ANÁLISIS DE ATAQUES RANSOMWARE EN SERVIDORES WEB, LINUX Y WINDOWS

AUTORES:

Ingrid Chilán González[1]
Francisco Bolaños Burgos[2]
Navira Angulo Murillo[3]
Gabriel Rodolfo García Murillo[4]

DIRECCIÓN PARA CORRESPONDENCIA: ichilan@uees.edu.ec

Fecha de recepción: 10-12-2018

Fecha de aceptación: 21-12-2018

RESUMEN

El presente trabajo realiza un análisis de revisión bibliográfica de ataques ransomware en Servidores Web basados en Sistemas Operativos Linux y Windows. Por ello se realizó un análisis comparativo de vulnerabilidad de los Servidores de aplicaciones JBoss, Apache y estructura de base de datos Redis. Los resultados evidencian que los ataques con mayor frecuencia están dirigidos a los Hospitales teniendo en cuenta que los cibercriminales suelen pedir entre $200 y $500 dólares para restaurar los archivos, para el caso del ransomware Samsam para Windows, el atacante interviene la red de la organización vía SSH se autentica al Servidor JBoos. A partir del estudio realizado se puede concluir con una matriz de análisis, de ataques ransomware de varias familias CTB-loker, SamSam, CryptoWall 4.0, Linux.Enconder y FairWare y un listado de herramientas de alerta temprana contra ataques ransomware visto que cifran los directorios de los Sitios Web, por ende permite plantear trabajos futuros de nuevos tipos de ransomware por medio de herramientas de simulación.

PALABRAS CLAVE: Ransomware; Servidor Web; Linux; Windows.

ANALYSIS OF RANSOMWARE ATTACKS ON WEB SERVERS, LINUX AND WINDOWS

ABSTRACT

The present work performs an analysis of bibliographic review of ransomware attacks in Web Servers based on Linux and Windows Operating Systems. Therefore, a comparative vulnerability analysis of the JBoss Application Servers, Apache and Redis database structure was carried out. The results show that the most frequent attacks are directed to Hospitals taking into account that

[1] Maestrante de Auditoria de Tecnologías de Información, Universidad Espíritu Santo – Ecuador.
[2] Maestrante de Auditoria de Tecnologías de Información, Universidad Espíritu Santo – Ecuador. E-mail: fcobolanos@uees.edu.ec
[3]
[4]

cybercriminals usually request between $ 200 and $ 500 dollars to restore the files, for the Samsam for Windows ransomware case, the attacker intervenes the organization's network via SSH authenticates to the JBoos Server. From the study carried out it can be concluded with a matrix of analysis, ransomware attacks of several families CTB-loker, SamSam, CryptoWall 4.0, Linux. Enconder and FairWare and a list of tools for early warning against ransomware attacks seen that encrypt the directories of the Websites, therefore allows to propose future works of new types of ransomware by means of simulation tools.

KEYWORDS: Ransomware; Web Server; Linux; Windows.

INTRODUCCIÓN

Shukla, Mondal, and Lodha (2016); Bhushan y Singh (2016), señalan que en la actualidad los ataques ransomware se están convirtiendo en un problema frecuente de seguridad, para las empresas y usuarios finales de computadoras de escritorio, móvil, laptop, así como para los hospitales, escuelas, Gubernamentales u otras instituciones públicas y privadas con información sensible y confidencial.Es decir, el Ransomware es un malware comparado como otros virus informáticos como el caballo de troya, gusanos y software espía. Respecto a Bhardwaj, Avasthi, Sastry, and Subrahmanyam (2016);Luo and Liao (2016); Kansagra, Kumhar, and Jha (2016)mencionan,que anteriormente se utilizaba la criptografía para proteger la información. Sin embargo, aparece el ransomware para extorsionar a la víctima mediante el cifrado de su valiosa información.

