema operativo Windows, por lo que es beneficioso estudiar el caso de la variante

WannaCry que fue capaz de infectar a miles de computadoras alrededor del mundo en solo unas horas. Esta variante fue particularmente dañina dada su capacidad para extenderse por toda la red de la organización o a través de Internet hacia otras organizaciones. Esta característica le da el calificativo de gusano o “Worm”.

Una de las cosas que más llamó la atención sobre este gusano, era que estaba explotando una vulnerabilidad crítica que había sido corregida por Microsoft 2 meses antes de la oleada de ataques. Este fallo de seguridad se conoció como “EternalBlue” y fue filtrada por un grupo de hackers que dijo a su vez que los organismos de inteligencia de Estados Unidos conocían de ella con mucha anterioridad, pero no habían alertado al público para poder realizar labores de espionaje cibernético.

“¿Qué es EternalBlue?: es el nombre de un exploit de una vulnerabilidad en el Implementación de Windows del Bloque de mensajes del servidor (SMB) protocolo (CVE-2017-0144). La vulnerabilidad fue el resultado de un defecto que permitió a un atacante remoto ejecutar arbitrariamente codificar en una computadora específica enviándola datos especialmente diseñados paquetes

El exploit fue supuestamente desarrollado por la ecuación cyber grupo de espionaje, pero fue parte de un tesoro de datos adquiridos por un misterioso grupo conocido como Shadow Brokers, que comenzó filtrando los datos en agosto de 2016. Hasta la fecha ha habido cinco fugas separadas y EternalBlue fue lanzado como parte de la mayor parte filtración reciente, el 14 de abril de 2017.

La vulnerabilidad fue reparada por Microsoft el 13 de marzo. 2017 (MS17-010), un mes antes de que se filtrara EternalBlue. Sin embargo, una cantidad significativa de computadoras sin parches permanecieron y fueron expuestos al exploit.” [15]

Queda en evidencia, por tanto, que las vulnerabilidades explotadas por estas aplicaciones son conocidas por agencias gubernamentales como explois “0-day” que son fallos de seguridad que conocen muy pocos y para los que no han diseñado

[15] Symantec. 2017. ISTR July 2017 Contents Executive summary and Key findings Ransomware: An overview A new breed of threat. Disponible en: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf. Pág. 9.

parches. Pueden costas millones de dólares conocerlos y pueden ser usados con fines políticos bajo la excusa de seguridad nacional o como arma ciber terrorista.

La siguiente línea de tiempo muestra cómo una debida gestión de las actualizaciones de seguridad puede evitarnos grandes dificultades:

Figura 3. Línea de tiempo de surgimiento de WannaCry

Fuente: https://www.welivesecurity.com/la-es/2017/05/16/check-eternalblue-pc-parcheada-wannacry/

El malware fue detenido de una manera curiosa. Por medio de un procedimiento llamado “Kill Switch” cargado en su PayLoad y que fue descubierto por un investigador llamado “@MalwareTech”, quien observó que el gusano hacía una petición HTTP a una dirección IP en internet sin registro, petición que al fallar le daba la orden al virus de ejecutar el cifrado de los archivos. Al percatarse que el dominio al que hacía referencia no estaba registrado, procedió a registrarlo por solo 10.69 dólares logrando de esta manera que las solicitudes fueran respondidas positivamente, bloqueando de esta manera la ejecución del código malicioso.

Después de haber sido develado el fallo de seguridad de Windows, Microsoft lanzó una actualización para parchear el agujero bajo el código “MS17-010” que podía incluso instalarse en versiones de Windows ya descontinuadas y sin soporte oficial, y aun así existe un número alto de equipos alrededor del mundo que siguen sin instalar dicha actualización.

Sin embargo, “el principal método de propagación es a través de troyanos en sitios web malintencionados o legítimos que han sido comprometidos por los cibercriminales. Las vías de infección más habituales son las páginas web con contenido pornográfico o de juegos, de modo que, cuando los usuarios seleccionan

alguno de los anuncios, se le redirige a otra página comprometida que les infecta con ransomware u otro malware.” [16]

Otros métodos usados comúnmente por los ciberdelincuentes, son las redes P2P, los correos basura o cualquier programa de mensajería que pueden ser usados para diseminar enlaces que, al seguirlos, conducen a sitios web adulterados o contaminados con malware que podrían contener ransomware u otro tipo de amenaza.

El protocolo de escritorio remoto también ha sido una herramienta para acceder por medio de alguna vulnerabilidad específica de este protocolo o por fuerza bruta, y de esta forma encriptar servidores por los que pueden eventualmente pedir cifras de dinero a cambio de devolver su información.

9.2 INSTALACIÓN

La instalación del malware se produce cuando se le otorga permisos de usuario a la aplicación infectada, permitiendo que esta realice cambios en el equipo o se instale en ubicaciones del sistema desde las que tiene acceso a archivos de programa o documentos.

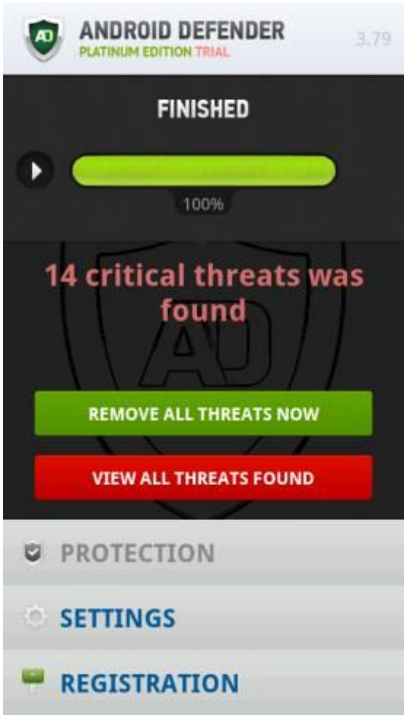
Normalmente esta asignación de privilegios al malware, la realizan los mismos usuarios del sistema de forma desprevenida, siendo engañados por publicidad atractiva creada para persuadir a incautos para que instalen aplicaciones con apariencia inofensiva o con ciertas utilidades que ocultan lo que en segundo plano está sucediendo, que es la instalación de código malicioso muchas veces indetectable a los antivirus comunes.

Los sistemas operativos de dispositivos móviles no se escapan a esta amenaza, “Un ejemplo de este tipo de ransomware es el Android.Fakedefender, un troyano que muestra falsas alertas de seguridad en un intento de convencer al usuario de pagar por la versión completa de la aplicación con el fin de eliminar el malware inexistente.”. [17]

[16] Infodasa**.** Ransomware: Métodos de infección, protección y recuperación. http://www.infodasa.com/web/newque sDetails.php?id_section=115&id=91

[17] INCIBE. David Cantón. 2014. Ransomware IV: Métodos de infección, protección y recuperación. Disponible en: https://www.incibe-cert.es/blog/ransomware-infeccion-proteccion-recuperacion

Figura 4. Captura de Android.Fakedefender



Fuente: Symantec

Los métodos de instalación o infección van variando a medida que surgen nuevos servicios. Por ejemplo, hay una versión de ransomware que afecta a los equipos con el servicio Team Viewer por lo que con cada nueva herramienta informática que utilice servicios de internet desde nuestros equipos debemos tomar medidas de prevención e investigar sus vulnerabilidades.

Otro método que ha resultado muy efectivo para infectar a incautos es por medio de mensajes de correo electrónico que suelen identificarse como provenientes de entidades del gobierno como la oficina de impuestos o incluso de la policía, en los que se advierte de alguna presunta irregularidad por la que será procesado a menos que siga las instrucciones que anexan.

A estos correos los delincuentes adjuntan un archivo con extensión ".pdf" o cualquier otra conocida para que la víctima lo abra en busca de mayor información y a la vez ejecute el malware que viene oculto en el archivo. Un ejemplo es el siguiente:

Figura 5. Correo con ransomware

Asunto: Errores en su Declaracion de Renta
Fecha: 26 Mar 2017 01:31:02 -0400
De: Agencia Tributaria <Tributos@mail.magclinic.com>
Para [redacted]

Estimado contribuyente,

Se han dectedado irregularidades en su declaración jurata de Renta correspondiente al 2016. Adjunto a este mensaje va su factura con la deferencia que debe abonar. En caso de no realizar el pago en fecha puede incurrir en cargos y multas extras.

Que tenga un buen día!

Agencia Tributaria
Av. de España, 8, 02002 Albacete. España.

_____ Alerta de ESET Internet Security, versión de la base de firmas de virus 15154 (20170327) _____

Alerta, ESET Internet Security ha encontrado las siguientes amenazas en este mensaje:

Factura.doc - VBA/TrojanDropper.Agent.UT Troyano - eliminado
Factura.doc = ZIP = word/vbaProject.bin - VBA/TrojanDropper.Agent.UT Troyano - eliminado

http://www.eset.com

Fuente: https://www.elconfidencial.com/tecnologia/2017-04-04/factura-timo-ciberataque-internet-seguridad-informatica_1360047/

9.3 IDENTIFICACIÓN DE ARCHIVOS A CIFRAR

"Como primera medida el malware se instala (generalmente en la carpeta Mis Documentos) otorgándose un nombre aleatorio, para luego crear una entrada en el registro de Windows y así poder activarse en caso de que el equipo se apague. Una vez concretado lo anterior, intenta conectarse a los servidores donde se aloja su centro de control.

En la mayoría de los casos son equipos previamente atacados, a los cuales los atacantes mantienen el acceso sin que sus dueños estén enterados. De esta manera mantienen el anonimato en caso de ser rastreados." [18]

El virus lo que hará básicamente es encontrar las ubicaciones clave que contienen generalmente los archivos de valor para el usuario que pueden estar diferenciados de acuerdo al perfil de la víctima pues en el caso de usuario comunes pueden ser solo archivos generados por aplicaciones ofimáticas y en el caso de equipos

[18] VHGROUP. 2017. Ransomware: secuestro digital. Disponible en: https://www.vhgroup.net/wp-content/uploads/2017/05/Articulo-Ransomware.pdf

corporativos podría atacar archivos de bases de datos como accde, db2, fxp, mdb o ndf o de copias de seguridad tales como .bak.

Extensiones .jpg, .gif, .bmp, .png, .doc, .pdf, .docx, .txt, .mp4, avi, . mkv, son algunas de las más apetecidas a la hora de cifrar archivos puesto que son los que suelen contener información valiosa para el usuario común sea de índole personal o profesional. Al estar ante la posibilidad de perder años de recuerdos fotográficos o fílmicos muchas personas entran en pánico y resuelven ceder ante las pretensiones de los criminales.

9.4 CIFRADO DE DATOS

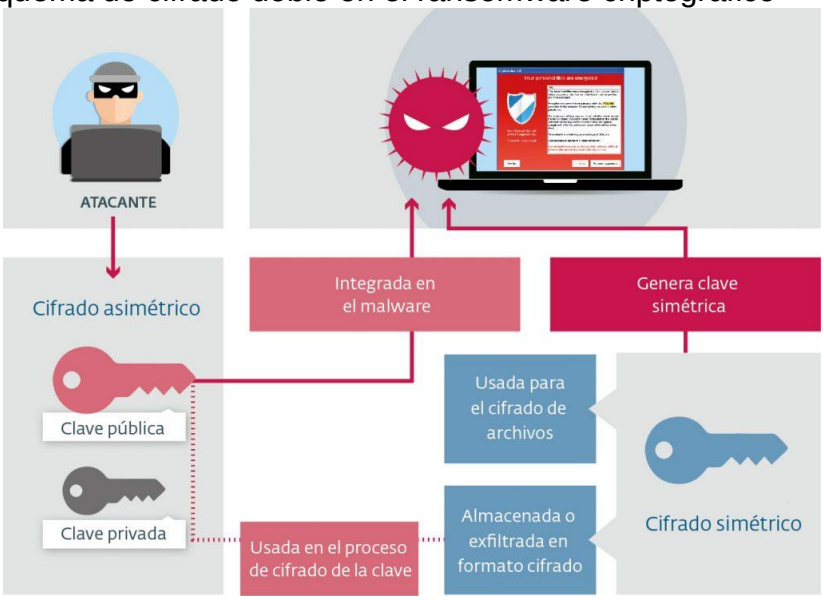
"Una vez que el ransomware criptográfico se apodera de un sistema, se inicia el cambio de los archivos o las estructuras críticas del sistema de manera tal que solo se podrán volver a leer o utilizar tras restaurarlos a su estado original. Esto requiere el uso de una clave conocida únicamente por los delincuentes que operan el malware." [19]

El cifrado asimétrico se basa en operaciones matemáticas sencillas en un sentido, pero muy complejas en sentido inverso. Las claves pública y privada se crean al mismo tiempo y esta relacionadas de tal forma que una es la llave de la otra, pero resulta extremadamente difícil determinar el tipo de relación por parte de la víctima del cifrado.

El modo de operación que suele emplearse es, utilizar el cifrado simétrico para encriptar los archivos y el cifrado asimétrico para proteger la llave privada. De este modo, la llave pública puede venir incorporada en el malware o se obtiene desde un servidor de comando y control, para que, una vez terminado el ataque, se proceda a encriptar la llave privada utilizada y enviarla al atacante para su almacenamiento.

[19] ESET. Cómo y por qué el cifrado moldeó al ransomware criptográfico. Disponible en: https://www.welivesecurity.com/la-es/2016/09/13/cifrado-ransomware-criptografico/

Figura 6. Esquema de cifrado doble en el ransomware criptográfico



Fuente: https://www.welivesecurity.com/la-es/2016/09/13/cifrado-ransomware-criptografico/

9.4.1 Cifrado AES. "Advanced Encryption Standard (AES) es uno de los algoritmos de cifrado más utilizados y seguros actualmente disponibles. Es de acceso público, y es el cifrado que la NSA utiliza para asegurar documentos con la clasificación "top secret".

La diferencia entre AES-128, AES-192 y AES-256 finalmente es la longitud de la clave: 128, 192 o 256 bits - todas las mejoras drásticas en comparación con la clave de 56 bits de DES. A modo de ilustración: El agrietamiento de una clave AES de 128 bits con un superordenador de última generación tomaría más tiempo que la presunta edad del universo." [20]

9.4.2 Cifrado RSA

"A diferencia de los sistemas tradicionales de cifrado simétrico, RSA trabaja con dos claves diferentes: una pública y una privada. Ambos trabajan complementarios entre sí, lo que significa que un mensaje cifrado con uno de ellos sólo puede ser

[20] BoxCryptor. Cifrado AES y RSA, Disponible en: https://www.boxcryptor.com/es/encryption/

descifrado por su contraparte. Dado que la clave privada no puede calcularse a partir de la clave pública, ésta está generalmente disponible para el público.

