DOI: https://doi.org/10.46296/yc.v4i7.0035

ESTUDIO EXPLORATORIO DE LAS ESTRATEGIAS PARA LA PROTECCIÓN A LAS REDES EMPRESARIALES DE LAS INFECCIONES RANSOMWARE

EXPLORATORY STUDY OF STRATEGIES FOR PROTECTING CORPORATE NETWORKS OF RANSOMWARE INFECTIONS

Vivanco-Toala Danny[1]*; Bolaños-Burgos Francisco[2]; Angulo-Murillo Navira[3]

[1]Magíster en Auditoría de Tecnologías de Información, Universidad Espíritu Santo. Guayaquil, Ecuador.
[2]Director y Docente de la Maestría de Auditoría de Tecnologías de Información, Universidad Espíritu Santo. Guayaquil, Ecuador.
[3]Magíster en Auditoría de Tecnologías de Información, Universidad Espíritu Santo. Guayaquil, Ecuador.

***Correo:** dvivancot@uees.edu.ec

Resumen

Las infecciones Ransomware a lo largo del tiempo han venido evolucionando, lo que ha desencadenado alertas en grandes y pequeñas empresas, por lo que, el objetivo de este artículo es realizar un estudio exploratorio de las estrategias para proteger las redes empresariales de las infecciones Ransomware, para lo cual, se plantea la necesidad de establecer un esquema de que tipos de infecciones ransomware son las más comunes, a través de una matriz de diferenciación de los tipos de ataques TeslaCrypt, CTB-Locker, CryptoWall, CryptoLocker y Locky del tipo Crypto Ransomware, con las características del ataque, el método del rescate y las estrategias recomendadas a ser empleadas. A partir del estudio realizado se puede concluir que la correcta aplicación de las medidas para prevenir los ataques Ransomware, como reducir el riesgo de exponerse al ataque, instalando programas de listas blancas de correo electrónico; realizar respaldos de información de la empresa, dividir y aislar la red de la empresa, en segmentos de red y tener una respuesta rápida de algún ataque que se presente, empleando herramientas de monitoreo de red o sistemas de detección o prevención de intrusos por algún comportamiento sospechoso en la red; lo cual, permitirá que las empresas minimicen el pago por rescate de información a ciberdelincuentes.

Palabras clave: Infecciones Ransomware, Crypto Ransomware, Redes Empresariales.

Abstract

Ransomware infections have been evolving over time, which has triggered alerts in large and small companies, so the aim of this article is to conduct an exploratory study of strategies to protect enterprise networks from infections Ransomware, for which, it is necessary to establish a scheme of which types of ransomware infections are the most common, through a matrix of differentiation of the types of attacks TeslaCrypt, CTB-Locker, CryptoWall, CryptoLocker and Locky of the type Crypto Ransomware , with the characteristics of the attack, the rescue method and the recommended strategies to be employed. In conclusion, from the study carried out we can conclude that the correct application of measures to prevent Ransomware attacks, such as reducing the risk of being exposed to attack, installing programs of white lists of electronic mail; perform company information backups, divide and isolate the company network, in network segments and have a quick response to any attack that may occur, using network monitoring tools or intrusion detection or prevention systems for some behavior suspect in the network; which will allow companies to minimize the payment for the rescue of information to cybercriminals.

Keywords: Infections Ransomware, Crypto Ransomware, Enterprise Networks.

Información del manuscrito:
Fecha de recepción: 02 de junio de 2020
Fecha de aceptación: 08 de julio de 2020
Fecha de publicación: 10 de julio de 2020

1. Introducción

Las infecciones ransomware han ido evolucionando con el pasar de los años, lo que ha desencadenado alertas en grandes empresas como Google, Microsoft, entre otras, donde almacenan gran cantidad de información en línea y usuarios que pueden acceder a la misma, desde cualquier dispositivo electrónico a través de PC, Tablet o celulares (Glassberg, 2016; Sgandurra, Muñoz-González, Mohsen, & Lupu, 2016). Así pues, el primer ransomware reconocido fue, el AIDS Trojan liberado en 1990, con tipo de cifrado simétrico, el cual se distribuyó en una conferencia en Panamá sobre la enfermedad del SIDA a través de un diskette, donde el software comenzó a cifrar los nombres de los archivos que se encontraban en los equipos, usando probablemente la misma clave pública para todos los cifrados, presentándose luego una pantalla para el pago a una localización en Panamá, el cual resultó ineficaz, ya que más tarde, fue publicado un programa para restaurar los nombres de archivos cifrados, el cual se distribuyó rápidamente a todos los equipos infectados (Orman, 2016; Salvi & Kerkar, 2015; Young & Yung, 1996).