Brewer (2016); Sittig and Singh (2016) señalan que más de cuatro millones de ataques ransomware se dieron en el segundo trimestre del 2015 con la cantidad de 1.2 millones de dólares, así como para el sector de salud las amenaza ransomware es mayor pues no es suficiente con enviarles un correo electrónico a los empleados para evitar ser atacados. Sin embargo Symantec (2016) informa aproximadamente el 0,2 % del total de ataques a finales de 2014 la cifra alcanzó el 4 % siendo el doble de ataques en el 2013, por lo tanto se registraron 8274 casos de ransomware para después aumentar la cifra 45 veces de 373.342 en el periodo del 2014, en este mismo año liberó el crypto-ransomware considerado mucho más dañino por lo tanto cifra los archivos personales y guarda las claves para descifrarlos en un sitio web externo. Así mismo del análisis locker vs crypto ransomware puesto que cada mes aumenta los ataques crypto ransomware en los últimos 12 meses se detectó el 64 % basado en archivos binarios mientras, que el 36 % restante por locker ransomware (Sharma, Zawar, & Patil, 2016).

En cuanto a las vulnerabilidades en los servidores Linux,Krebs (2015);Cabaj, Gawkowski, Grochowski, and Osojca (2015)exponen, basado en los intentos de conexión de la forma que un exploit intenta infiltrarse en los ordenadores de las víctimas, así como los servidores comprometidos utiliza el protocolo HTTP, de los cuales los archivos son cifrados por medio del CryptoWall a causa del administrador web proporciona. Así mismo Constantin (2015); Kovalev, Otrashkevich, Sidorov, and Rassokhin (2014) exponen de la expansión en los ataques a servidores web, es decir fue descubierto por investigadores de malware por los antivirus Doctor Web y Yandex utilizaron una campaña masiva de infección en el tercer trimestre del 2013.

Respecto a Shahzad, Shahzad, and Farooq (2013) exponen que recientemente se detectaron 114 malware para Linux, considerado con una precisión del 96 % en actividades maliciosas por otro lado menciona Bitdefender (2016a)los ataques a servidores web están orientados en robar datos; como Sitios web desarrollados con la tecnología de LAMP (Linux, Apache, Mysql, y PHP),

Gestor de contenidos como Wordpress, Joomla y Drupal para Windows y Linux tienen el mismo impacto de vulnerabilidad con el nuevo ransomware de la familia CTB loker en efecto McAfee (2015) informa un aumento del 165 % durante el primer trimestre. Así mismo el Linux.esconder1 es un tipo de ransomware que utiliza un algoritmo de cifrado de alta seguridad y criptografía de clave pública, es decir este malware cifra la página de inicio y las carpetas asociadas para luego pedir un rescate Bonderud (2016). Además Pauli (2016) indica, de los ataques SamSam ransomware están dirigidos a los servidores JBoss vulnerables de los Hospitales. Así pues Lawrence (2016) indica sobre ataques Fairware ransomware en servidores web Linux, cifrando la carpeta root, basado en las configuraciones de base de datos Redis. En efecto, tiene que pagar dos bitcoins para recuperarlos.

El presente trabajo tiene como objetivo analizar los ataques Ransomware de Servidores Web en, Sistemas Operativos basados en Linux y Windows, en referencia a la revisión bibliográfica comparativa de estudios realizados por expertos, Así mismo de varios tipos de ransomware a causa de ataques frecuentes dirigidos a sectores de Salud, Educación, Organizaciones y Gobiernos dependiendo de la criticidad del negocio para los atacantes.

MARCO TEÓRICO

Ransomware

Pathak (2016); Dubell (2016); Di-Lorio et al. (2015) definen el Ransomware como una variante reciente del scareware, este tipo de malware pretende extorsionar a la víctima con el fin de infectar y tomar el control de los computadores con su valiosa información. En efecto pedir un rescate de dinero para descifrar la información. Por otro lado Sgandurra, Muñoz, Mohsen, and Lupu (2016) y Luo and Liao (2007) Señalan, que el ransomware bloquea o encripta los documentos y archivos para impedir el acceso; por medio de una clave secreta sólo conocida por los autores del malware después con la publicación del rescate muestra a través de un archivo de texto o sitio web, este tipo de malware obliga a la víctima a pagar el rescate exigido, puede ser entregado por un kit de exploit para utilizar las vulnerabilidades en el equipo infectado conocido como Cryptovirology. Así pues Kharraz, Robertson, Balzarotti, Bilge, and Kirda (2014) demuestra con un análisis de una muestra de 1.359 de familia ransomware de similares características de ataques a equipos y archivos.