Estas propiedades permiten que los criptosistemas asimétricos se utilicen en una amplia gama de funciones, como las firmas digitales. En el proceso de firma de un documento, una huella digital cifrada con RSA, se adjunta al archivo, y permite al receptor para verificar tanto el remitente como la integridad del documento. La seguridad de RSA se basa principalmente en el problema matemático de la factorización entera. Un mensaje que está a punto de ser cifrado se trata como un gran número." [21]

Los anteriores son los algoritmos de encriptación más utilizados por los criptovirus modernos, que como se puede ver son tecnologías que son empleadas con fines legales como la protección de documentos oficiales o la ´transmisión de certificados digitales en la red.

Sin embargo, tienen un poder que, en las manos incorrectas puede causar mucho daño como efectivamente lo han hecho con los malware de secuestro de datos que han aumentado el número de bits de encriptación para evitar que en un futuro cercano se puedan descifrar las claves de que utilizan y seguir obligando a las víctimas a ceder a sus pretensiones económicas.

9.5 NOTIFICACIÓN A USUARIOS

Cada variante de malware presenta un método distinto de notificación, aunque en términos generales poseen la misma estructura.

Figura 7. Notificación de Ransomware Wanna DecryptOr 2.0

[21] Ibid.

Fuente: https://www.juancmejia.com/temas-varios/solucion-para-el-virus-wanna-cry-conozca-que-es-y-como-limpiar-el-malware-tipo-ransomware/

Como se puede observar en la Figura 6. En primer lugar, informa a la víctima qué ha ocurrido con sus archivos diciéndole que sus fotos, videos, documentos, bases de datos y otros tipos de archivos han sido encriptados de manera irreversible si no se cuenta con una clave privada para el descifrado.

En segundo lugar, el atacante informa que sí puede recuperar sus archivos, pero tendrá que pagar y deberá hacerlo antes que acabe un tiempo determinado que pueden ser horas o días, de lo contrario amenazan con dejar sus archivos inservibles permanentemente. El pago normalmente se efectúa por medio de la red TOR en sitios especializados en criptomonedas que debido al anonimato que proveen a los dueños de estas cuentas son el escondite ideal para permanecer fuera del alcance de las autoridades.

En tercer lugar, señalan el mecanismo de pago que deberán surtir, facilitando un link que dirige a la víctima a una llamada cartera de BitCoin u otro tipo de criptomoneda en la que se le exige que deposite unos fondos especificados en dólares o en moneda virtual.

En ocasiones no emplean ventanas tan elaboradas como las de la figura anterior, sino un simple mensaje de texto plano con la misma información. Estas notificaciones las dejan ubicadas en cada directorio donde han encontrado archivos para cifrar, de tal manera que sean visibles al usuario de forma inmediata.

En el caso de utilizar un cifrado asimétrico, como sucede en la gran mayoría de los casos, también dejarán visible la clave pública que se ha generado para esta víctima en particular y que deberá ser usada para generar el script de desencriptación.

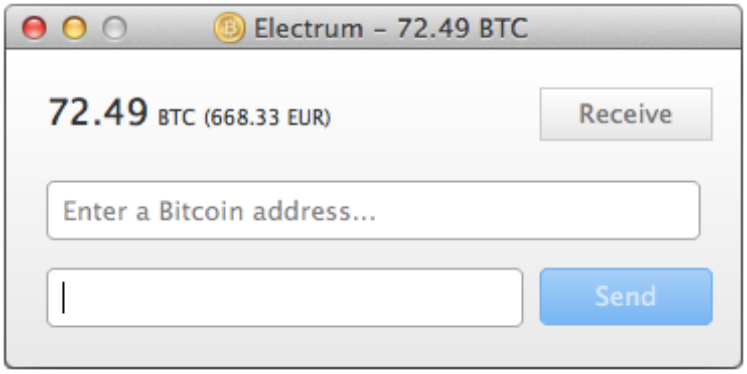
9.6 ESPERA POR PAGO

En esta etapa se el atacante queda a la espera de que la víctima acepte el chantaje y realice el pago que exige. Los métodos han variado desde los inicios de los criptovirus en los que se pedía enviar dinero en efectivo por el correo convencional. Ahora, los delincuentes buscan a toda costa ser rastreados por las autoridades y se refugian en el anonimato que les ofrece la red profunda o “deep web”.

“La razón principal para este éxito del ransomware como un vector de ataque del malware es su eficacia y la capacidad de los cibercriminales para generar dinero. Los servicios de pago anónimo como Bitcoin hacen que los pagos del ransomware sean simples para las víctimas y libres de riesgo para los autores de dicho ransomware. Las empresas incluso comienzan a tener listo un monto de rescate en Bitcoin en caso de que lleguen a ser infectadas y no logren recuperarse del ataque.

Actualmente, Bitcoin continúa siendo el método de pago más popular, pero otras criptomonedas como las más sofisticadas Ethereum y las menos conocidas Litecoin y Dogecoin también son una opción. Las dos últimas monedas han quedado atrás de Bitcoin en términos de transacciones, pero todas estas criptomonedas pueden lavarse fácilmente a través de la red oscura, lo que permite cobrar fondos de forma fácil y anónima.” [22]

Figura 8. Billetera de Criptomonedas



Fuente: https://sl.m.wikipedia.org/wiki/Slika:Electrum_Bitcoin_Wallet.png

La anterior imagen muestra una ventana de la Criptomoneda “Electrum”, en la que se coloca la dirección electrónica de otra billetera y el monto de la cantidad a enviar.

“El gobierno de California decidió darles a los ataques cibernéticos tipo Ransomware el carácter de delito de extorsión, un crimen que atenta contra los derechos universales de la humanidad.

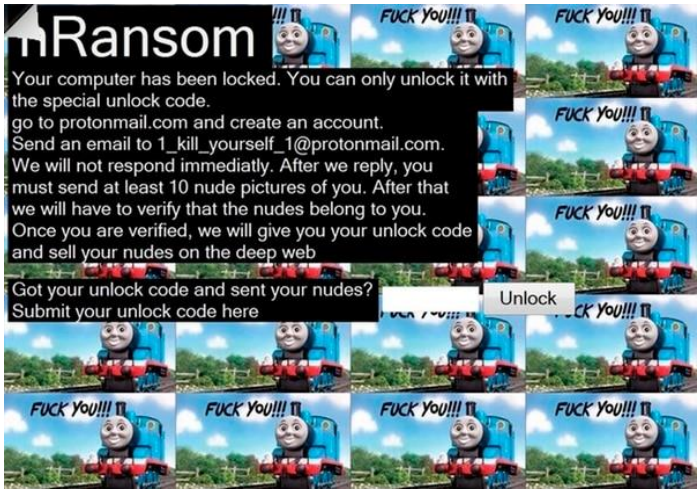
[22] SCOTT-COWLEY, Orlando, 2018. Pagos de ransomware: Financiando el negocio del crimen cibernético, , Disponible en: https://www.veeam.com/blog/es-lat/frequent-methods-for-ransomware-payments.html

La ley SB-1137 fue firmada este martes por el Gobernador Jerry Brown, siendo esta la primera vez que un gobierno extiende la definición de extorsión hasta los ataques ransomware. A partir de ahora, las autoridades podrán lograr sentencias de prisión de 2 a 4 años para aquellos piratas informáticos que desarrollen este tipo de malware o lo propaguen en la red." [23]

Es importante anotar que existe otro medio de pago distinto al económico exigido por algunas variantes de ransomware como el llamado "nRansom", que "como todos los ransomware, el sistema al ingresar al equipo cifra la información y la vuelve inaccesible al usuario.

Pero a diferencia de los demás ransomware, éste no exige un pago económico, sino que la víctima le envíe al menos 10 fotos desnuda, lo que a largo plazo representa una mejor posibilidad para el atacante de poder seguir extorsionando indefinidamente a la víctima aun cuando ya no tenga sus archivos cifrados en lo que se conoce como "sextorsión" o simplemente para ser redistribuidas en internet a través de sitios pornográficos.

Figura 9. Notificación del "nRansom"



Fuente: https://www.infobae.com/america/tecno/2018/08/09/alerta-por-nransom-el-ciberataque-que-secuestran-archivos-y-piden-fotos-de-desnudos-de-rescate/

[23] Infobae, Alerta por nRansom, el ciberataque que secuestra archivos y pide fotos de desnudos de rescate. Disponible en: https://www.infobae.com/america/tecno/2018/08/09/alerta-por-nransom-el-ciberataque-que-secuestran-archivos-y-piden-fotos-de-desnudos-de-rescate/

Por medio de la red anónima TOR que cuenta con su propio navegador se puede acceder a estas billeteras virtuales por lo que el usuario atacado queda en el juego del atacante sacándolo de su zona de seguridad.

Si bien, la pérdida de archivos o bases de datos puede ser frustrante y desastroso para cualquiera, la recomendación de las autoridades sigue siendo no pagar los rescates, puesto que no hay garantías de recibir la clave de descifrado o de que le virus desaparecerá completamente del sistema y no volverá a atacar.

Como se verá más adelante existen contramedidas que pueden ayudar en casos específicos de cifrado para los que se han encontrado sus claves privadas de desencriptación.

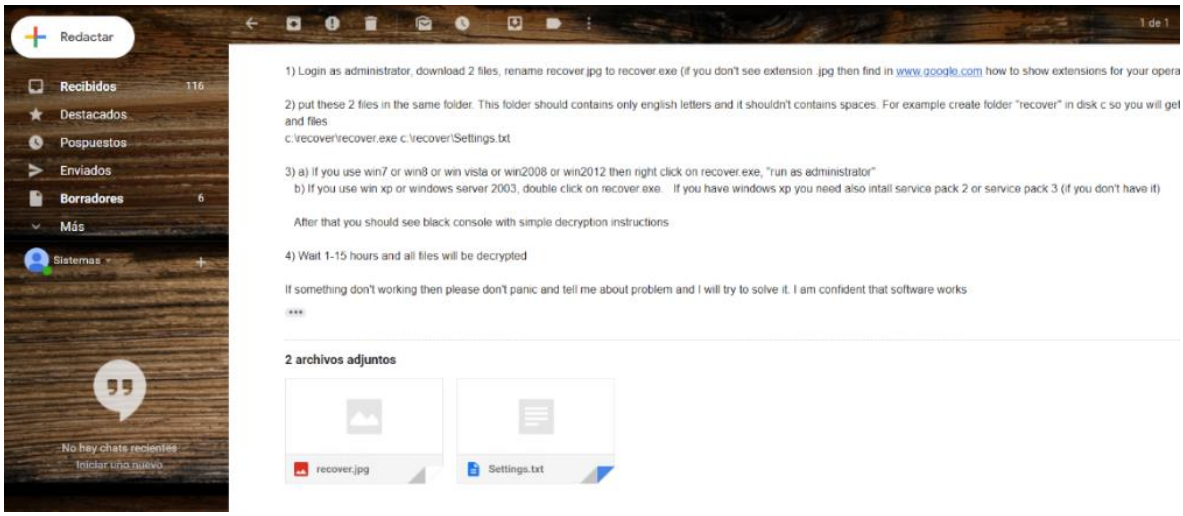
9.7 ENTREGA DE LAS CLAVES DE DESCIFRADO

El método usual para entregar la llave de descifrado es el de ganarse la aprovecharse del temor de la víctima de perder sus archivos y acceder a las pretensiones del atacante. En la mayoría de los casos el mensaje de notificación va acompañado de un correo electrónico que será usado para que la víctima se comunique con el atacante enviándole uno de los archivos cifrados junto con la clave pública que aparece en la notificación, para que éste se lo devuelva descifrado y así constatar que sí se puede recuperar la información.

Luego de que la víctima recibe el archivo desencriptado, llega a sentirse motivado a realizar el pago, que hará por medio de una transacción en línea y de forma anónima. Luego de realizar el pago la víctima notifica al delincuente al correo que se ha realizado el pago.

En este punto, no es posible asegurar que habrá respuesta del atacante puesto que en muchas ocasiones abandonan a la víctima a pesar de haber recibido el pago. Aunque en otros casos, el atacante envía a la víctima un archivo ejecutable con una serie de instrucciones para la desencriptación de los archivos.

Figura 10. Archivos para desencriptar enviados por el atacante



Fuente: Autor

En el caso anterior ilustrado en la figura 10, el atacante envía dos archivos: 1 fichero .jpg y uno .txt con las instrucciones para descifrar los archivos. Entre las instrucciones se especifica que el archivo ".jpg" es en realidad un ejecutable al que hay que cambiar de extensión y ejecutar con privilegios de administrador, lo que, en teoría, puede ocasionar un problema de seguridad puesto que no es posible determinar si este ejecutable contiene otro malware o si creará una puerta trasera para futuros ataques.

10. IMPACTO ORGANIZACIONAL DEL RANSOMWARE

En el año 2017 se identificaron cerca de 1190 variantes de ransomware, lo que representó un aumento del 60 % respecto al año 2016. [24] Esto supone un extraordinario desafío para el sector empresarial que se desarrolla especialmente en los países de más alto impacto del malware.

Las empresas pequeñas, medianas y grandes se han convertido en uno de los objetivos más apetecibles por los atacantes, dado su afán de conseguir recursos económicos o simplemente para hacer más visibles sus actuaciones.