Asimismo, los cyber criminales comenzaron a darse cuenta que podían lucrarse utilizando infecciones ransomware, por lo que, en el año 2006, organizaciones criminales utilizaron ransomware con cifrado asimétrico RSA, y utilizaron programas maliciosos como: The Archiveus Trojan, The Gpcode, Troj.Ransom.A, Krotten, May Archive y Cryzip, los cuales comenzaron a utilizar un esquema de asimetría RSA más sofisticado aumentando el tamaño de la clave. (Salvi & Kerkar, 2015)

Masfield-Devine (2016) señala que, en el reporte del Internet Organised Crime Threat Assessment [IOCTA] de la European Police Office [EUROPOL], los ataques ransomware están como la preocupación dominante en las leyes aplicadas en los Estados Unidos. De igual manera, Barth (2016); Kaspersky (2016); O'Gorman and McDonald (2012); Sgandurra et al. (2016) indican, que muchas de las victimas que han sido atacadas, han pagado el rescate, por ejemplo en el año 2012 Symantec fue capaz de

desmantelar una red de Comando y Control que que había sido atacada por el ransomware CrytoDefense, donde el estudio de seguimiento del ataque mostró que el 2,9% de las víctimas, de 68.000 infecciones realizadas a la red, habrían pagado el rescate. Asimismo en el año 2016 se detectaron 372.602 ataques de ransomware a empresas grandes, pymes y consumidores, de los cuales el 17% iba dirigido a todo tipo de empresas grandes y pymes, donde el mayor porcentaje de ataques se evidencia para los consumidores o usuarios.

Glassberg (2016); Liao (2008), indica que, entre los años 2013 y 2015, el número de ransomware detectados en las empresas grandes, pymes y usuarios atacados se han incrementado en un 270%, debido a las consecuencias de tener medidas de seguridad inadecuadas, que resultan tan catastróficas tanto para ambos tipos de empresas. Del mismo modo, McAfee (2015) a través de la Cyber Threat Alliance, señala, que revelaron la campaña de un ransomware basado en el malware CrytoWall, con el cual, recaudaron los criminales cibernéticos alrededor de $325.000 en dos meses. No obstante, en el año 2016, ocurrieron dos ataques ransomware en empresas públicas de Israel, el primero en la autoridad eléctrica y el segundo en los municipios de servicios públicos, donde recibieron ataques phishing vía correo electrónico y estuvieron fuera de servicio el centro de datos y áreas administrativas, lo que, sin embargo, no causó efecto en el servicio de poder eléctrico y/o operaciones industriales.

Así también, en el 2016, la empresa Intel Security reportó amenazas ransomware, donde habría existido un incremento del 127% en ataques ransomware a empresas grandes y Pymes respecto a los años anteriores, así pues, la empresa Trend Micro encontró que el 44% de las empresas atacadas habrian sufrido al menos una infección ransomware en los dos ultimos años, y el 27% habría sido atacada más de una vez, mientras que el 65% de las empresas afectadas habrian pagaron el rescate; en el informe que presenta la empresa Trend Micro se indica, que existen 79 nuevas familias de ransomware en el año 2016 en comparación con las 29 familias que existian en el año 2015. (Masfield-Devine, 2016).

Asimismo, existen varios autores como es el caso de Brewer and LogRhythm (2016), que señalan que los Estados Unidos es la nación más orientada a ataques ransomware, ya que es uno de los países que poseen grandes y pequeñas (Pymes) empresas, las cuales podrían pagar magnificas cantidades de dinero por el rescate de la información. Así también, según Liao (2008), señala que durante el año 2006, las empresas pymes de todo el mundo gastaron alrededor de 11.400 millones de dólares en seguridad de TI, según un informe publicado por la firma analista AMI-Partners, la inversión representó un aumento del 23% respecto al año 2005, cuando las pymes desembolsaron 9.300 millones de dólares en productos de seguridad, dado que, la tendencia en ataques ransomware no muestra señales de desaceleración, sin embargo, de acuerdo a lo antes expresado, es necesario que las empresas cuenten con el suficiente conocimiento de las estrategias o procedimientos a seguir para proteger sus redes de las infecciones Ransomware y disminuir posibles pagos de rescate de información.

De acuerdo a lo antes expuesto, el propósito de este artículo es determinar las estrategias más apropiadas para proteger las redes Empresariales de los siguientes ataques ransomware: TeslaCrypt, CTB-Locker, CryptoWall, CryptoLocker y Locky del tipo Crypto Ransomware; por lo que, se plantea la necesidad de establecer un esquema de que tipos de infecciones ransomware son las más comunes, a través de una matriz de diferenciación los ataques antes mencionados con la forma de ataque, rescate y estrategias a ser empleadas.