Hampton and Baig (2015) manifiestan que el primer ransomware registrado es el PC Cyborgtroyano (SIDA) pionero en el año 1989, fue distribuido vía correo electrónico, enviando a miles de personas y empresas para luego instalar AUTOEXC.BAT en los equipos de las víctimas. Es decir, el cibercriminal realiza un conteo del número de veces del reinicio de los equipos que los usuarios realizan, utilizando clave simétrica al cifrar y descifrar los datos por ende la clave está en algún lugar del malware. Más tarde en 1996Shillam (2012),se creó el cifrado asimétrico visto que los autores del ransomware solo conocían la clave de descifrado, después esta idea fue desarrollada para prueba de ataques contra un Macintosh SE / 30 por Adam Young y Moti Yung.

En cuanto a Salvi and Kerkar (2015) Indican, que en el 2006 las organizaciones criminales empezaron con la encriptación ASA asimétrica efectiva, troyanos como archivo, Gpcode, TROJ.RANSOM.A, Krotten, Archive y Cryzip, para luego utilizar esquemas de encriptación RSA, con tamaños de clave cada vez mayores. Sin embargo, Aziz (2016). Menciona para tener una combinación de algoritmo simétrico como AES y Algoritmo de cifrado asimétrico como RSA resultará en un nuevo método llamado FEK (Archivo de clave de encriptación), está técnica

funciona más rápido para los hackers en definitiva, pueden cifrar y descifrar archivos de gran cantidad y tamaño durante el proceso de infección.

En relación con los atacantes de varias familias de ransomware han desarrollado con diferentes lenguajes de programación como JavaScript, PHP, PowerShell o Python, para desarrollar aplicaciones de escritorio para Windows, Linux y Mac OS X con JavaScript por lo tanto, para evadir la detección es decir la adopción de nuevas técnicas demuestra que están evolucionando constantemente para mantener su posición y seguir siendo rentables (Symantec, 2016).

Sgandurra et al., (2016), Menciona que el primer ransomware se creó en año 2006 con el nombre Archiveus, el cual realiza cifrado de tipo RSA, más adelante se encuentra la Tabla1 con la cronología de ransomware, listado con el año y características de los tipos de malware.

Tabla1: Cronología de Ransomware

Nombre	Año	Características
Archiveus	2006	Primer Ransomware para usar el cifrado RSA
CryptLocker	Sept. 2013	Obtiene una clave pública de C & C
CryptoWall	Nov. 2013	Requiere que el navegador TOR haga pagos
Critroni	Jul2014	Similar a CryptoWall
TorrentLocker	Ag 2014	Stealthiness: Conexiones SSH
CTB-Locker	Dec. 2014	Utiliza Criptografía de Curva Elíptica, TOR y Bitcoins
CryptoWall 3.0	Jun2015	Utiliza exclusivamente TOR para el pago
TeslaCrypt	Feb. 2015	Añade la opción PayPal para pagar con tarjetas de crédito

Fuente:(Sgandurra et al., 2016)

Tabla1: Cronología de Ransomware

Nombre	Año	Características
Hidden Tear	Ago. 2015	Ransomware de Código libre para fines educativos
CryptoWall 4.0	Nov. 2015	Cifra también nombres de archivo
Linux.Encoder.1	Nov. 2015	Cifra los directorios de Linux y del sitio web
DMA-Locker	Jun. 2016	función de descifrado incorporada
CTB-Locker para WebSites	Febr. 2016	Targets Wordpress
Samas	Mar 2016	Para servidores JBOSS
Jigsaw	Abr. 2016	Presiona a las víctimas para que paguen el rescate
CryptXXX	May 2016	Monitorea las actividades y evade el entorno de la caja de seguridad

RAA	Jun 2016	Escrito en Javascript
Stampado	Ju 2016	Promovido a través de campañas publicitarias de Dark web

Fuente:(Sgandurra et al., 2016)