Figura 11. Crecimiento de los ataques en Latinoamérica

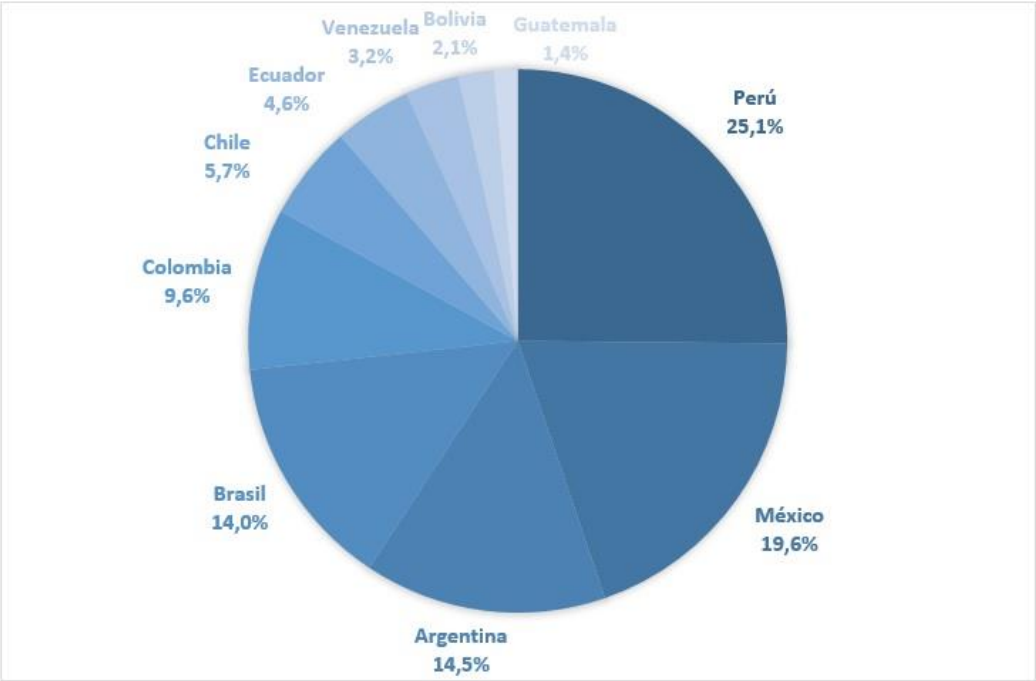
Fuente: https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/

De las 1190 variantes de ransomware identificadas en el 2017, el 33% de ellas tuvo impacto sobre Latinoamérica, lo que revela la fragilidad de la seguridad informática en esta región del mundo y pone de relieve la necesidad de incentivar la modernización de las prácticas tecnológicas en sus organizaciones.

[24] Mendoza, Miguel Ángel. 1 Mar 2018, El impacto del ransomware en Latinoamérica durante 2017. Disponible en: https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/

La primera posición la tiene Perú con un 25.1% del total de ataques, el segundo lugar lo ocupa México con el 19,6% de las detecciones, seguido de Argentina (14,5%), Brasil (14,0%) y Colombia (9,6%). La lista la complementan Chile (5,7%), Ecuador (4,6%), Venezuela (3,2%), Bolivia (2,1%) y Guatemala (1,4%), como los diez países con mayores porcentajes de detección en la región.

Figura 12. Porcentaje de incidencia en Latinoamérica por país



Fuente: https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/

Otros países no aparecen en el gráfico debido a que presentan porcentajes por debajo del uno por ciento, tal es el caso de Costa Rica (0,9%), Panamá (0,9%), El Salvador (0,8%), Honduras (0,7%), Nicaragua (0,5%), República Dominicana (0,5%), Uruguay (0,5%) o Paraguay (0,4%)." [25]

"Se concluyó que el ransomware resulta muy caro para las organizaciones que han sido víctimas de uno de estos ataques. El costo total promedio de un ataque fue de $133,000 – esto incluye el costo del rescate, horas de trabajo perdidas, tiempo de

[25] Ibid.

inactividad, costos de dispositivos y redes, y las oportunidades perdidas. Los ataques más agresivos se volvieron muy caros muy rápidamente: 5% de los encuestados reportaron ataques de ransomware que costaron de $1.3 a $6.6 millones." [26]

El 2017 fue un año crítico para la seguridad de la informática empresarial, teniendo en cuenta que se observó un aumento porcentual de los ataques a empresas en comparación en el año 2016.

10.1 RESEÑA DE LOS PRINCIPALES ATAQUES A EMPRESAS

En junio de 2017 se desató uno de los mayores ataques a nivel mundial registrados por parte de un criptovirus llamado Petya, que irónicamente se aprovechaba de una vulnerabilidad que había sido usada un año atrás por el virus "WannaCry".

Sin embargo, muchas empresas hicieron caso omiso a las recomendaciones de seguridad y no parchearon sus sistemas por lo que quedaron desprotegidos ante esta amenaza. El diario "El Confidencial" de España publicaba la siguiente noticia a mediados de 2017:

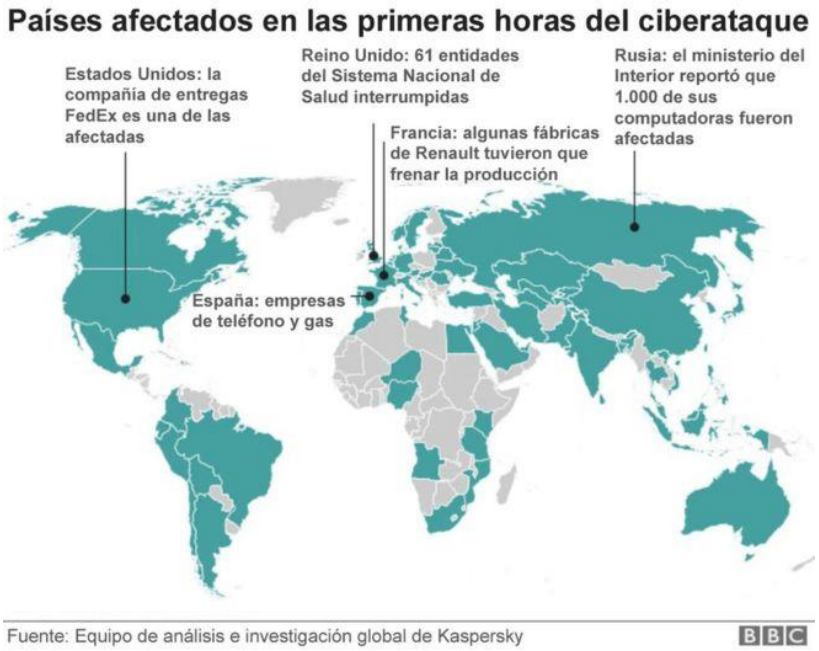
"La empresa de alimentación Mondelez (matriz de empresas como Cadbury y Nabisco y dueña de marcas como Oreo, Chips Ahoy, TUC) y el bufete DLA Piper, una de las mayores firmas legales de todo el mundo, han sufrido esta mañana un ataque de 'ransomware' similar al ocurrido con Wannacry hace apenas un mes. Y no son las únicas. Otras multinancionales, como la danesa Maersk, gigante del sector transporte y logística, la firma de publicidad WPP, la farmacéutica estadounidense MSD (Merck Sharp & Dohme), o Saint Gobain se están viendo afectadas en España y a nivel mundial.

La situación de Maersk ha afectado también al puerto de Barcelona, que se ha visto obligado a cerrar parte de sus instalaciones. APM Terminals, propiedad de Maersk, se ha visto obligada a cerrar su terminal ubicada en el Puerto de Barcelona. El ciberataque ha afectado a 17 terminales de carga de APM en distintos puertos del mundo, entre ellos Rotterdam y Barcelona. Otra de las empresas que opera en

[26] Phillion, Matthew. El Impacto de los Ataques Repetidos de Ransomware. Disponible en: https://gmsseguridad.com/impacto-sophos-ransomware.html

Cataluña y que se ha visto afectada por el ciberataque es Saint Gobain, que fabrica materiales para la construcción.” [27]

Figura 13. Mapa de incidencia del ataque WannaCry en 2017



Fuente: https://www.bbc.com/mundo/noticias-39929920

Como puede observarse gran cantidad de empresas de distintas nacionales y distintos sectores de la economía e incluso entidades gubernamentales vieron afectadas sus operaciones al perder información de días o semanas de trabajo que afectaron en última instancia a los usuarios de sus servicios, algunos de ellos críticos como clínicas u hospitales que perdieron sus servidores de imagenología o historias clínicas de sus pacientes.

El impacto fue monumental teniendo en cuentas que grandes transportadores como Fedex o Maersk disminuyeron sus operaciones de envío de mercancías alrededor del mundo lo que ocasionó retrasos en operaciones de otras compañías que no fueron afectadas directamente por el virus.

[27] C, Otto. Un nuevo ataque de 'ransomware' paraliza grandes empresas en todo el mundo. Disponible en: https://www.elconfidencial.com/tecnologia/2017-06-27/ataque-ransomware-dla-piper-wannacry_1405839/

10.1.1 Trenes alemanes. “Las pantallas electrónicas en las estaciones anunciando llegadas y salidas fueron afectadas, pero los servicios de trenes no se vieron interrumpidos, dijo la compañía ferroviaria Deutsche Bahn.

10.1.2 Hospital de Indonesia. Los pacientes del Hospital de Cáncer de Dharmais no pudieron obtener números para hacer fila y esperaron varias horas, mientras que el personal buscaba registros en papel, informaron medios locales. Los pacientes en el hospital de Yakarta tuvieron que esperar varias horas para ser atendidos.

10.1.3 Policía estatal de India. Los sistemas informáticos de la policía en el estado de Andhra Pradesh fueron golpeados, informaron medios locales. Alrededor de 18 sistemas fueron secuestrados y deshabilitados, informó el diario Business Standard.

10.1.4 Hospitales de Reino Unido. Algunas de las mayores interrupciones fueron causadas por ataques al sistema de salud de Reino Unido. Hospitales y clínicas se vieron obligados a rechazar a los pacientes después de perder el acceso a las computadoras.

Las imágenes en las redes sociales mostraban pantallas de computadoras del National Health Service (NHS) con mensajes que decían: "¡Ooops, tus archivos fueron cifrados!" [28]

Los anteriores reportes de uno de los eventos ciber delictivos más importantes de los últimos años, pone al descubierto una radiografía preocupante de dos realidades que son mayormente las responsables de este tipo de desastres informáticos.

“El ransomware no solo tiene como objetivo usuarios caseros, los equipos usados en la industria también pueden ser infectados, lo que podría generar consecuencias negativas como:

- Pérdida temporal o permanente de información sensible o propietaria
- Interrupción de operaciones
- Pérdidas financieras causadas al restaurar sistemas y archivos

[28] BBC. 2017. Ciberataque masivo: ¿quiénes fueron los países e instituciones más afectados por el virus WannaCry? Disponible en: https://www.bbc.com/mundo/noticias-39929920

- Daño potencial a la reputación de la organización” [29]

La segunda razón es la desatención de las corporaciones a los asuntos de seguridad de sus sistemas de información, que en algunas ocasiones desestiman la inversión de recursos suficientes para la adquisición de tecnología de defensa y de detección de amenazas y en otras ocasiones a pesar de invertir millones en tecnología olvidan que el eslabón más débil de la cadena es el usuario final que cuenta con privilegios innecesarios en sus cuentas, que al final por su descuido son usadas para realizar los ataques desde el interior de la misma red de la compañía.

Es claro que los malware de esto tipo se ensañan contra las organizaciones, puesto que tienen una mayor superficie de exposición, pero principalmente porque en teoría tiene mucho más que perder que un usuario común, por lo que pueden obtener mayores réditos económicos.

Sin embargo, a pesar de acceder a los pagos, muchas de estas empresas se han quedado a espera del descifrado ya que los atacantes nunca más los volvieron a contactar. El pago de las recompensas, según las autoridades, estimula a los delincuentes y los anima a seguir atacando otras empresas continuando el ciclo delictivo.

Las lecciones aprendidas, especialmente de la oleada de ataques del 2017, son muy valiosas para todo el sector empresarial antiguo y el naciente. Todas sin excepción, deben tomarse en serio la seguridad de sus sistemas informáticos, creando un gobierno organizado de su infraestructura, que garantice que sus servicios están protegidos entre otras cosas, con software licenciado y confiable, sistemas antivirus reconocidos y especialmente planes de contingencia bien diseñados y probados para este y otros tipos de desastres.

La gestión de la seguridad informática debe convertirse en un activo por demás valioso para cualquier organización, teniendo en cuenta que el mundo se encuentra ante un escenario que trasciende las limitaciones físicas y con posibilidades casi infinitas. Las empresas deben desarrollar toda una mentalidad enfocada al aprovechamiento de todas las ventajas que ofrecen las nuevas tecnologías de información, siempre de la mano con las medidas de prevención necesarias para mantenerse a flote en un océano plagado de peligros como el ransomware.

[29] Sánchez J, Roberto. Soledad, García Velázquez, Demian Roberto. Boletín de Seguridad UNAM-CERT-2014-011 Crypto Ransomware. Disponible en: https://www.seguridad.unam.mx/historico/vulnerabilidadesDB/index.html-vulne=6521

11. VULNERABILIDADES USADAS POR CRIPTOVIRUS

11.1 RCE EN MSMPENG

"MsMpEng es el servicio de Protección contra Malware que está habilitado por defecto en Windows 8, 8.1, 10, Windows Server 2012 y posteriores. MsMpEng se ejecuta como NT AUTHORITY\SYSTEM sin sandboxing y es accesible remotamente sin autenticación a través de varios servicios de Windows, incluidos Exchange, IIS, etc.

Es decir, un atacante puede acceder a la funcionalidad de mpengine simplemente enviando un mensaje de correo electrónico a la víctima (sin que sea necesario incluso abrirlo), visitando enlaces en un navegador web, por mensajería instantánea, etc." [30]

Parche de Seguridad: "Microsoft la ha considerado tan crítica que publicaron un parche de emergencia incluso para versiones de sus sistemas que ya están por fuera del ciclo de soporte. El parche puede encontrarse en el Microsoft Security Advisory 4022344." [31]

11.2 ETERNALBLUE

"EternalBlue aprovecha una vulnerabilidad en la implementación del protocolo Server Message Block (SMB) de Microsoft. Esta vulnerabilidad, denotada como CVE-2017-0144 en el catálogo Common Vulnerabilities and Exposures (CVE), se debe a que la versión 1 del servidor SMB (SMBv1) acepta en varias versiones de Microsoft Windows paquetes específicos de atacantes remotos, permitiéndoles ejecutar código en el ordenador en cuestión." [32]

---

[30] Motos, Vicente. ¿Cuál ha sido la vulnerabilidad que ha explotado el ransomware que ha puesto en jaque a Telefónica y a otras grandes compañías? Disponible en: https://www.hackplayers.com/2017/05/cual-ha-sido-la-vulnerabilidad-del-ransomware-de-telefonica.html

[31] Microsoft. Microsoft Security Advisory 4022344, Disponible en: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2017/4022344

[32] ESET North America. Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN, Disponible en: http://support.eset.com/ca6443/?locale=en_US&viewlocale=en_US

Parche de Seguridad: Instalar la actualización de seguridad MS17-010 de Microsoft para resolver esta vulnerabilidad.