2. Marco Teórico

Ransomware

Gazet (2010); Luo and Liao (2007); Rhoades (2016); Sittig and Singh (2016), señalan que ransomware es un tipo de malware o esquema de extorsión por el cual los atacantes secuestran y cifran los archivos de las computadoras de las víctimas, para que luego soliciten un rescate o pago, para así poder recuperar los archivos en buenas condiciones o el acceso total al sistema, por consiguiente, Asimismo Sgandurra et al. (2016) indica, que hay dos tipos

principales de ransomware, los cuales son: el Locker Ransomware y el Crypto Ransomware, donde el objetivo del Locker Ransomware es bloquear la computadora del usuario, utilizando mecanismos sencillos o sofisticados, para hacer que el usuario no pueda recuperar el acceso al equipo, mostrándose un mensaje en la pantalla del equipo, donde se exige el pago, concediéndose el acceso sólo si el usuario paga el rescate, mientras que, el Crypto Ransomware busca silenciosamente cifrar los archivos de los usuarios, para luego pedir a las víctimas pagar un rescate y puedan obtener la clave de descifrado para acceder a ellos nuevamente, en ciertas ocasiones el Crypto Ransomware no cifra todo el disco duro, solo busca extensiones específicas como .doc, .jpg .pdf o documentos de presentaciones, entre otros, que suelen contener valiosa información (Hollis, 2016) .

Ilustración 1: *Tipos principales de ransomware.*
Fuente: *(Savage, Coogan, & Lau, 2015).*

¿Cómo trabajan los Ransomware?

Luo and Liao (2009); Savage et al. (2015), señalan que una vez que el atacante envía a la víctima el precio del rescate por la información cifrada, el atacante podría utilizar las siguientes alternativas para el secuestro de información; ya sea por vía web o email, primero, podría comprimir todos los archivos del equipo ubicados en un paquete comprimido por contraseña Zip; segundo, podría también cifrar individualmente cada archivo localizado y a continuación quitar los archivos originales, por ejemplo si el archivo original es PaperFinal.doc, ransomware creará un nuevo archivo como “Encryted_PaperFinal.doc”; tercero, en definitiva, el atacante podría crear un carpeta oculta y mover todos los archivos a esa carpeta, produciendo un engaño a la víctima, esta última alternativa conlleva el menor daño y es factible que la víctima recuperé todos los archivos perdidos. Asimismo, Orman (2016) indica que una vez que el atacante cifra la información, este informa a las víctimas los sistemas anónimos de pago u red Bitcoin a ser utilizados, de tal manera que protegen a los extorsionadores moviéndose el dinero del rescate sin

identificar sus cuentas bancarias o su ubicación.

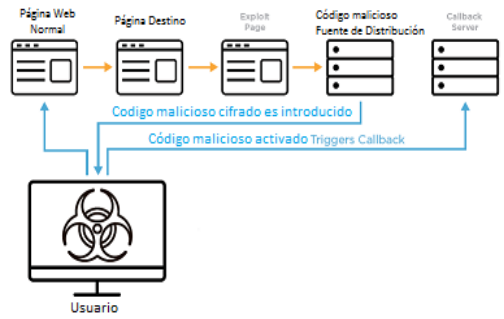

Ilustración 2: *Cómo ransomware infectan a víctimas vía Web.*
Fuente: (*FireEye, 2016)*

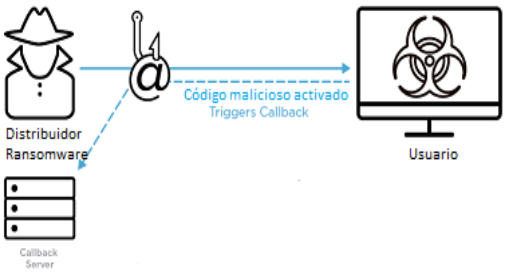

Ilustración 3: *Cómo ransomware infectan a víctimas vía Email.*
Fuente: *(FireEye, 2016)*

Tipos de ataques Ransomware

U.S.Government (2016), señala las siguientes variantes de tipos de ataques ransomware más importantes:

- **CryptoWall**

Según Cabaj, Gawkowski, Grochowski, and Osojca (2015), CryptoWall fue la primera variante de ransomware desde el año 2014, que sólo aceptó pagos de rescate en Bitcoin. Las cantidades de rescate asociadas con CryptoWall suelen estar entre $200 y $10.000. Asimismo, CryptoWall se ha convertido en la variante de ransomware más exitosa con víctimas en todo el mundo, teniendo este ataque dos formas de infectar los equipos, una por correo electrónico Spam con malware en el archivo adjunto y otra a través de los sitios web infectados con Angler Exploit Kit, para así, después de una infección exitosa, ponerse en contacto con los servidores de Internet y tan pronto se reciba la clave pública RSA de 2048 bits para el cifrado de los archivos importantes del equipo, creándose en cada directorio cifrado dos archivos adicionales los cuales son HELP_DECRYPT.PNG y HELP_DECRYPT.URL.