Ataques por tipo de Ransomware en servidor Web

CryptoWall se obtuvo de un equipo infectado en la facultad, proporcionados por la comunidad de seguridad desde la perspectiva del usuario. Ahora bien existen dos formas conocidas que puede infectar el equipo de correo electrónico, spam con malware, archivos adjuntos y SitiosWeb donde instala un Exploit Kitpara ataques Drive-by-Download. Después la vulnerabilidad de Java Runtime Environment (JRE) y reproductor Adobe Flash, En la Fig2 muestra la secuencia de los proxis comprometidos, mediante la generación de clave en el servidor y el servidor HoneyClient por medio de la red e Internet, en efecto el tipo de Kit de exploración está evolucionando, como el ransomware más destructiva en internet, como los infectados de más de 600.000 sistemas entre marzo y agosto con 5.250 millones de archivos cifrados. Cabaj et al. (2015),Kiire and Goto (2016); Harshada and Ravindra (2015). Así pues Thakkar (2014) menciona que el malware, está extendido a través de mecanismos de infección como kits de exploración de navegadores, enlaces maliciosos, descargas, archivos adjuntos, correo electrónicos maliciosos, envíos enlaces de descargas maliciosos por medio de botnes de spam, se incrementos a mediados de mayo del 2014frecuentemente spam de Cutwail.

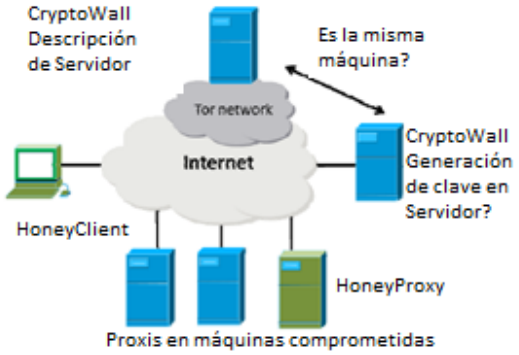


Fig2: infraestructura de CryptoWall.

Fuente:(Cabaj et al., 2015)

CTB-Locker desarrollado en PHP, ransomware orientado en la web y para computadoras de versión Windows. En el caso de un Servidor Web este malware reemplaza el archivo index.php del Sitio Web y crea una llamada cryto en el directorio es decir contiene los archivos adicionales de PHP que los cifra en el directorio Web, cuando se recibe una solicitud diseñada por un atacante.(Scaife, Carter, Traynor, & Butler, 2016). En la Fig3 muestra los porcentajes de las victimas detectadas por este tipo de ataque, obteniendo el mayor porcentaje de 50% en Norteamérica y menor de 2% en África, consultadas en el informe de (McAfee, 2015).

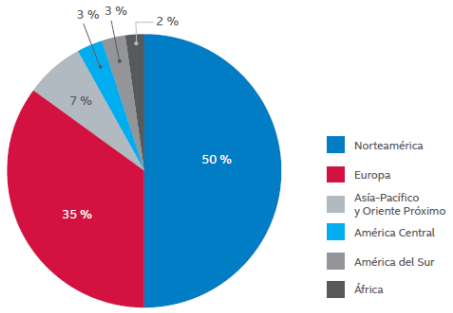


Fig3:Víctimas de CTB-locker detectadas.

Fuente:(McAfee, 2015)

Linux. Esconder es un ransomware para Sistemas Operativos Linux, tipo de ataque contra Servidores Web, actualmente está afectando en los últimos meses. Ahora bien existen tres versiones Linux.Encoder1, Linux.Encoder2 y Linux.Encoder3 están logrado descifrar esta información y proporcionar una herramienta de descifrado Linux.Enconder libre para cualquier victima infectada. Además en Internet se basa en Servidores Web Linux-powered, a veces se puede alojar más de un Sitio Web que podrían verse afectados.(Bidefender, 2015).Después Herzog and Balmas (2016) mencionan que hicieron una de las modificaciones al malware que eventualmente involucró el hashing de la marca de tiempo 8 veces y usar el resultado como una clave AES. Por un ladoDR.WED (2016) comenta sobre el ransomware Linux.Enconder.3 es cifrado para Linux escrito en C luego usando la biblioteca Polar SSL es decir se trata de una modificación avanzada del Linux.Enconder.1 y Linux.Enconder2.

En particular, para cifrar cada archivo el troyano genera una clave AES después que los archivos son encriptados usando un algoritmo AES-CBC-128.Luego se adjuntan con la extensión encrypted en cada directorio que contiene los archivos cifrados README_FOR_DECRYPT.txt con una petición de rescate. En efecto para el descifrado, Linux.Encoder.1 utilizará una clave privada RSA para recuperar las claves AES de archivos cifrados.(Herzog & Balmas, 2016).