11.3 REDES PEER TO PEER P2P

Estar conectado a una red P2P puede convertir su computadora en un bot que puede recibir instrucciones o comandos desde un centro de comando y control por medio de protocolos como IRC o HTTP u otros protocolos P2P especialmente diseñados para esta tarea. Esta estrategia distribuida hace que sea más difícil poder contener un ataque proveniente desde este tipo de redes mientras que convierte su equipo en un propagador potencial de los ransomware.

Parche de Seguridad: No instalar programas de tipo P2P y tener activo un firewall con las medidas mínimas de seguridad para evitar conexiones salientes o entrantes no autorizadas.

11.4 VERSIONES ANTIGUAS DE SISTEMAS OPERATIVOS

“El 7% de los ordenadores mundiales, que todavía funcionan con Windows XP, según datos de la consultora de mercados Netmarketshare. Estos equipos, que también resultaban afectados por Wannacry, dejaron de tener apoyo regular en abril del 2015, pese a las protestas de muchos de sus irreductibles usuarios, para quienes era una de las versiones más agradecidas del sistema Windows. Entonces, la compañía se comprometió a dar actualizaciones críticas hasta el 2020, pero la de Wannacry ha sido la primera en tres años.” [33]

La desactualización de los sistemas operativos, especialmente en entornos corporativos, es una de las variables de más difícil modificación puesto que en muchas ocasiones este problema está asociado al uso de software ilegal que no soporta actualizaciones o que ya incorporan vulnerabilidades de origen.

Muchas pequeñas y medianas empresas rehúsan someterse a un proceso de licenciamiento dado los costos que esto conlleva, priorizando otras inversiones que consideran más rentables o urgentes. Esto las convierte en objetivos informáticos que sólo actúan o mejoran procesos de seguridad de forma reactiva, o en función

[33] Jané, Carmen. 2017. La mitad de los ordenadores mundiales funcionan con sistemas operativos antiguos. Disponible en: https://www.elperiodico.com/es/sociedad/20170522/la-mitad-de-los-ordenadores-mundiales-funcionan-con-sistemas-operativos-antiguos-6054398

de los ataques de los que van siendo víctimas, soportando los altos costos que conlleva la restauración de un sistema atacado.

La inexistencia de un SGSI (Sistema de Gestión de la Seguridad de la Información) es otro factor determinante que aumenta las probabilidades de tener sistemas o equipos sin las debidas actualizaciones o controles preventivos de seguridad. Al no tener personal encargado de probar los parches que producen lo fabricantes, optan por ignorarlos y funcionar con la filosofía “si no está roto, no lo toques”; lo que para efectos prácticos significa continuar con vulnerabilidades implantadas en los sistemas, a pesar de tener el licenciamiento de sus paquetes de software.

Parche de Seguridad: Instalar versiones recientes de sistemas los sistemas operativos y con instaladores directos del fabricante con licenciamiento y soporte de actualizaciones.

11.5 TROYANOS

“Se denomina caballo de Troya, o troyano, a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.” [34]

Aunque este tipo de amenazas no solía tener relación con los criptovirus, ha salido una nueva generación que toma características de ambas como es el caso de “Android LokiBot”. “Los investigadores de la firma de seguridad SfyLabs alertan que es un troyano bancario para Android que se convierte en ransomware en caso de que la víctima intente quitarle los privilegios de administrador.

Se trata de un troyano que tiene como objetivo robar los datos financieros de la víctima. Al igual que otros ejemplos de malware bancario para móviles, esta pieza maliciosa suplanta a las aplicaciones de los bancos, mostrando una pantalla falsa de inicio de sesión para robar las credenciales. Además, está capacitado para suplantar a otras apps, como WhatsApp, Skype o Outlook.” [35]

Parche de Seguridad: Sistemas antivirus y antimalware reconocidos en el mercado.

[34] Panda Security. Troyanos, Disponible en: https://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/trojan/

[35] ComputerHoy. Troyano bancario para Android se convierte en ransomware al eliminarlo. Disponible en: https://computerhoy.com/noticias/moviles/troyano-bancario-android-convierte-ransomware-eliminarlo-70115

12. RANSOMWARE EN SISTEMAS LINUX

Debido a que la mayoría de los equipos que fueron víctimas de la ola de ataques han contado con sistemas Windows, algunas empresas de todos los tamaños, consideraron que los más seguro era tener sistemas basados en Linux especialmente en sus servidores. Sin embargo, los atacantes crearon también variantes capaces de penetrar estos sistemas y encriptar sus sistemas de archivos.

12.1 EREBUS

"Erebus se ha convertido en uno de los ransomware más preocupantes de los que tienen como objetivo a los servidores Linux. El motivo está en lo que le ha pasado a la empresa de hosting surcoreana NAYANA, que vio cómo 153 de sus servidores Linux eran infectados por este malware." [36]

El efecto de este ciberataque fue aún mayor al tener en cuenta que la información de más de 3400 empresas que tenían sus datos alojados en sus servidores, fueron cifrados de paso, aumentando de esta forma el impacto del ataque.

"Utiliza el algoritmo RSA para cifrar las claves AES, cifrando los ficheros con claves AES únicas. Para permanecer en el sistema utiliza un falso servicio de Bluetooth para garantizar su inicialización incluso tras reiniciar el sistema y emplea una rutina cron para verificar cada hora la ejecución del malware. Debido a que el objetivo aquí son las empresas, el rescate en un principio era más alto, de 10 Bitcoints (24.689 dólares), aunque posteriormente bajó hasta los 5 (12.344 dólares).

La variante de Erebus contra Linux infecta un total de 433 tipos de archivo (aunque Linux internamente no trabaja con extensiones como las de Windows), entre los cuales están pptx, docx, xlslx, sql, mbd, dbf, odb, zip, rar, eml, msg, html, css, php, java, avi y mp4." [37]

[36] MEDINA, Eduardo. Erebus, el ransomware para Linux que está causando estragos a muchas empresas. Disponible en: https://www.muyseguridad.net/2017/06/26/erebus-ransomware-linux-empresas/

[37] Ibid.

12.2 SAMBACRY

“Otra variante muy peligrosa se ha descubierto recientemente, se trata de ejecución de código remoto que convivía desde hace 7 años en el software de red Samba. Éste podría permitir a un atacante remoto tomar el control de las máquinas Linux y Unix afectadas.

Samba permite que los sistemas operativos que no sean Windows, como GNU / Linux o Mac OS X, compartan carpetas compartidas de red, archivos e impresoras con el sistema operativo Windows.

La vulnerabilidad CVE-2017–7494 reside en la forma en que Samba maneja las bibliotecas compartidas. Un atacante remoto podría usar esta vulnerabilidad para cargar una biblioteca compartida en un recurso compartido escribible y luego hacer que el servidor cargue y ejecute código malicioso.

La vulnerabilidad es muy fácil de explotar: sólo se requiere una línea de código para ejecutar código malicioso en el sistema afectado: simple.create_pipe("/path/to/target.so")” [38]

El sistema operativo que se conocía por su robustez también es vulnerable al ransomware, lo que propone un gran desafío para los especialistas en seguridad teniendo en cuenta que la mayoría de los servidores en el mundo corren bajo sistemas Unix. Se deben reanudar esfuerzos para detectar oportunamente los agujeros de seguridad en Linux antes que lo hagan los delincuentes y se genere un caos igual o mayor que el de 2017.

[38] SALAZAR, Edgar David, SambaCry CVE-2017–7494. Disponible en: https://blog.guayoyolabs.com/sambacry-cve-2017-7494-permite-a-los-hackers-acceder-a-miles-de-ordenadores-linux-de-forma-remota-b4014ac281d9

14. PROTOCOLO DE CONTROL Y PREVENCIÓN

Según el estudio llamado “Estado Global de Ciberseguridad 2017”, sólo el 53 por ciento de las organizaciones tienen un plan en marcha para enfrentarse a la amenaza ransomware (Isaca, 2017). [39]

Esto pone sobre la mesa una alarmante realidad que es el caldo de cultivo de nuevas oleadas de ataques cada vez mayores, teniendo en cuenta que las lecciones no parecen estar siendo aprendidas por las empresas, quienes siguen viendo el tema de la ciberseguridad sólo en términos de los costos que les genera y a lo intangible del retorno de esa inversión.

Hasta que los consejos de administración no se tomen en serio los riesgos a los que esta expuestos, es muy difícil que se tomen las medidas suficientes para contener un ataque que les puede costar muchas veces más que lo que invertirían en hardware o software para proteger sus datos. Las organizaciones modernas deben madurar con rapidez y desarrollar una filosofía empresarial que le conceda prioridad a la seguridad digital, diseñando una estructura administrativa de gobierno que se ajuste a sus características, pero suficiente para gerenciar la implementación de políticas y controles que disminuyan la superficie de exposición de un ataque, que capacite a los usuarios, que adquiera y administre equipos de seguridad perimetral, entre otras medidas.

“Persuadir a un miembro del personal para que haga clic en un enlace permite al atacante desarrollar una presencia en la red, omitiendo todos los controles del perímetro. Combinado con las redes internas generalmente abiertas, esto permite a los atacantes o al malware buscar a través de la organización, encontrar datos interesantes y exfiltrarlos –o traer el ataque de WannaCry– para causar daño.

Desafortunadamente, no hay bala de plata, por lo que los controles deben ser puestos en capas para ser eficaces.” [40]

[39] Isaca. 2017. STATE OF CYBERSECURITY 2018. Disponible en: https://cybersecurity.isaca.org/state-of-cybersecurity

[40] Rory Aslop. 10 áreas de control para mitigar contra los ataques de malware. Disponible en: https://searchdatacenter.techtarget.com/es/opinion/10-areas-de-control-para-mitigar-contra-los-ataques-de-malware

La multinacional tecnológica CISCO en el año 2017 una serie de recomendaciones que han demostrado ser muy efectivas para mitigar el riesgo de un ataque ransomware, y que coinciden con los consejos de otras empresas de seguridad.

14.1 CONSERVE COPIAS DE SEGURIDAD

"Para reducir el impacto, es necesario mantener una copia de respaldo programada con regularidad. Para ello, se deberá realizar una limpieza del sistema. Cuanto más frecuentemente realice copias de respaldo, menos datos perderá. Todo dispositivo estará cifrado, por lo que el almacenamiento de la información debe ser externo y no conectado al dispositivo después de haberse completado la copia." [41]

Este punto de control es fundamental para cualquier empresa grane o pequeña. Estas deben contar con planes de contingencia diseñados para minimizar el impacto de un secuestro de datos. La recuperación de la información va a depender en gran medida de la frecuencia con que se hagan los backups y de la calidad de estas, puesto que deben ser probadas en ambiente controlados para garantizar que pueden ser restauradas en breve tiempo y soportar la continuidad del negocio.

Las copias de seguridad deben ser un servicio integrado en el plan maestro de seguridad informática de la empresa, debe tener responsables directos y hacérsele seguimiento continuo por parte del gobierno TIC o de un supervisor encargado se esa tarea.

De igual forma deben ser integrales, de tal forma que abarquen la totalidad de la compañía y no solo los ambientes de servicios críticos. Debe incluir los datos de usuarios y operarios de todos los niveles de tal forma que no existan brechas de seguridad que puedan ser aprovechadas por el malware.

14.2 IMPLEMENTAR ESTRATEGIA DE PRIVILEGIOS MÍNIMOS

Es más común de lo que querría, la peligrosa práctica de ofrecer privilegios de usuario innecesarios a usuarios que no lo requieren. Incluso se da el caso en que personal que ya no labora en la empresa sigue teniendo usuarios y privilegios activos que podrían ser usados por terceros para ocasionar daños a los sistemas.

[41] CISCO. 2017. Ransomware: Puntos claves para evitar y combatir sus ataques. Disponible en: https://gblogs.cisco.com/cansac/ransomware-puntos-claves-para-evitar-y-combatir-sus-ataques/

Se requiere que exista una política estricta y restrictiva de asignación de privilegios mínimos a los roles de usuario, pues, aunque esto no evitará que un ataque ransomware ocurra, sí dificultará o evitará que el malware tenga acceso a recursos no autorizados para el usuario afectado conteniendo de esta forma la propagación de la amenaza.

14.3 ACTUALIZACIONES DE SEGURIDAD

Los criptovirus están diseñados para aprovecharse de las vulnerabilidades más comunes en los sistemas operativos de más alta demanda. Por ello, un sistema desactualizado, es un sistema con agujeros de seguridad sin parchear, lo que se traduce en una puerta abierta a la entrada de distintos tipos de malwares.

"Si te haces el hábito de actualizar tu software con frecuencia, reducirás significativamente la posibilidad de convertirte en víctima del ransomware. Algunos fabricantes lanzan actualizaciones de seguridad periódicas de rutina, como por ejemplo Microsoft y Adobe, pero también existen actualizaciones adicionales no programadas para casos de emergencia. Siempre que sea posible, habilita las actualizaciones automáticas, o ve directamente al sitio web del fabricante, ya que a los creadores de malware también les gusta hacer pasar sus creaciones como actualizaciones de software." [42]

14.4 CAPACITAR A LOS USUARIOS

Se ha dicho que por el eslabón más débil es por donde se rompe una cadena. De igual forma, de poco sirve contar con avanzadas tecnologías de seguridad si un usuario desprevenido sigue descargando aplicaciones o documentos sin verificar sus fuentes y visitando sitios web de dudosa procedencia.

"Capacite a sus usuarios sobre situaciones de amenaza de ingeniería social. La trampa más común es de un correo electrónico de suplantación de identidad u otro esquema de ingeniería social. Un empleado puede dejar expuesta su información." [43]

---

[42] Lisa Myers. ESET. 11 formas de protegerte del ransomware, incluyendo Cryptolocker. Disponible en: https://www.welivesecurity.com/la-es/2015/07/08/11-formas-protegerte-del-ransomware-cryptolocker/

[43] CISCO. 2017. Ransomware: Puntos claves para evitar y combatir sus ataques. Disponible en: https://gblogs.cisco.com/cansac/ransomware-puntos-claves-para-evitar-y-combatir-sus-ataques/

Es aconsejable realizar jornadas de capacitación en temas de seguridad que involucre a todos los funcionarios de la empresa, incluso si no opera un equipo de cómputo puesto que puede ser usado para obtener información relacionada a la empresa que sería útil en manos de un atacante.