Así pues, Salvi and Kerkar (2015) mencionan variantes de CryptoWall, los cuales son: CryptoWall 2.0, se propaga mediante archivos adjuntos de correo electrónico pdf maliciosos y varios kits de exploits, utiliza TOR para ocultar la red de Comando y Control (C&C) mientras que, CryptoWall 3.0, utiliza I2P (Proyecto de Internet Invisible) para el anonimato, obtiene acceso a la escala de privilegios en el Sistema

por el uso de Exploit y deshabilita muchas características de seguridad del Sistema principal, y finalmente CryptoWall 4.0, la diferencia más importante es que cifra los nombres de los archivos ya cifrados, lo que hace más difícil de descifrar los archivos que necesitan ser recuperados.

Así también CyberThreatAlliance (2016) indican que, entre los años 2014 y 2015, Internet Crime (IC3) recibió 992 quejas relacionadas con CryptoWall, con víctimas reportando pérdidas por un total de más de $18 millones. De la misma forma, CryptoWall se distribuye principalmente a través del correo electrónico no deseado, pero también infecta a las víctimas a través de descargas en la unidad de disco y publicad infectada.

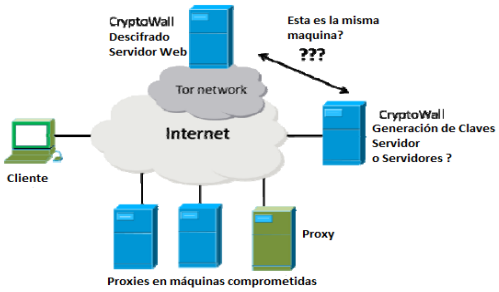

Ilustración 4: *Infraestructura CryptoWall.*
Fuente: *(Cabaj et al., 2015).*

- **TeslaCrypt**

FireEye (2016); Scaife, Carter, Traynor, and Butler (2016) señala que, TeslaCrypt fue descubierto por primera vez en el año 2015, dirigiéndose inicialmente a la comunidad de videojuegos cifrando archivos de juegos en línea. Asimismo, este tipo de ataque cifra varios tipos de archivos como documentos, imágenes y archivos de base de datos, utilizando una búsqueda en profundidad, es decir, no cifra en el primer directorio al cual accede, sino hasta haber alcanzado el directorio más profundo. Es así que, una vez que los datos se cifran, TeslaCrypt intenta eliminar todas las copias de volumen local y puntos de restauración del sistema para evitar la recuperación de archivos, y reducir las posibilidades de las víctimas de bloquear o remediar facilmente los ataques. De tal manera, TeslaCrypt se distribuye a través de los kits de explotación Angler, Sweet Orange y Nuclear. Así pues, Kirda (2015) indica también que, TeslaCrypt no utiliza algoritmos asimétricos RSA-2048 para cifrar archivos, sino utiliza en su lugar algoritmo simétrico AES.

- **CTB-Locker**

ESETSecurity (2015) señala que, CTB-Locker surgió en el año 2014 y es una de las primeras variantes de

ransomware en utilizar la red TOR para su infraestructura Comando y Control (C2). Asimismo, CTB-Locker utiliza TOR exclusivamente para sus servidores C2 y sólo se conecta al C2 después de cifrar los archivos de las víctimas. Además, a diferencia de otras variantes de ransomware que utilizan la red TOR para cualquier comunicación, los componentes de TOR están incrustados en el malware CTB-Locker, haciéndolo más eficiente y más difícil de detectar. Así pues, CTB-Locker se distribuye a través de descargas de unidad de disco y correos electrónicos de SPAM. Asimismo Sharma, Zawar, and Patil (2016) señalan que CTB-Locker se distinguió de las variantes de ataques antes mencionadas, a través de características, tales como, un servidor de control basado en TOR y direcciones Bitcoin generadas automáticamente, únicas para cada víctima, donde, el rescate sigue siendo vendido a criminales cibernéticos; y es así que, la mayoría de las víctimas atacadas por el ransomware CTB-Locker y detectadas por McAfee Labs se encuentran en Norteamérica.