Samsam es un ransomware que utiliza vulnerabilidades en Servidores de aplicaciones JBoss, WebSphere y Weblogic, con objetos de datos en Java, una vez que el atacante obtiene el control del servidor carga JexBoss para permitir el acceso a través de backdoor einstalar Samsam, y normalmente hay más de una webshell en los servidores comprometidos de JBoss, por ende existe variedad de backdoors en el mismo servidor con nombres como "mela". "Shellinvoker", "jbossinvoker", "zecmd", "cmd", "génesis" y "sh3ll".

"(Lemos, 2016).Así pues Thomson (2016) señala que este tipo de ransomware está afectando a los hospitales, escuelas, gobiernos y otras organizaciones es decir este exploits es un agujero en middleware del Servidor JBoss.

Así mismo Pauli (2016) indica que los ataques SamSam están dirigidos a los Servidores Vulnerables de los Hospitales. Por otro lado Jasper (2016) señala que recientemente un Hospital de los Ángeles en EE.UU “Hollywood Presbyterian Medical Center” tuvo que pagar $ 17.000 por un rescate para obtener la clave de descifrado y ser capaz de acceder a sus datos de nuevo. Las motivaciones para los cibercriminales para atacar un hospital están considerando la criticidad del negocio y, por supuesto, el aumento de la probabilidad de pago. Luego Beek (2016) comenta que la red del Hospital cayó durante una semana junto con la pérdida de correo electrónico y datos de los pacientes, en efecto los Cibercriminales suelen pedir entre $200 y $500 dólares para restaurar

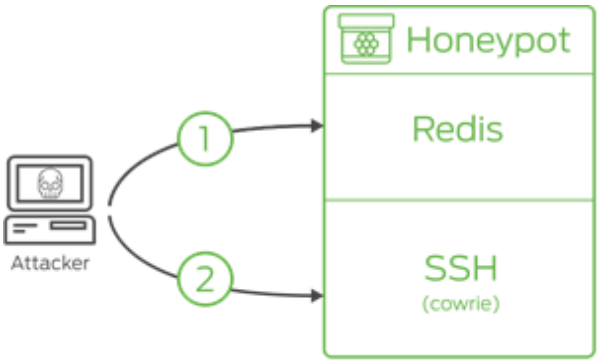
los archivos pero en este caso exigieron el pago de $3.6 millones de dólares. Así pues Kirk (2016).Señala, que el Hospital MedStar también fue atacado por los hackers, pidiendo rescate para desbloquear todas las computadoras 45 bitcoins, cerca de US $ 18.500.

Con respecto a la herramienta JexBoss es de código abierto para ser utilizadas como pruebas y de los servidores de aplicaciones JBoss, es decir una vez que tenga acceso a la red procede a cifrar varios Sistemas Operativos Windows utilizando SamSam. Además de encriptar diferentes tipos de archivos con Rijndael luego con el código de cifrado RSA-2048 bits esto no es recuperable al menos que el autor cometa error en la implementación del algoritmo de cifrado. Así mismo, el componente de RE Georg, tunnel.jsp. RE Georg es un Framework de código abierto para crear socks proxy para la comunicación, este archivo se encuentra en la versión no modificada del tunnel.jsp.(CISCO, 2016).

En cuanto a la herramienta que recolecta detalles de Active Directory, se obtuvo una lista de movimientos laterales de la red. Por una parte, permite desplegar múltiples sistemas para luego generar claves públicas y privadas. Después la clave pública para los sistemas accesibles, utilizan la secuencia de comandos barch f.bat para la distribución de los archivos y eliminación de las copias, evitando la restauración de archivos. Así pues, la muestra contiene; VSS.exe/delete como primeras funciones y de los directorios SamSam.exe, C: \ Windows \ System32 está la función de la clave pública y su ubicación en el sistema de las víctimas, además de tener dos archivos incrustados en la sesión de recurso; Del.exe y Selfdel.exe.(Beek & Furtak, 2016).