Debe asegurarse que sus trabajadores no descarguen ningún tipo de archivo desde sus correos personales, no acceder a enlaces no relacionados a la actividad de la compañía, no utilizar aplicaciones que no autorice el departamento de seguridad así parezcan inofensivas, no desactivar por ninguna razón los sistemas antivirus, no conectar ningún dispositivo externo al equipo sin la supervisión de un técnico autorizado.

Es aconsejable también realizar simulacros en los que el departamento de seguridad intente realizar ataques de ingeniería social o de otro tipo a usuarios de su compañía y luego socializarlos para aprender las lecciones necesarias.

14.5 ANALIZAR LOS CORREOS ELECTRÓNICOS

Un consejo muy útil es realizarse las siguientes tres preguntas antes de abrir un correo en particular:

- ¿Conozco al remitente?
- ¿Realmente necesito abrir este archivo o acceder a este enlace?
- ¿Solicité realmente algo de esta empresa?

Lo ideal, es que cada empresa cuente con su propio servicio de correo electrónico, de forma que los usuarios no se vean tentados a utilizar sus correos personales para actividades de la empresa. Además, se obtiene un mejor control sobre el tipo de archivos que pueden o no enviarse o recibirse a través de un e-mail.

14.6 FILTRADO ANTI-SPAM

Es necesario que todo e-mail por muy inofensivo que parezca pase a través de sistemas de detección de spam o correo basura. Esto correos pueden, en ocasiones, resultar engañosos debido a su presentación similar a correos

corporativos y que van acompañados de ficheros o enlaces maliciosos. Se debe recordar que algunas variantes ransomware usan especialmente este medio de propagación como lo es por ejemplo el virus “Locky”.

14.7 PROTEGER LAS REDES DE DATOS

Se recomienda que se configure un sistema de capas de seguridad para las redes de datos internas, lo que se denomina “Defensa en Profundidad”. Con esto se dificulta mucho la tarea de los atacantes teniendo un efecto disuasivo sobre ellos. También, la seguridad multicapa ayuda a ganar tiempo para que sistemas especializados de detección de intrusos logren detectar a tiempo un ataque e informar a los administradores.

Los firewalls tradicionales basados en puertos se están quedando en el pasado y cada vez son más vulnerables ante las técnicas de los hackers. Por ello se aconseja invertir en los llamados Firewall de Próxima Generación o NGFW, que son “capaces de detener los ataques mediante la inspección de tráfico avanzada y la detección y control de aplicaciones y usuario (independientemente de los protocolos/puertos usados). Algunas de sus características principales son:

- Detección y prevención de intrusiones (IPS): Protección contra amenazas de red examinando flujos de tráfico (basado en firmas y en comportamientos anómalos).
- Filtrado web: Protege bloqueando acceso a páginas inapropiadas y/o peligrosas.
- Anti-SPAM: Reduce el volumen de SPAM en el perímetro.
- Anti-Virus: Protección frente amenazas a nivel de contenidos en el perímetro.
- Amenazas Persistentes Avanzadas (APT): Protección frente a APTs mediante el uso de sandboxing (local o en la nube).
- Análisis tráfico encriptado (HTTPS)
- Acceso remoto SSL/VPN” [44]

Además del firewall, se deben implementar sistemas detección de intrusos en red como una barrera de protección adicional.

14.8 SEGMENTAR LA RED

[44] Ingenia. Firewalls de nueva generación. Disponible en: https://www.ingenia.es/es/servicio/firewalls-de-nueva-generacion-ngfw

Se trata de limitar la cantidad de recursos a los que un ciberdelincuente puede acceder. Esto se hace agrupando de manera lógica los recursos y servicios de red evitando que un usuario o equipo puede acceder a servicios que no le corresponden, además de evitar la propagación de malwares, conteniéndolos y facilitando la eliminación de la amenaza.

14.9 MONITOREAR LA RED

Se debe contar con un centro de control y monitoreo de las redes de datos, con personal entrenado para detectar actividad anormal, tráfico sospechoso o conexiones que provenga de lugares o dispositivos poco comunes. Esta es una medida que es fundamental para detectar a tiempo un ataque y evitar su consumación.

14.10 FORTALECER EL CONTROL DE TERMINALES

No es suficiente con tener sistemas antivirus en cada equipo de escritorio. Cada vez es más común que los empleados se conecten a los sistemas de la empresa desde sus propios dispositivos portátiles, por lo que se debe controlar qué clase de dispositivos pueden conectarse y bajo qué parámetros, limitando al máximo los privilegios de navegación de estos mientras estén conectados a la red corporativa.

14.11 DESHABILITAR EL USO DE MEDIOS EXTRAÍBLES USB

Los medios extraíbles como discos duros o dispositivos flash USB son un vector de ataque que debe vigilarse puesto que algunas versiones de criptovirus se han especializado en propagarse por este medio. Lo que se aconseja es elaborar y aplicar una directiva general que impida el uso se medios extraíbles en los equipos de la organización, y exigir el acompañamiento de personal de seguridad informática en caso de requerirse el uso de uno de estos medios.

14.12 AISLAMIENTO DE APLICACIONES (SANDBOXING)

“El aislamiento de aplicaciones es un método de reclusión de aplicaciones para que sólo tengan acceso a un estricto conjunto de recursos que son estrictamente

controlados, como memoria y espacio en el disco. Normalmente, se impide que aplicaciones aisladas puedan ejecutar cambios permanentes en el disco duro." [45]

Este mecanismo ayuda a evitar que el ransomware potencialmente escondido en aplicaciones tenga acceso a la información almacenada o a los recursos compartidos en la red. Cabe anotar que la última versión de Windows "Windows 10 May 2019 Update" provee de una herramienta de sandoboxing que ofrece al usuario la posibilidad de abrir sus ficheros y aplicaciones en un entorno de escritorio ligero de forma segura y aislada del sistema operativo principal. Ninguno de los cambios realizados en este entorno es permanente.

14.13 SHADOW COPYS

A pesar de que algunos ransomware están diseñados para cifrar las copias de volumen Shadow Copy, tenerlas aumenta las posibilidades de recuperar versiones anteriores de los archivos encriptados. El sistema Windows realizar copias de seguridad instantáneas de los archivos dando la posibilidad de obtener una versión de los ficheros anterior a su cifrado.

14.14 CAPTURAS DE MÁQUINAS VIRTUALES

En lo posible se debe optar por migrar la infraestructura total de terminales y servidores de la empresa hacia máquinas virtuales que permiten tener un mejor control de copias de seguridad de los sistemas, así como la restauración de estos en cada cierre de sesión a su estado original.

"La Virtualización de un servidor de infraestructura es bastante común, pero también es posible proteger el servidor contra Ransomware, mediante la toma de capturas instantáneas, a máquinas virtuales, programadas regularmente que pueden permitir regresar el estado de una máquina virtual a un punto previo en el tiempo. Esto puede proporcionar una opción de recuperación alternativa en el caso de que un ataque Ransomware sea realidad." [46]

14.15 PROGRAMA DE LICENCIAMIENTO

Es imprescindible que la suite de software que posea la empresa esté completamente licenciada, porque esto asegura que las instalaciones en los

[45] Christopher M. Frenz & Christian L. Diaz. OWASP. Guía Contra Ataques Ransomware. Disponible en: https://www.owasp.org/images/3/39/Guia_Contra_Ransomware.pdf
[46] Ibid.

equipos no se encuentran comprometidas con “backdoors” o malwares que sirvan de portal a las criptoamenazas.

Es sabido que las distribuciones ilegales de software poseen muchas veces códigos maliciosos capaces de comunicarse de forma inadvertida para el usuario con potenciales atacantes en cualquier parte del mundo. Por ello la importancia de adquirir software legal y con todo el soporte de actualizaciones de seguridad al día.

14.16 CONTAR CON UN SGSI

Los Sistemas de Gestión de Seguridad de la Información o SGSI, es un proceso metodológico, documentado y sistemático, que busca garantizar un alto nivel de protección para los activos de información con los que operan las organizaciones, procurando mantener su confidencialidad, integridad y disponibilidad.

Su objetivo principal es gestionar la información y los sistemas de apoyo, como lo que son, activos de alto valor para la compañía, utilizando para ello estándares internacionales de gestión del riesgo y manuales de buenas prácticas que guíen la implementación de controles precisos y eficaces que eviten la ocurrencia de incidentes indeseados dentro de los que está el ransomware.

Este sistema de gestión procura involucrar a toda la organización desde su alta dirección hasta el último empleado con responsabilidades informáticas en la creación y mantenimiento de una política corporativo de protección, prevención y gestión del riesgo. Anticipándose a las amenazas y minimizando la probabilidad de ocurrencia de un ataque o en todo caso de daños que sean irreparables.

14.17 REALIZAR SIMULACROS

Es muy importante que, las organizaciones realicen pruebas a sus planes de contingencia planificando al menos una vez por año simulacros en los que se genere de forma controlada un escenario de secuestro de datos de un servidor o de equipos clientes previamente preparados.

El personal de la empresa debe haber sido preparado previamente para dar respuesta al incidente activando todos los protocolos previstos en el plan. Esto permitirá medir la efectividad de las acciones de respuesta e identificar posibilidades de mejora que fortalezcan el esquema de seguridad de la información.

15. RECURSOS ANTI-RANSOMWARE

Cuando se trata de defender y proteger los datos bajo su responsabilidad, toda empresa debe contar con una estrategia clara y probada que identifique en primer lugar las vulnerabilidades que sufran sus sistemas por medio de pruebas especializadas de penetración y explotación, además de invertir en herramientas de hardware y software confiables, que ayuden a crear anillos de seguridad alrededor de los sistemas críticos, que tengan poder persuasivo contra el atacante y que sean capaces de detectar y responder ante un posible a ataque.

A continuación, se detallarán algunas de las utilidades más reconocidas del mercado para la prevención de ataques ransomware, herramientas que pueden equipos físicos dedicados o producto de software diseñados para identificar comportamientos potencialmente dañinos y responder ante estos.

15.1 HERRAMIENTAS DE HARDWARE

Una de las herramientas más útiles para contrarrestar la amenaza de ingreso de malware a la infraestructura de red interna, son los Sistemas de Prevención de Intrusos IPS, que básicamente son dispositivos que tienen como objetivo detectar actividades o tráfico sospechoso que circule a través de determinada red de datos, actividades que pueden originarse en equipos internos o externos.

Poseen las siguientes características:

- “La detección de intrusos se realiza comparando las firmas de las actividades sospechosas con las firmas de las actividades ya conocidas y que se incluyen en un fichero de identificadores.

- Para que las tareas de protección contra intrusiones sean efectivas, un sistema IPS debe disponer de un sistema de actualización continuo mediante el cual, el fichero que contiene los identificadores de intrusiones se actualizará en todo momento.

- Un sistema de prevención de intrusos puede estar compuesto por software, hardware o la combinación de ambos elementos.” [47]

[47] Panda Security. ¿A qué se denomina Sistema de Prevención de Intrusos o IPS? Disponible en: https://www.pandasecurity.com/usa-es/support/card?id=31452

Entre las opciones que se hallan en el mercado, se encuentran las siguientes:

- **FortiGate 200E Series**: Se trata de un firewall de nueva generación diseñado por la empresa Fortinet para medianas y grandes empresas, que cuenta con un módulo IPS que puede procesar 2.2 Gbps de datos y Firewall hasta 20 Gbps.

  Su ficha técnica asegura que puede detectar y proteger contra distintas clases de amenazas como malwares, exploits y sitios webs maliciosos usando continuamente los sistemas inteligentes provistos por los laboratorios de seguridad de FortiGuard.

Fig. 14. FortiGate E200 Series

Fuente:https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_200E_Series.pdf

- **Mcafee Network Security Platform NS7350:** Es un sistema de prevención de intrusiones (IPS) de próxima generación que descubre y bloquea amenazas de malware sofisticadas en toda la red. Utiliza técnicas avanzadas de detección y emulación, que van más allá de la mera coincidencia de patrones para defenderse de ataques sigilosos con un alto grado de precisión. [48]

Fig. 15. McAfee NS7350

Fuente: http://amartastore.com/index.php?route=product/product&product_id=2940

- **Cisco Firepower 4110 NGFW Appliance**: El Firewall de próxima generación (NGFW) de Cisco Firepower es el primer NGFW totalmente integrado y centrado en amenazas de la industria. Ofrece una gestión de políticas completa y unificada de las funciones de firewall, control de aplicaciones, prevención de amenazas y protección avanzada contra malware desde la red hasta el punto final.

[48] AmartaStore. MCAFEE NETWORK SECURITY PLATFORM NS7350. Disponible en: http://amartastore.com/index.php?route=product/product&product_id=2940

Entre sus características están las siguientes:

- “Proporciona un sistema de prevención de intrusos de última generación (NGIPS) para ofrecer una protección contra amenazas líder en la industria

- Incluye una solución de protección contra malware avanzado (AMP) totalmente integrada que aborda amenazas conocidas y desconocidas, junto con un recinto de seguridad integrado

- Te da la posibilidad de rastrear y contener infecciones de malware

- Correlaciona automáticamente los eventos de amenazas con las vulnerabilidades de su red para que pueda enfocar sus recursos en las amenazas que más importan

- Analiza las debilidades de su red y recomienda las mejores políticas de seguridad para implementar

- Se integra con una serie de productos de seguridad de red de Cisco para aprovechar sus inversiones anteriores y brindar una mayor seguridad”[49]

Fig. 16. Cisco Firepower 4110 NGFW Appliance

Fuente: https://www.secureitstore.com/Firepower-4110.asp

15.2 HERRAMIENTAS DE SOFTWARE

Las principales compañías de seguridad digital, han repotenciado sus productos estrella, dotándolos de módulos de rastreo de malware y sistemas inteligentes antiransomware, capaces de detectar comportamientos sospechosos en los ficheros protegidos y alertando al usuario para que tome las medidas pertinentes.