- **CryptoLocker**

Europol (2016); Saiyed (2016) señala que, las primeras versiones del malware CryptoLocker fueron publicadas en el 2013, por lo que, este Ransomware entra en las empresas por medio del correo electrónico, es decir, si el usuario hace clic en el ejecutable adjunto al correo inmediatamente comienza a analizar las unidades de red, cambia el nombre de todos los archivos, carpetas y los cifra. Por otra parte, CryptoLocker 2.0, es una versión nueva y mejorada de CryptoLocker en el mismo año 2013, implementando el malware en C#, Asimismo, la red TOR se utilizó para el anonimato y los métodos de pago como Bitcoin se emplearon para la extorsión. Utilizó cifrado RSA de 2048 bits. Esta última variante no es detectada por el antivirus o firewall (ESETSecurity, 2016; U.S.Government, 2016).

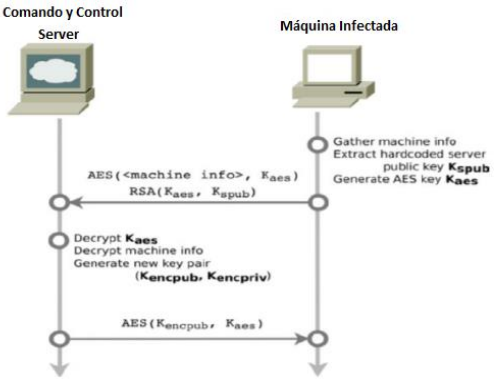

Ilustración 5: *CryptoLocker y Servidor C&C*
Fuente: *(Kansagra, Kumhar, & Jha, 2016)*

- **Locky**

Fue descubierto a principios del año 2016, donde se observó una variante destructiva de Ransomware que infecta computadoras pertenecientes a empresas de todo el mundo. Así también, Locky se propaga a través de correos electrónicos de Spam que incluye documentos maliciosos de Microsoft Office o archivos adjuntos comprimidos, por ejemplo .rar .zip que anteriormente estaban asociados con troyanos bancarios como Dridex y Pony. Ahora bien, los archivos adjuntos maliciosos contienen macros o archivo JavaScript para la descarga del malware Locky y puede llegar a cifrar más de 160 tipos de archivos diferentes incluyendo discos virtuales, bases de datos y archivos bitcoin wallet (wallet.dat). En la actualidad este ransomware se ha distribuido utilizando el Kit de Explotación Nuclear (Europol, 2016; Symantec, 2016).

¿Cómo proteger las redes empresariales de los ataques Ransomware?

Glassberg (2016) señala que las redes empresariales tanto para grandes como pequeñas empresas (PYMES) pueden protegerse de los ataques ransomware, tomando medidas orientadas a las buenas prácticas del día a día, donde el riesgo se minimiza más no se elimina. Así pues, la primera medida a mencionar es él, reducir el riesgo de exponerse al ataque, quiere decir instalar programas de listas blancas de correo electrónico, para no abrir correos donde no conozca el remitente y no abrir enlaces o descargar archivos adjuntos, realizar "scripts" bloqueando plugins no seguros en el navegador y aplicarlo en todas las computadoras de los empleados. Así también, capacitar a los empleados en seguridad básica sobre todo en lo que respecta a correos electrónicos de phishing, asimismo, asegurarse que todos los equipos y servidores se actualicen con el último software y/o parches de seguridad, de la misma forma, que utilicen programas robustos de detección de malware con soporte anti-phishing, con un firewall moderno y evitar el uso de dispositivos o medios externos conectados a las máquinas de los usuarios (Pathak & Nanded, 2016).

Por otro lado, Luo and Liao (2007), indican también como otra de las medidas a seguir para prevenir ataques Ransomware es la de, mantener respaldos de información de la empresa, donde se deben realizar copias de seguridad (Backups) de la información en discos duros y/o externos, si bien es técnicamente imposible realizar una copia de todos los archivos que se tiene en la red corporativa, se puede clasificar la información más crítica de la empresa y aislarla con copias de seguridad. Así también, cuando se utilicen dispositivos de almacenamiento físico, asegurarse de que no estén conectados a la red porque podrían infectarse. De la misma forma, utilizar almacenamiento de información asociada en la nube con cierto tipo de información valiosa, ya que está proporcionará un nivel adicional de seguridad para la recuperación completa de la información, donde las copias de seguridad de datos son los elementos más importantes de una defensa contra Ransomware.

Asimismo, Symantec (2016) indica dentro de sus recomendaciones para prevenir ataques ransomware otras medidas, el cual menciona que se debe dividir y aislar la red de la empresa, en segmentos de red, aplicando Listas de Control de Acceso (ACL), de tal manera que dificulta al malware a difundir de una máquina que este infectada a los equipos de los empleados. Otra de las medidas es tener una respuesta rápida de algún ataque que se presente, empleando herramientas de monitoreo de red para administración de eventos sospechosas en la red, sistemas de detección o prevención de intrusos (IDS/IPS), los cuales permiten detectar rápidamente actividades maliciosas. En el caso, que el usuario reciba una notificación de Ransomware en el equipo, simplemente desconecte el mismo del Internet (Brewer & LogRhythm, 2016).