[49] SecureItStore. Cisco Firepower 4110 NGFW Appliance. Disponible en: https://www.secureitstore.com/Firepower-4110.asp

Existen soluciones diseñadas para los sistemas operativos de mayor demanda como Windows, Linux o Mac. Estas deben ser implementadas en cada equipo que se desee proteger y son un complemento preventivo de las demás medidas de seguridad que se han mencionado anteriormente.

15.2.1 Antiransomware para Windows y Mac:

- **Kaspersky® Anti-Ransomware Tool for Business**: es una herramienta creada para prevenir ataques ransomware antes que surtan efecto sobre los ficheros. Trabaja en segundo plano y monitorea el tráfico de red del equipo en búsqueda de comportamientos que coincidan con los patrones conocidos del malware. Es gratuito y es ideal para entornos empresariales. [50]

- **Malwarebytes anti-ransomware**: Antes llamado CryptoMonitor, es un producto adquirido por la compañía MalwareBytes, que sirve para bloquear el cifrado de ficheros, además de monitorear la red en búsqueda de patrones sospechosos y trabaja en tiempo real. [51]

- **McAfee Ransomware Interceptor**: Es una herramienta gratuita distribuida por la empresa de ciberseguridad McAfee, que posee aprendizaje automático y heurístico para detectar, bloquear y eliminar aplicaciones protegiendo los archivos del cifrado. Aún está en fase piloto pero ha arrojado buenos resultados, aunque en ocasiones puede presentar falsos positivos.[52]

- **Trend Micro Lock Screen Ransomware Tool**: Es una utilidad diseñada para bloquear y eliminar la variante de ransomware conocida como “Lock Screen” o de bloqueo de pantalla que, si bien no cifra archivos, los deja inaccesibles con un bloqueo al iniciar la terminal. Esta herramienta puede instalarse en una USB extraíble de tal forma que puede limpiar un equipo infectado booteando desde la USB o iniciando en Modo Seguro y ejecutando la herramienta desde el sistema operativo.[53]

15.2.2 Antiransomware para Linux: Aunque los sistemas basados en UNIX suelen dar la sensación de ser más seguros contra el ransomware, la realidad es que

[50] Techworld Staff. Marzo 26 2018. Best anti-ransomware tools and decryptors 2018. Disponible en: https://www.techworld.com/security/best-anti-ransomware-tools-and-decryptors-3626974/
[51] Ibid.
[52] Ibid.
[53] Ibid.

también son vulnerables a los criptoataques como se ha demostrado en un apartado anterior llamado “Ransomware en Sistemas Linux”.

En vista de que la mayor parte de los servidores en el mundo tiene sistemas Linux, es importante hacer uso de servicios y aplicaciones que funcionen nativamente en estos ambientes y logren brindar seguridad adicional contra el cifrado de archivos.

- **Sophos Antivirus:** Es un antivirus de licencia comercial además de correr en Windows, se ha adaptado para ejecutarse en múltiples distribuciones de Linux como CentOS, Debian, Mint, RedHat, SUSE y Ubuntu. Su versión mejor equipada cuenta con un módulo antiransomware especialmente pensada en servidores. [54]

- **CryptoStalker:** Desarrollada por Sean Williams es una herramienta para Linux, capaz de detectar cambios al sistema de ficheros mientras busca archivos recién escritos, si estos contienen datos aleatorios, si tienen señales de estar cifrados o si fueron escritos a alta velocidad, por lo que puede informar de forma temprana sobre la presencia de ransomware en el sistema.[55]

[54] Taylor, Dave. 2017. Linux antivirus and anti-malware: 8 top tools. Disponible en: https://www.csoonline.com/article/3238884/linux/linux-antivirus-and-anti-malware-8-top-tools.html

[55] Cimpanu, Catalin. Marzo 26 de 2016. Cryptostalker, a Tool to Detect Crypto-Ransomware on Linux. Disponible en: https://news.softpedia.com/news/cryptostalker-a-tool-to-detect-crypto-ransomware-on-linux-502002.shtml

16. GUIA DE RECUPERACIÓN DE ATAQUES

Hay que tener conciencia que, hasta ahora, la mejor medida de defensa contra un criptoataque es la prevención. “Más vale prevenir que curar” y en el caso del ransomware, “curar” es algo que no siempre está garantizado.

Como se ha visto, los algoritmos de encriptación han avanzado de tal forma que es prácticamente imposible recuperar información cifrada con las últimas técnicas de criptografía, a menos que exista una vulnerabilidad en el código del malware o en el algoritmo utilizado, algo poco común.

Sin embargo, también es cierto que no existe seguridad invencible, y si después de sellar todas las vulnerabilidades conocidas (humanas e informáticas), se es víctima de un criptomalware, es importante que se sigan las siguientes recomendaciones que buscan mitigar el impacto del ataque restringiendo la capacidad extensiva del virus y aumentar las posibilidades de recuperar la disponibilidad de los sistemas y los datos en el menor tiempo posible.

16.1 PRIMER PASO (APAGAR Y AISLAR)

El ransomware no suele detectarse hasta que ya se encuentran encriptados los ficheros, pues una vez ejecutado realiza el cifrado en poco tiempo. Sin embargo, en el caso de detectar un ataque en progreso lo que se debe hacer de forma inmediata es desconectar el equipo atacado de la red y apagarlo.

En un entorno corporativo lo ideal, es apagar los dispositivos de red (switches, routers) para evitar que el malware logre propagarse y contener el ataque lo mejor posible.

16.2 SEGUNDO PASO (COMITÉ DE CRISIS)

Inmediatamente, se contenga el ataque se debe contactar el comité de crisis que debe estar conformado en toda organización para responder de forma acertada y oportuna a eventualidades como estas, y que está previsto en el plan de contingencia de la empresa.

El comité debe contar con personal informático, administrativo, de comunicaciones y si se cuenta, asesoría externa.

16.3 TERCER PASO (CONTROL DE DAÑOS)

Una vez se ha contenido el ataque, lo siguiente es hacer una evaluación del daño ocasionado por el cifrado. Se debe iniciar por revisar el estado de los servicios críticos, es decir, aquellos de los cuales depende la disponibilidad de los servicios prestados al público o que soportan las operaciones diarias de la empresa.

Se deben identificar todos y cada uno de los equipos que hayan sido afectados y su nivel de criticidad, además de un inventario de los sistemas, bases de datos y ficheros de importancia comprometidos en el ataque.

16.4 CUARTO PASO (RESPALDO DE FICHEROS CIFRADOS)

Los equipos afectados y aislados deben ser sometidos a un proceso en el que se realice una clonación completa de sus discos de almacenamiento, las copias deben ser rotuladas, identificadas con sumas HASH y resguardadas para su posterior procesamiento.

Este respaldo de los datos cifrados, servirá de soporte para un eventual análisis forense del ataque en el que se intente determinar la metodología, el vector de ataque y el origen del ataque; información que puede ser útil para procesos judiciales o para retroalimentar la estrategia de seguridad de la empresa.

Otro de los motivos del respaldo, es verificar con posterioridad la posibilidad de recuperar la información con técnicas actuales o en un futuro cercano dependiendo de los resultados de las investigaciones forenses y las herramientas de desencriptación que produzcan los organismos de seguridad.

16.5 QUINTO PASO (RESTAURAR COPIAS)

El siguiente paso es ejecutar el plan de contingencias, que debe proveer la ruta para restaurar las copias de seguridad más reciente de los datos afectados, de tal

manera que los servicios críticos que pudieran haberse detenido con el ataque, entren en funcionamiento en el menor tiempo posible.

Las copias de seguridad incluyen respaldos de bases de datos, puntos de restauración del sistema, shadow copys, backups en la nube, etc. La compañía ARCSERVE ofrece las siguientes recomendaciones en cuanto a las copias de seguridad:

- "Sí, el backup es importante, pero lo es más no llegar a ser infectado. Para ello, debemos tomar precauciones y una de ellas es la educación en seguridad a nuestros usuarios. Podemos ayudarles a identificar un mensaje sospechoso y tener una correcta "higiene en seguridad" evitando abrir indiscriminadamente todos los ficheros y enlaces recibidos por medios sociales o correo electrónico.

- Un acuerdo de nivel de servicio es esencial para planificar una defensa antiransomware y, para ello, es necesario establecer cada qué tiempo necesitamos realizar un backup de nuestra información crítica ¡El negocio depende de ello!

- Es importante seguir un criterio de copias de seguridad adecuado, no solo la periodicidad sino el número de copias a mantener. Recomendamos una estrategia 3-2-1: Mantener 3 copias de la información (2 copias + origen), en mínimo 2 medios distintos y 1 de ellas, offsite.

- Asegúrate que la solución de copia de seguridad elegida incluye el modo de espera virtual para sistemas críticos para una recuperación más rápida.

- Y, por último, recordar que si el malware tiene acceso al backup ¡también lo cifrara! Protégelo." [56]

Es importante, que los backups realizados, se almacenen en equipos o dispositivos que permanezcan aislados de cualquier conexión cableada o inalámbrico, ya que el ransomware buscará cifrar extensiones comunes de ficheros con copias de seguridad.

[56] ACSERVE. 2017. Cómo Recuperarse de un Ataque de Ransomware. Disponible en: https://arcserve.es/como-recuperarse-de-un-ransomware/

Se aconseja que la restauración de las copias de seguridad se haga sobre un sistema operativo recién instalado, de forma que se pueda asegurar que no habrá otro proceso de cifrado con posterioridad.

16.6 SEXTO PASO (NO PAGUE)

La desesperación puede hacer que se cometan errores que cuestan caro. El pago de la extorsión es el objetivo principal de los criptoataques, que normalmente vienen acompañados de plazos perentorios para realizar el pago, bajo amenaza de no poder recuperar los archivos para siempre.

Ante este panorama miles de personas y empresas en el mundo han optado por ceder ante la presión y realizar el pago del rescate, lo que ha causado más efectos contraproducentes que beneficios. Las siguientes son algunas de las razones por las que no debe realizar el pago:

- El pago no garantiza la ausencia de peligro: Aun cuando el atacante devuelva los archivos, nada garantiza que el malware no siga en el sistema y vuelva a ejecutarse en el futuro.

- El pago te convierte en objetivo: Una vez que se ha cedido a pagar, el atacante considera que esta empresa o persona es proclive a pagar rescates y seguramente intentará atacar de nuevo para obtener nuevas ganancias.

- El pago estimula nuevos ataques: Detrás de estos ataques puede haber empresas criminales organizadas que obtienes millones de dólares en ganancias y que con cada pago se sientes animadas a realizar nuevos ataques cada vez más sofisticados.

- El pago no garantiza el rescate: Aunque pueden encontrase casos en los que las víctimas han logrado recuperar sus datos después de pagar, la verdad es que son muchas también las que no logran obtener la llave de descifrado y el atacante desaparece sin dejar rastro.

- Aprende la lección: De las peores situaciones de aprenden lecciones valiosas. Por ello, es importante reflexionar sobre las debilidades de los sistemas que fueron explotadas y diseñar una estrategia de seguridad más consciente y efectiva para evitar nuevos daños.

17. DESPUÉS DEL ATAQUE

Una vez que se detectó el ataque a uno de los sistemas y se ha respondido conteniendo la infección, es muy importante que se sigan las siguientes recomendaciones:

17.1 REALICE UN ANÁLISIS FORENSE

Sería realmente valioso que se realicen procedimientos forenses por parte de expertos en la materia, comenzando en primer lugar por crear copias de seguridad de los discos o sistemas de almacenamiento afectados por el ataque, usando herramientas de software especializadas que no alteren la secuencia original bits y que no borren archivos de sistema o logs que pueden ser muy útiles para establecer las causas del ciberataque.

Se debe identificar el vector de infección que pudo ser un enlace enviado por correo electrónico o en un sitio web, la instalación de una aplicación sospechosa o una simple macro en un documento de Office, entre otras posibles causas. Se busca también, conocer el procedimiento usado para infiltrar el vector en los sistemas de la compañía, las direcciones IP que puedan estar involucradas, el tipo de software utilizado y especialmente, la versión del ransomware que realizó el cifrado de los archivos.

17.2 INFORME A LAS AUTORIDADES

En el caso de Colombia, la policía nacional y la fiscalía general de la nación poseen equipos y personal especializado para realizar investigaciones sobre delitos informáticos. Por ello, es importante denunciar el incidente ante las autoridades competentes y ofrecer toda la colaboración y la información recolectada en el paso anterior, con el fin de esclarecer los hechos y de ser posible dar con los responsables del ataque; evitando que vuelvan a atacar a otras empresas o reincidan con la suya.

Los ciberdelitos como el ataque por ransomware se encuentran tipificados en el código penal colombiano y al estar asociados generalmente con otros delitos conexos como la extorsión, representan penas privativas de la libertad entre 36 y 96 meses de cárcel, con agravantes en casos especiales como se detalla a continuación en la ley 1273 de 2009 expedida por el congreso de la república.

17.3 IDENTIFIQUE EL MALWARE

Identificar la versión exacta del malware usado para la infección puede ser útil cuando por alguna razón, no se cuenten con copias de seguridad de los datos encriptados, puesto que existen herramientas de libre acceso que actualmente permiten reconocer el tipo de ransomware simplemente diligenciando un formulario que pide dos archivos que hayan sido cifrados y el mensaje que dejó el virus con los detalle pertinentes como dirección de monedero de bitcoin, dirección TOR y/o dirección de correo electrónico.