Kaspersky (2016) menciona también que, si por alguna razón, los archivos se cifran con ransomware y se solicita el pago de un rescate, no se debe pagar, ya que cada bitcoin transferido a manos de los cibercriminales aumenta la rentabilidad de este tipo de delitos informáticos, que a su vez conducen a la creación de nuevo ransomware.

Por otra parte Liao (2008) indica que las grandes empresas tienen equipos de seguridad que vigilan

constantemente cualquier actividad maliciosa, mientras que, en las empresas pequeñas (PYMES) los ataques ransomware se consideran un problema más serio, ya que las empresas deben tener recursos para obtener una protección de seguridad adecuada, como las tiene las grandes empresas, ya que, los sistemas de respaldo para las PYMES pueden resultar ser mucho más costoso, lo que lo hace ser más susceptible a los ataques. Es por esto que, las empresas PYMES deben implementar un antivirus actualizado, actualizar los sistemas operativos y navegadores, tener un firewall, de tal manera que controle la información que los usuarios puedan acceder, mantenerse al día con los parches de seguridad y utilizar un bloqueador de ventanas emergentes (Salvi & Kerkar, 2015).

Diferenciación de los ataques Ransomware en función de las formas de ataque y rescate.

Sgandurra et al. (2016) menciona las características de ataques y método de rescate Ransomware más representativas, utilizadas por los ciberdelincuentes, por lo que, se expondrán con las estrategias recomendadas a aplicarse en los ataques realizados, los cuales se detallan en el Apéndice “A”. De igual manera, Liao (2008); Luo and Liao (2007) señala también todas las formas usadas por los ataques ransomware recientes y los métodos de rescate a implementarse con el valor de la demanda por ataque.

3. Conclusiones, limitaciones y trabajos futuros

Saber cómo trabajan los ataques ransomware, permiten a las empresas grandes y pequeñas PYMES, observar las alternativas que pueden emplearse para el secuestro de la información, ya sea por vía web o email, donde, como primera opción para un ataque, se pueden comprimir todos los archivos del equipo, y ser ubicados en un paquete comprimido con contraseña Zip, también se podrían cifrar individualmente cada archivo localizado y luego quitar los archivos originales y crear un nuevo nombre de archivo cifrado y por último podrían crear una carpeta oculta y mover todos los archivos a esa carpeta, produciendo un engaño a la víctima, donde esta alternativa conlleva el menor daño y es factible

que la víctima recupere todos los archivos perdidos.

El detallar los tipos de ataques ransomware descritos en el objetivo planteado, permiten a las grandes y pequeñas empresas PYMES, conocer las características y comportamientos de los ransomware, es decir la forma de propagación del ataque, ya sea a través de los correos electrónicos como spam con archivos adjuntos, por publicidad infectada o por sitios web infectados con angler exploit kit, para luego, utilizar en el cifrado de información de las víctimas, algoritmos simétrico AES o asimétrico RSA, dependiendo del tipo de ransomware que se emplee.

Describir cómo proteger las redes empresariales de los ataques ransomware, facilita a las empresas la implementación de las siguientes medidas orientadas a las buenas prácticas, como, reducir el riesgo de exponerse al ataque, es decir, instalar programas de listas blancas de correo electrónico y realizar scripts de bloqueo de plugins no seguros en el navegador, asimismo, realizar respaldos de información de la empresa, donde se deben de efectuar copias de seguridad (Backups) de información de la empresa, de la mismo forma, dividir y aislar la red de la empresa, a través de segmentos de red aplicando ACL y tener una respuesta rápida de algún ataque que se presente, empleando herramientas de monitoreo de red para alguna detección sospechosa en la red o implementar sistemas de detección o prevención de intrusos los cuales detectan rápidamente actividades maliciosas; y dado el caso que el usuario reciba una notificación de Ransomware en el equipo, simplemente desconecte el mismo del Internet.

De acuerdo a lo antes expresado, alrededor del mundo existen una mayor cantidad de empresas pymes que grandes empresas, lo que, muestra una limitante, ya que existen organizaciones que por falta de recurso económico y conocimiento de los ataques ransomware, no pueden proteger las redes empresariales, y en otros casos las pymes que poseen recursos se ha demostrado que la adquisición de herramientas y equipos de seguridad TI, los obtienen con porcentajes altos de compra de un año a otro, lo que provoca, que empresas se vean en la obligación de pagar el rescate a los ciberdelincuentes.