Una de estas herramientas es el sitio web "NoMoreRansom.org" que es una iniciativa adelantada por cuatro socios que son EUROPOL, el European Cybercrime Centre EC3, Politie y la empresa de ciberseguridad McAfee. Además, con el paso del tiempo se han sumado los apoyos de entidades como Avast, Bitdefender, ESET, Kaspersky Lab., Cisco, Bleeping Computer, entre otras. [57]

Fig. 17. Herramienta Web para identificar criptovirus

Fuente: https://www.nomoreransom.org/es/partners.html

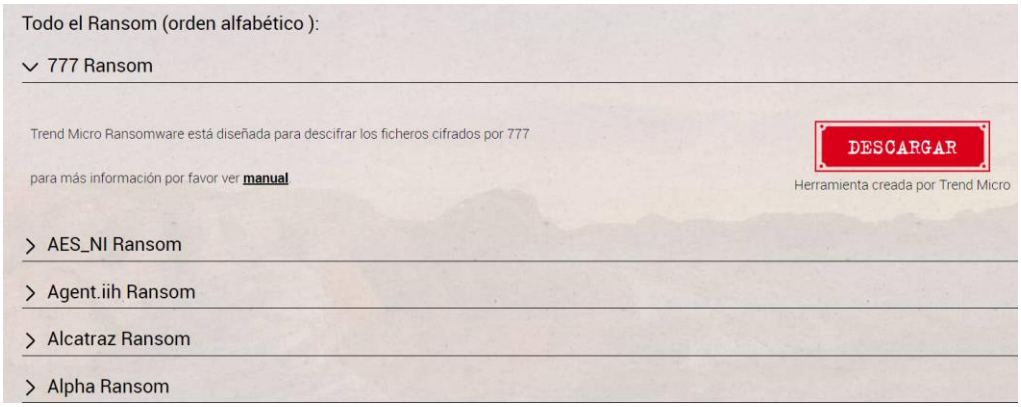
17.4 INTENTE DESCIFRAR LOS DATOS

Una vez se ha identificado plenamente el tipo de malware utilizado en el ataque, la víctima tiene una posibilidad de poder descifrar sus archivos sin necesidad de pagar un rescate por ello. Esto, gracias a que las empresas asociadas a la iniciativa

[57] NoMoreRansom.org. Quiénes somos. Disponible en: https://www.nomoreransom.org/es/partners.html

NoMoreRansom, han puesto a disposición de los usuarios aplicativos de desencriptación, que son el producto de años de investigación, ingeniería inversa o analistas de seguridad que han liberado las claves privadas de los criptovirus para el uso público. El sitio web mencionado, permite descargar la herramienta que lleva por nombre el mismo identificador que se conoce a nivel global el virus.

Fig. 18. Herramientas de descifrado



Fuente: https://www.nomoreransom.org/es/decryption-tools.html

Existe también otra utilidad que se actualiza periódicamente que recopila información de utilidad sobre las familias de ransomware más conocidas, como fecha de aparición, herramientas de descifrado, algoritmo de encriptación o extensión del virus y debería ser consulta en caso de no contar con la forma de recuperar sus archivos. [58]

La herramienta puede encontrarse en el siguiente enlace: https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml

17.5 MITIGUE LOS EFECTOS

Se trata de conseguir reducir al máximo posible los efectos perjudiciales de la infección reduciendo el número de ficheros infectados o recuperándose total o parcialmente de los daños ocasionados. Algunas de las medidas recomendadas son las siguientes:

[58] CN-CERT. Centro Criptológico Nacional. 2017. CCN-CERT BP-04-16, Buenas Prácticas. Disponible en: https://www.coursehero.com/file/26329671/CCN-CERT-BP-04-16-Ransomwarepdf/?justUnlocked=1#/quiz

- Luego de haber aislado el equipo infectado, se debe analizar todos los equipos en riesgo de la organización por medio de herramientas de detección de malware provistos por empresas especializadas.

- Intente restaurar el sistema y los ficheros cifrados. Existen varias formas de hacerlo: Una es por medio de las Shadow Copies, el File History, la Restauración del Sistema o los Herramientas de Backup, que se desarrollarán más adelante en este documento.

- Revisar el contenido de sus sistemas de correo electrónico en busca de enlaces o remitentes sospechosos y publicar los resultados a los empleados para que eviten el acceso o diseminación de la amenaza.

- Revisar la configuración de los firewalls y proxys en busca de agujeros de seguridad que puedan seguir poniendo en riesgo a la empresa.

17.6 APRENDA DEL CASO

Aunque suene doloroso, normalmente se aprende más de los errores que de las victorias. Muchas de los consejos aportados sobre el tratamiento de esta amenaza provienen de lo aprendido en eventos registrados de secuestro de datos en donde se identificaron los métodos y herramientas utilizadas para realizar el ataque.

Por ello es valioso que luego de ser víctima de uno de estos ataques, realice una revisión de los sistemas que pudieron haber fallado, los controles que no se aplicaron, las negligencias que se cometieron e incluso los responsables de la comisión de las mismas. Esta información debe ser valorada por personal competente y presentada a la administración junto con las recomendaciones pertinentes, para que se tomen las medidas suficientes para evitar la repetición de los hechos.

18. CONCLUSIONES

- Reconocer la existencia y la peligrosidad del ransomware es el paso principal antes de poder prepararse adecuadamente para un ataque dirigido. Es necesario contar con el recaudo suficiente de conocimiento relacionado a las variantes, métodos de propagación, mecanismos de encriptación y posibles consecuencias en caso de ser víctimas de una infección.

- El ransomware continúa siendo una amenaza muy importante, aunque las estadísticas muestren una disminución en el número de ataques a nivel mundial. Se debe tener en cuenta que estos ataques suelen intensificarse cuando se descubre una vulnerabilidad peligrosa en un sistema operativo, cosa que puede ocurrir en cualquier momento y sin previo aviso.

- No existe una solución única, efectiva y permanente. Por desgracia, la mayor parte de los algoritmos de cifrado utilizados por las distintas variantes de malware no son reversibles a menos que se cuente con las llaves necesarias. La solución real está en prevenir y contar con un conjunto de directivas y controles que prioricen ante todo el respaldo offline completo y de calidad de los datos, además de un plan de contingencia que le permita a la organización garantizar la continuidad del negocio recuperando en el menor tiempo posible los servicios afectados.

- El protocolo desarrollado al final de este documento puede ser una herramienta útil para que, en entornos empresariales, se tomen con seriedad y responsabilidad y seriedad el potencial de daño de esta amenaza y avancen proactivamente en la gestión de su seguridad, tomando como referencia las recomendaciones y buenas prácticas ofrecidas aquí.

- Se concluye de igual forma que, pagar una extorsión no debería ser una opción al ser víctimas de un secuestro de datos, pues contribuye al crecimiento del delito, lo incentiva y no existe garantía de recuperación de los daños. La mejor opción siempre será evitar llegar hasta este escenario, haciendo de la seguridad un elemento estratégico en el crecimiento de cada organización y concienciando a cada usuario del sistema de la importancia de seguir las recomendaciones de seguridad que se establezcan para proteger los activos que usan a diario.

19. RECOMENDACIONES

Resulta claramente aconsejable que se las empresas e instituciones con infraestructura TIC se tomen con la mayor seriedad la amenaza del ransomware puesto que ya no es un asunto solo tenga relevancia para grandes corporaciones, sino que cada vez más se está desplazando hacia las PYMES, pudiendo potencialmente comprometer sus operaciones y la integridad de su información.

Se deben organizar grupos de trabajo interdisciplinarios en estas organizaciones dedicados a analizar la documentación existente sobre esta temática e iniciar cuanto antes con el diseño de una estrategia de seguridad que integre las recomendaciones dadas en este documento y otros existentes con el propósito de implementarla cabalmente con el seguimiento y control que se requiere en el tiempo para asegurarse que sea permanente y con ejecución de calidad.

Paralelo a lo anterior, es imperativo que todo el personal operativo con funciones TIC sea concienciado y reentrenado en las mejores prácticas de tratamiento seguro de la información, teniendo en cuenta que ellos son el eslabón más débil de una cadena que una vez ha sido rota puede afectar masivamente la empresa.

Una protección efectiva de los datos y activos de alto valor, no solo depende de la tenencia de planes de contingencia, sino que obedece a la conjunción de distintas medidas de seguridad informática activas y pasivas, por lo que se recomienda que se consolide y optimice el SGSI, de tal manera que la contención de la amenaza contemple la búsqueda proactiva de brechas de seguridad en todos los niveles de la organización al igual que la utilización de herramientas especializadas de diagnóstico y detección de comportamientos sospechosos en tiempo real.

Las cripto amenazas aún están lejos de ser una pesadilla pasada, siguen evolucionando para hacerse más lesivas y camuflándose mejor para incursionar en los sistemas de información de formas inadvertidas, por lo que debe existir por parte del equipo de seguridad de la organización, una actualización permanente en cuanto al desarrollo tecnológico de la amenaza y en cuanto a métodos de contención y prevención eficaces para hacerle frente.

20. DIFUSIÓN

La presente guía de prevención y atención de ataques antiransomware está al alcance de las PYMES que deseen obtener una aproximación lo suficientemente detallada a los criptovirus y busquen un manual con recomendaciones bien fundamentadas sobre cómo hacerles frente en sus organizaciones. Como documento está disponible en el repositorio de trabajos académicos de la UNAD en donde estará también disponible a la comunidad estudiantil que desee consultarlo.

BIBLIOGRAFÍA

ACSERVE. “Cómo Recuperarse de un Ataque de Ransomware”. 2019. Disponible en: (https://arcserve.es/como-recuperarse-de-un-ransomware/)

AMARTASTORE. “Mcafee Network Security Platform Ns7350”. 2019. Disponible en: (http://amartastore.com/index.php?route=product/product&product_id=2940)

ARTEAGA, Sandra. “Troyano bancario para Android se convierte en ransomware al eliminarlo”. 2019. Disponible en: (https://computerhoy.com/noticias/moviles/troyano-bancario-android-convierte-ransomware-eliminarlo-70115)

ASLOP, Rory. “10 áreas de control para mitigar contra los ataques de malware”. 2019. Disponible en: (https://searchdatacenter.techtarget.com/es/opinion/10-areas-de-control-para-mitigar-contra-los-ataques-de-malware)

BBC. “Ciberataque masivo: ¿quiénes fueron los países e instituciones más afectados por el virus WannaCry?”. 2019. Disponible en: (https://www.bbc.com/mundo/noticias-39929920)

BOXCRYPTOR. “Cifrado AES y RSA”. 2019. Disponible en: (https://www.boxcryptor.com/es/encryption/)

C, Otto. “Un nuevo ataque de 'ransomware' paraliza grandes empresas en todo el mundo”. 2019. Disponible en: (https://www.elconfidencial.com/tecnologia/2017-06-27/ataque-ransomware-dla-piper-wannacry_1405839/)

CANTÓN, David. “Ransomware: Métodos de infección, protección y recuperación”. 2019. Disponible en: (https://www.incibe-cert.es/blog/ransomware-infeccion-proteccion-recuperacion)

CIMPANU, Catalin. “Cryptostalker, a Tool to Detect Crypto-Ransomware on Linux”. 2019. Disponible en: (https://news.softpedia.com/news/cryptostalker-a-tool-to-detect-crypto-ransomware-on-linux-502002.shtml)

CISCO CANSAC. “Ransomware: Puntos claves para evitar y combatir sus ataques”. 2019. Disponible en: (https://gblogs.cisco.com/cansac/ransomware-puntos-claves-para-evitar-y-combatir-sus-ataques/)

CISCO. “Ransomware: Puntos claves para evitar y combatir sus ataques”. 2019. Disponible en: (https://gblogs.cisco.com/cansac/ransomware-puntos-claves-para-evitar-y-combatir-sus-ataques/)

CN-CERT. CENTRO CRIPTOLÓGICO NACIONAL. “CCN-CERT BP-04-16, Buenas Prácticas”. 2019. Disponible en: (https://www.coursehero.com/file/26329671/CCN-CERT-BP-04-16-Ransomwarepdf/?justUnlocked=1#/quiz)

CONGRESO DE COLOMBIA. “Ley 1273 de 2009”. 2019. Disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html)
ECURED, Enciclopedia colaborativa en la red cubana. “Criptografía”. 2019. Disponible en: (https://www.ecured.cu/Criptografía)

ERNST & YOUNG, EY. “Encuesta Global de Seguridad de la Información 2018-19”. 2019. Disponible en: (https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2018-19/$FILE/ey-encuesta-global-seguridad-informacion-2018-19.pdf)

ESET, North America. “Vulnerability CVE-2017-0144 in SMB exploited by WannaCryptor ransomware to spread over LAN”. 2019. Disponible en: (http://support.eset.com/ca6443/?locale=en_US&viewlocale=en_US)

ESET. “Cómo y por qué el cifrado moldeó al ransomware criptográfico”. 2019. Disponible en: (https://www.welivesecurity.com/la-es/2016/09/13/cifrado-ransomware-criptografico/)

ESET. “Guía de Ransomware”. 2019. Disponible en: (https://www.welivesecurity.com/wp-content/uploads/2017/10/guia-ransomware-eset.pdf)

FRENZ, Christopher M. DIAZ, Christian L. OWASP. “Guía Contra Ataques Ransomware”. 2019. Disponible en: (https://www.owasp.org/images/3/39/Guia_Contra_Ransomware.pdf)

GNUPG, Guía de Gnu Privacy Guard. “Sistemas de cifrado asimétrico”. Junio de 2019. Disponible en: (https://www.gnupg.org/gph/es/manual/x212.html)

INFOBAE, “Alerta por nRansom, el ciberataque que secuestra archivos y pide fotos de desnudos de rescate”. 2019. Disponible en: (https://www.infobae.com/america/tecno/2018/08/09/alerta-por-nransom-el-ciberataque-que-secuestran-archivos-y-piden-fotos-de-desnudos-de-rescate/)

INGENIA. “Firewalls de nueva generación”. 2019. Disponible en: (https://www.ingenia.es/es/servicio/firewalls-de-nueva-generacion-ngfw)

ISACA. “State Of Cybersecurity 2018”. 2019. Disponible en: (https://cybersecurity.isaca.org/state-of-cybersecurity)

JANÉ, Carmen. “La mitad de los ordenadores mundiales funcionan con sistemas operativos antiguos”. 2019. Disponible en: (https://www.elperiodico.com/es/sociedad/20170522/la-mitad-de-los-ordenadores-mundiales-funcionan-con-sistemas-operativos-antiguos-6054398)

MEDINA, Eduardo. “Erebus, el ransomware para Linux que está causando estragos a muchas empresas”. 2019. Disponible en: (https://www.muyseguridad.net/2017/06/26/erebus-ransomware-linux-empresas/)

MENDOZA, Miguel Ángel. “El impacto del ransomware en Latinoamérica durante 2017”. 2019. Disponible en: (https://www.welivesecurity.com/la-es/2018/03/01/impacto-ransomware-latinoamerica-2017/)

MICROSOFT. “Microsoft Security Advisory 4022344”. 2019. Disponible en: (https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2017/4022344)

MOTOS, Vicente. “¿Cuál ha sido la vulnerabilidad que ha explotado el ransomware que ha puesto en jaque a Telefónica y a otras grandes compañías?”. 2019. Disponible en: (https://www.hackplayers.com/2017/05/cual-ha-sido-la-vulnerabilidad-del-ransomware-de-telefonica.html)

MYERS, Lisa. “11 formas de protegerte del ransomware, incluyendo Cryptolocker”. 2019. Disponible en: (https://www.welivesecurity.com/la-es/2015/07/08/11-formas-protegerte-del-ransomware-cryptolocker/)

NOMORERANSOM.ORG. “Quiénes somos”. 2019. Disponible en: (https://www.nomoreransom.org/es/partners.html)

NOTICIAS CARACOL. “Colombia es muy débil en materia de ciberseguridad: expertos”. 2017. Disponible en: (http://caracol.com.co/radio/2017/06/09/nacional/1497042960_148590.html)

PANDA SECURITY. “¿A qué se denomina Sistema de Prevención de Intrusos o IPS?”. 2019. Disponible en: (https://www.pandasecurity.com/usa-es/support/card?id=31452)

PANDA SECURITY. “Troyanos”. 2019. Disponible en: (https://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/trojan/)

PASTOR FRANCO, José, SARASA LÓPEZ, Miguel Ángel, SALAZAR RIAÑO, José Luis, “Criptografía digital: fundamentos y aplicaciones”, Ed. Prensas Universitarias de Zaragoza, 1998.