Una vez que se observó, el comportamiento de los ataques ransomware tanto para empresas grandes como para pequeñas, se requiere plantear como trabajo futuro, el análisis comparativo de los tipos de ataques ransomware que se han dado en las empresas grandes y pymes en Latinoamérica y el impacto económico que se tuvo por tipo de empresa.

Bibliografía

Barth, B. (2016). Survey: 48% of organizations attacked by ransomware over 12-month period. SC Magazine US.

Brewer, R., & LogRhythm. (2016). Ransomware attacks: detection, prevention and cure. Network Security, 5-9.

Cabaj, K., Gawkowski, P., Grochowski, K., & Osojca, D. (2015). Network activity analysis of CryptoWall ransomware. Przegląd Elektrotechniczny, 91(11), 201-204.

CyberThreatAlliance. (2016). CryptoWall Version 4 Threat Report. Retrieved from

ESETSecurity. (2015). ESET Security Report Latinoamérica 2015. Retrieved from www.eset-la.com

ESETSecurity. (2016). Tendencias 2016 (in) Security everywhere. Retrieved from

Europol. (2016). IOCTA 2016. Retrieved from

FireEye. (2016). Ransomware response strategies. Retrieved from www.FireEye.com

Gazet, A. (2010). Comparative analysis of various ransomware virii. Journal in computer virology, 6(1), 77-90.

Glassberg, J. (2016). Defending Against the RANSOMWARE threat. 4.

Hollis, M. (2016). Breaches and ransomware skyrocket: Maintaining Safe Harbor.

Kansagra, D., Kumhar, M., & Jha, D. (2016). Ransomware: A Threat to Cyber security. Indian Journal of Forensic Medicine and Toxicology, 224-227.

Kaspersky. (2016). Aumentan un 30% las víctimas de ransomware en el primer trimestre de 20016 según Kasperky Lab. Retrieved from

Kirda, E. (2015). Most Ransomware Isn't As Complex As You Might Think Yes, we should be able to detect most of it. Lastline Labs, 1-6.

Liao, Q. (2008). Ransomware: A growing threat to SMES. 360-366.

Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware

Prevention. . 195-202. doi:10.1080/10658980701576412

Luo, X., & Liao, Q. (2009). Ransomware: A New Cyber Hijacking Threat to Enterprises. International Journal of Cognitive Informatics and Natural Intelligence, 1-6.

Masfield-Devine, S. (2016). Ransomware: taking businesses hostage. Network Security, 10.

McAfee. (2015). Informe de McAfee Labs sobre amenazas. Retrieved from

O'Gorman, G., & McDonald, G. (2012). Ransomware: A growing menace. Retrieved from

Orman, H. (2016). Evil Offspring – Ransomware and Crypto Technology. IEEE Internet Computing, 6.

Pathak, P., & Nanded, Y. M. (2016). A Dangerous Trend of Cybercrime: Ransomware Growing Challenge.

Rhoades, G. (2016). Ransomware and other malware. The Indexer, 34(3), 126-128.

Saiyed, C. (2016). Cryptoloker. ISSA Journal, 14-18.

Salvi, H. U., & Kerkar, R. V. (2015). Ransomware: A cyber extortion. Asian Journal of Convergence in Tecnology, 6.

Savage, K., Coogan, P., & Lau, H. (2015). The evolution of Ransomware. Retrieved from

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). Cryptolock (and drop it): stopping ransomware attacks on user data. Paper presented at the Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on.

Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016). Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection. Cornell University Library, 1-12.

Sharma, M. P., Zawar, M. S., & Patil, S. B. (2016). Ransomware analysis: internet of things (IOT) security issues, challenges and open problems in the context of worldwide scenario of security of systems and malware attacks. 1-8.

Sittig, D. F., & Singh, H. (2016). A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Applied Clinical Informatics.

Symantec. (2016). Internet Security Threat Report. Retrieved from www.symantec.com

U.S.Government. (2016). How to Protect your Networks from Ransomware.

Young, A., & Yung, M. (1996). Cryptovirology: Extortion-Based Security Threats and Countermeasures. IEEE Symposium on Security and Privacy, 13.

APÉNDICE A

Tabla 1: Tipos de ataques ransomware representativos en función de la(s) características de ataque, formas de rescate y estrategias a aplicarse.

Nombre	Año Creación	Características de ataque	Método de Rescate	Estrategia(s) recomendada(s) a aplicarse
CryptoWall	2014	Infecta los equipos por correo electrónicos spam y por sitios web que utilizan Angler Exploit Kit	Los ciberdelincuentes requieren las cantidades de rescate entre $200 y $10.000.	**Reducir el riesgo de exponerse al ataque**, implementando listas blancas de correo electrónico y realizar scripts de bloqueo de plugins no seguros en el navegador.
CryptoWall 2.0	2014	Se propaga mediante archivos adjuntos de correo electrónico pdf maliciosos y varios kits de exploits y utiliza TOR para ocultar la red de Comando y Control (C&C).	La primera cantidad exigida por CryptoWall 2.0 es de $500 o 500€	**Emplear herramientas de seguridad de monitoreo de red**, para evitar la ejecución de malware y prevenir el acceso a sitios maliciosos.
CryptoWall 3.0	2015	Utiliza I2P (Proyecto de Internet Invisible) para el anonimato, obtiene acceso a la escala de privilegios en el Sistema por el uso de Exploit, deshabilita muchas características de seguridad del Sistema principal y utiliza exclusivamente TOR para pagos.	Requieren como rescate de la información el valor de $500 pagables en 2.33 al cambio Bitcoins dentro de las 170 horas de realizada el cifrado, luego pasada las horas indicadas el valor se duplica.	**Realizar respaldos de información de la empresa**, donde se deben de realizar copias de seguridad (Backups) de la información y asegurarse que unidades de respaldo solo se conecten a los equipos para realizar mencionada copia.

Nombre	**Año Creación**	**Características de ataque**	**Método de Rescate**	**Estrategia(s) recomendada(s) a aplicarse**
CryptoWall 4.0	2015	Cifra los nombres de archivos ya cifrados, y les cambia el nombre al archivo, lo que hace más difícil de descifrar mencionados archivos que necesitan ser recuperados.	Para recuperar la información requieren un pago de 1,83 Bitcoin que equivale a 600 euros y puede variar incluso llegando a superar los $10.000.	**Emplear herramientas de monitoreo de red y anti-malware**, que permita detectar actividades sospechosas en la red.
TeslaCrypt	2015	Este tipo de ataque cifra varios tipos de archivos como documentos, imágenes y archivos de base de datos, utilizando una búsqueda en profundidad, es decir, no cifra en el primer directorio al cual accede, sino hasta haber alcanzado el directorio más profundo. El ransomware fue dirigido inicialmente a la comunidad de los videojuegos.	El rescate de pago se puede realizar por Sistema Paypal o por Bitcoin, y cuesta alrededor de $1000 el ransoware por PayPal y $500 por Bitcoin.	**Emplear herramientas de monitoreo de red y anti-malware**, que permita detectar actividades sospechosas en la red.
CTB-Locker	2014	Utiliza TOR exclusivamente para sus servidores C2 y sólo se conecta al C2 después de cifrar los archivos de las víctimas, los componentes de TOR están incrustados en el malware. Utiliza Criptografía de	Requieren como rescate alrededor de 8 Bitcoins, equivale a **1680 dólares** en la actualidad.	**Dividir y aislar la red de la empresa**, a través de segmentos de red y aplicar herramientas de monitoreo de red.

Nombre	Año Creación	Características de ataque	Método de Rescate	Estrategia(s) recomendada(s) a aplicarse
		Curva Elíptica, TOR y Bitcoin.		
CryptoLocker	2013	Este ransomware se filtra por medio del correo electrónico, es decir, si el usuario hace clic en el ejecutable adjunto al correo, inmediatamente comienza a analizar las unidades de red, cambia el nombre de todos los archivos, carpetas y los cifra. Obtiene una clave pública de C & C	El sistema de pagos es por Bitcoins y se encuentra alrededor de $300.	**Reducir el riesgo de exponerse al ataque**, implementando listas blancas de correo electrónico y realizar scripts de bloqueo de plugins no seguros en el navegador. **Dividir y aislar la red de la empresa**, a través de segmentos de red y aplicar herramientas de monitoreo de red.
Locky	2016	Se propaga a través de correos electrónicos de Spam que incluye documentos maliciosos de Microsoft Office o archivos adjuntos comprimidos que contienen macros o JavaScript por ejemplo .rar .zip que anteriormente estaban asociados con troyanos bancarios como Dridex y Pony.	El sistema de pagos es por Bitcoins y los precios están alrededor de 0,5 a 1 Bitcoin, donde cada Bitcoin aproximadamente e encuentra a $400.	**Reducir el riesgo de exponerse al ataque**, implementando listas blancas de correo electrónico y realizar scripts de bloqueo de plugins no seguros en el navegador. **Dividir y aislar la red de la empresa**, a través de segmentos de red y aplicar herramientas de monitoreo de red.

Fuente: Elaboración propia adaptado de Kaspersky (2016); Masfield-Devine (2016)