PHILLION, Matthew. “El Impacto de los Ataques Repetidos de Ransomware”. 2019. Disponible en: (https://gmsseguridad.com/impacto-sophos-ransomware.html)

POLLITT, Mark M.. "Cyberterrorism ¿Fact or Fancy?" Computer Fraud & Security. 1998. Pág. 8-10.

SALAZAR, Edgar David. “SambaCry CVE-2017–7494”. 2019. Disponible en: (https://blog.guayoyolabs.com/sambacry-cve-2017-7494-permite-a-los-hackers-acceder-a-miles-de-ordenadores-linux-de-forma-remota-b4014ac281d9)

SÁNCHEZ J, Roberto. GARCÍA VELÁZQUEZ, Soledad. DEMIAN, Roberto. “Boletín de Seguridad UNAM-CERT-2014-011 Crypto Ransomware”. 2019. Disponible en: (https://www.seguridad.unam.mx/historico/vulnerabilidadesDB/index.html-vulne=6521)

SCAIFE, N., CARTER, H., TRAYNOR, P., & BUTLER, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)

SCOTT-COWLEY, Orlando. “Pagos de ransomware: Financiando el negocio del crimen cibernético”. 2019. Disponible en: (https://www.veeam.com/blog/es-lat/frequent-methods-for-ransomware-payments.html)

SECUREITSTORE. “Cisco Firepower 4110 NGFW Appliance”. 2019. Disponible en: (https://www.secureitstore.com/Firepower-4110.asp)

SYMANTEC. “ISTR July 2017 Contents Executive summary and Key findings Ransomware: An overview A new breed of threat”. 2019. Disponible en: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf. Pág. 9.

TAYLOR, Dave. “Linux antivirus and anti-malware: 8 top tools”. 2019. Disponible en: (https://www.csoonline.com/article/3238884/linux/linux-antivirus-and-anti-malware-8-top-tools.html)

TECHWORLD STAFF. “Best anti-ransomware tools and decryptors 2018”. 2019. Disponible en: (https://www.techworld.com/security/best-anti-ransomware-tools-and-decryptors-3626974/)

TECNÓSFERA, El Tiempo. “Colombia, el país de Latinoamérica más afectado por ransomware en 2018”. 2019. Disponible en: (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/los-paises-mas-afectados-por-ransomware-en-2018-313224)

URUEÑA CENTENO, Francisco J. “Ciberataques, La Mayor Amenaza Actual”. 2015. Disponible en: (http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf)

VHGROUP. “Ransomware: secuestro digital”. 2019. Disponible en: (https://www.vhgroup.net/wp-content/uploads/2017/05/Articulo-Ransomware.pdf)

VPNMENTOR. “Historia de la amenaza conocida como Ransomware: pasado, presente y futuro”. 2019. Disponible en: (https://es.vpnmentor.com/blog/historia-de-la-amenaza-conocida-como-ransomware-pasado-presente-y-futuro/)

ANEXOS

Resumen Analítico Especializado (RAE)

Información General	
Tema	Desarrollar un protocolo de prevención de ataques del tipo Ransonware y guía de manejo de desastres para pequeñas y medianas empresas con infraestructura tecnológica de información.
Titulo	Estudio monográfico sobre la amenaza ransomware, su impacto en las organizaciones y buenas prácticas para su prevención y manejo
Autor(es)	José Carlos Pérez Castro
Director	MSc Frey de Jesús Castro
Fuentes Bibliográficas	Se referencia un total de 58 fuentes bibliográficas.
Año	2019
Resumen	Ransomware es el término acuñado para definir una clase de software malicioso o "malware" que se ha convertido en una auténtica pesadilla para los administradores de TI. Es una palabra compuesta por "ransom" y "software" que traduce "software de rescate", en otras palabras, una aplicación diseñada y diseminada por ciberdelincuentes capaz de infectar un sistema y cifrar sus ficheros por medio de un algoritmo robusto de encriptación, con el fin de extorsionar a su administrador exigiéndole un pago a cambio de poder recuperar su información. Sin embargo, esta definición no hace justicia al nivel de daño que esta amenaza puede provocar en los servicios económicos, políticos, sanitarios o de seguridad, que afectan sensiblemente a los ciudadanos del común que tienen aspectos de su vida vinculados a dichos sistemas de información. Por lo tanto, la finalidad de este documento es analizar en detalle las características de los criptovirus, su arquitectura, sus variantes, algoritmos de cifrado más utilizados, métodos de ataque, perfil de los atacantes, métodos de detección y especialmente generar un protocolo de buenas prácticas para preparar los sistemas objetivos del malware y proporcionarles un blindaje multicapa ante la posible incidencia del ataque; además de una guía de manejo ante una eventual infección y métodos de recuperación para mantener ante todo la disponibilidad de los servicios ofertados en la compañía.
Palabras Claves	Ransomware, criptovirus, amenaza, rescate, criptomoneda, seguridad, disponibilidad, cibercriminalidad, contingencia, prevención, controles
Contenido	A través de este proyecto, se realiza un estudio sobre los conceptos fundamentales del Ransomware, sus antecedentes, modos de operación y evolución histórica. Se analizan los aspectos legales a la luz de la legislación vigente en Colombia. Posteriormente se analiza el ciclo operativo de esta amenaza desde la infección inicial, tipos de archivos propensos a cifrar, métodos de cifrado y sistemas de pago que usan los criminales para cobrar las extorsiones. El documento realiza también un listado de las principales vulnerabilidades que aprovechan los ciberdelincuentes para infiltrar los sistemas operativos de usuarios personales y de empresas que han sido identificados y que pueden ser corregidos

	atendiendo las recomendaciones dadas por los desarrolladores de los sistemas y las empresas de seguridad. Cumpliendo con los objetivos trazados, se registra un compendio de consejos técnicos que han probado ser efectivos para contrarrestar la amenaza y reducir la probabilidad de convertirse en víctima de un ataque criptográfico. Se hacen recomendaciones en cuanto a equipos de hardware y software especializados en la detección y contención de malware ransomware. La guía de recuperación de ataques es uno de los objetivos de este trabajo y efectivamente esta presentada como una ruta de actuación inmediata una vez que ha sido detectada la presencia de una infección por criptovirus de modo que se pueda contener y aislar minimizando el daño. El documento también ofrece una serie de procedimientos a realizar con posterioridad al ataque hincapié en comprender lo que pudo haber fallado en la estrategia de seguridad de la empresa y aprender las lecciones que eviten la repetición del incidente.
Descripción del problema de investigación	
Colombia, según el vicepresidente de Planeación Estratégica de la Sociedad Internacional de Automatización, "… ha desarrollado una serie de prácticas para la seguridad de los gobiernos y de la prestación de servicios públicos. Las Fuerzas Militares y la Policía están preparadas, pero el país en general se ha ratificado en un nivel de riesgo intermedio. Un estudio de ciberseguridad industrial muestra que alrededor del 40% de las empresas que fabrican algún tipo de producto en el sector real, no han hecho una evaluación de riesgos por ciberataques". Un reporte provisto por la empresa tecnológica ESET, informa que del total de eventos de infecciones por Ransomware en Latinoamérica "el 30 por ciento de los casos se presentaron en Colombia, seguido de Perú con un 16 por ciento, México (14 por ciento), Brasil (11 por ciento) y Argentina con el 9 por ciento" con la particularidad que en Colombia se detectó el mayor número de casos de ataque de la variante de criptovirus "Crysis" que, valiéndose de técnicas de ingeniería social, se propaga por medio de correos electrónicos conteniendo archivos infectados y alertando a la víctima de supuestas deudas comerciales. Las consecuencias de un ataque ransomware pueden ser realmente devastadoras. El secuestro de activos de información de una entidad financiera, estatal o incluso de una PYME tiene el potencial de generar pérdidas económicas cuantiosas, indisponibilidad de los servicios, traumatismos operacionales, afectaciones a terceros, daño reputacional y/o retrasos importantes e irrecuperables en el desarrollo de toda clase de proyectos empresariales. Estas afectaciones se ven acentuadas si las víctimas no cuentan con la infraestructura o preparación estratégica para enfrentar una contingencia de este tipo, si no cuentan con sistemas de respaldo o con tecnologías de protección que prevengan la propagación de los ciberataques hacia sistemas críticos o neurálgicos. Formulación del Problema: ¿De qué maneras puede prepararse una organización para evitar la ocurrencia de un ataque ransomware y para mantener la disponibilidad de sus sistemas en caso de ser víctimas de un ataque?	
Objetivos	

General:
Desarrollar un protocolo de prevención de ataques del tipo Ransonware y guía de manejo de desastres para pequeñas y medianas empresas con infraestructura tecnológica de información.

Específicos:

- Compilar información relacionada al ataque ransomware que permita comprender su arquitectura, metodología, motivaciones, variantes y alcance de su impacto en las organizaciones.
- Definir controles y planes de mejoramiento pertinentes para la prevención de ataques por criptovirus.
- Establecer una guía de manejo y recuperación de desastres en caso de ser víctimas de secuestro de datos.

Metodología

El presente trabajo se ha centrado en reunir evidencia documental de ámbito tecnológico y noticioso concerniente a la amenaza Ransomware con el objeto de realizar un análisis cualitativo y en base a este análisis producir un manual práctico de prevención y control que resulte de utilidad para la PYMES en nuestro país.
Se ha usado un método descriptivo y analítico del contenido recabado concerniente a la historia y evolución de las criptoamenazas, además de realizar un análisis de casos de distintos tipos de ciberataques a organizaciones en diversos lugares del mundo que ejemplifican el potencial destructivo de los ataques informáticos de este tipo. Gracias a esta conceptualización y referenciación se diseña una guía concreta de prevención, control y recuperación de ataques.
Se obtuvo material principalmente de fuentes electrónicas, sin embargo, también hay un aporte proveniente de la experiencia personal del autor en relación al enfrentamiento al ransomware en un entorno de producción.

Referentes teóricos y Conceptuales

Se consulta diferentes fuentes y se centra la descripción de los temas principales que son las características del ransomware, métodos de ataque, efectos potenciales y métodos de prevención. Las fuentes con mayor número de consultas son:
VPNMENTOR. Historia de la amenaza conocida como Ransomware: pasado, presente y futuro.
ESET. Guía de Ransomware.
CISCO. 2017. Ransomware: Puntos claves para evitar y combatir sus ataques.
INCIBE. David Cantón. 2014. Ransomware IV: Métodos de infección, protección y recuperación.

Resultados

Elaboración de una reseña de la evolución del Ransomware como amenaza y la identificación de las principales variantes modernas.
Descripción del ciclo de infección y ataque por medio del cifrado extorsivo de datos.
Reseña de ataques a distintos tipos de organizaciones con el fin de determinar la cantidad de daño potencial que puede causar en los activos de las empresas y en el desarrollo de sus operaciones.
Elaboración de un protocolo de prevención y control que minimiza las posibilidades de ser víctimas de los criptovirus.
Elaboración de una guía de respuesta y contención en caso de ser objeto de un ataque criptográfico con el fin de proteger el mayor número de activos posibles y mantener aislada la amenaza y mantener la continuidad del negocio.

Conclusiones

- Reconocer la existencia y la peligrosidad del ransomware es el paso principal antes de poder prepararse adecuadamente para un ataque dirigido. Es necesario contar con el recaudo suficiente de conocimiento relacionado a las variantes, métodos de propagación, mecanismos de encriptación y posibles consecuencias en caso de ser víctimas de una infección.
- El ransomware continúa siendo una amenaza muy importante, aunque las estadísticas muestren una disminución en el número de ataques a nivel mundial. Se debe tener en cuenta que estos ataques suelen intensificarse cuando se descubre una vulnerabilidad peligrosa en un sistema operativo, cosa que puede ocurrir en cualquier momento y sin previo aviso.
- No existe una solución única, efectiva y permanente. Por desgracia, la mayor parte de los algoritmos de cifrado utilizados por las distintas variantes de malware no son reversibles a menos que se cuente con las llaves necesarias. La solución real está en prevenir y contar con un conjunto de directivas y controles que prioricen ante todo el respaldo offline completo y de calidad de los datos, además de un plan de contingencia que le permita a la organización garantizar la continuidad del negocio recuperando en el menor tiempo posible los servicios afectados.
- El protocolo desarrollado al final de este documento puede ser una herramienta útil para que, en entornos empresariales, se tomen con seriedad y responsabilidad y seriedad el potencial de daño de esta amenaza y avancen proactivamente en la gestión de su seguridad, tomando como referencia las recomendaciones y buenas prácticas ofrecidas aquí.
- Se concluye de igual forma que, para una extorsión no debería ser una opción al ser víctimas de un secuestro de datos, pues contribuye al crecimiento del delito, lo incentiva y no existe garantía de recuperación de los daños. La mejor opción siempre será evitar llegar hasta este escenario, haciendo de la seguridad un elemento estratégico en el crecimiento de cada organización y concienciando a cada usuario del sistema de la importancia de seguir las recomendaciones de seguridad que se establezcan para proteger los activos que usan a diario.