FairWare: nueva amenazaran somware para Servidores Web, basado en las configuraciones de base de datos Redis inseguras por defecto, seguidamente reemplaza la clave SSH del servidor para luego acceder a los directorios incluido el directorio Web donde se almacenan los Sitios Web en la que dejan una nota de rescate. (Constantin, 2016b). Sin embargo Lawrence (2016) señaló que Redis estaba instalado en las secciones de varias víctimas de FairWare con la clave "crackit" y dirección de correo electrónico que estaba presente en los almacenes de datos después de borrar toda la carpeta web y luego piden dos bitcoins de $1.150 para restaurarlo.

Redis: es un almacén de estructuras de base de datos en memoria, de código abierto en efecto no es recomendado acceder directamente desde internet. Considerando que se informaron alrededor de 13.000 bases de datos tenían un registro llamado "crackit" que contenía una clave SSH pública como valor asociado. Así pues, los atacantes engañaron el software al modificar las configuraciones es decir reemplazan la clave de autenticación SSH desde la cuenta raíz del Servidor.(Wright, 2016).



1) El atacante compromete la instancia Redis en el Honeypot y agrega una clave SSH para /root/.ssh/authorized:keys.
2) El atacante se registra en el Honeypot Cowrie sobre SSH usando la clave SSH agregada

Fig5. Ataque FairWare ransomware

Fuente: (Wright, 2016)

¿Qué es BITCOIN y cómo funciona?

Bitcoin es una moneda digital o electrónica en efectivo creada en el 2009 no depende de una organización está localizada en distintos lugares del mundo y utiliza un sistema de encriptación. Por consiguiente, cada transacción es anónima por este motivo es muy utilizada en el mundo de los Cibercriminales, además cuenta con aplicaciones desarrolladas para Windows, GNU/Unix y Mac OS X. En particular el usuario de Bitcoin tiene una cartera digital, una clave pública y una privada.(Moure, 2015);(Nakamoto, 2014).

Por otro lado Mehmood (2016) indica por la exigencia de rescates los cibercriminales destinan fondos para desarrollar ransomware complejos, para luego lanzarlos en una escala mucho más amplia. Symantec (2016)estimó que el 2,9% de las víctimas pagó el rescate. Más adelante, la Universidad de Kent hizo una encuesta con un resultado del 40% de las víctimas pagó el rescate por medio de Bitcoins.

Herramientas de alerta temprana de ataques Ransomware

CryptoDrop: Se centra en la detección de ransomware, a través de la supervisión de cambio en tiempo real de los datos del usuario, luego realizaron un análisis de 14 familias distintas de ransomware incluyendo 4 familias descubiertas previamente Scaife et al. (2016). Así mismo se basa en SecureDrop una fuente abierta de sistemas de presentación de denuncias que permite aceptar documentos confidenciales de fuentes anónimas a través de interfaz web (Maheswaran, Jackowitz, Wolinsky, Wang, & Ford, 2014).

BitDefender: Herramienta para descifrar los archivos de forma gratuita de los ataques ransomware Locky, TeslaCrypt, CBT-Locker y Linux.Enconder focalizadas a Servidores Web vulnerables, en Sistema Operativo Linux. (Bitdefender, 2016b); (Caragea, 2016).

EldeRan: Sistema de detección de alerta temprana para ransomware para actividades de archivos y alerta al usuario en caso de sospecha, utilizando unión de tres características (tipo de archivo, la medición de la similitud y la entropía). (Sgandurra et al., 2016).

Hidden Tear: Es una herramienta de código libre, útil para evitar pagar rescate de los archivos encriptados. Esta aplicación contiene tres carpetas; para el modo online, offline y decrypter que es utilizado para descifrar los archivos infectados. Seguidamente para el modo online tiene una configuración de un Servidor Web con lenguaje scripting, puede ser PHP o Python, es decir el servidor debe tener un archivo que escriba el parámetro GET a un archivo de texto, además está basada en Windows (García & Us, 2015)

Análisis comparativo de Ataques Ransomware entre Windows y Linux

Recogiendo lo más importante a las vulnerabilidades en Servidores Web, recientemente los atacantes ejecutan el Trojan.Ransomcrypt.AE detrás de SamSam Ransomware en Windows para atacar a toda la red de este malware. Por otro lado, las Vulnerabilidades en Sistema Operativo Linux está el Linux. Enconder que es una variante del CTB-loker cuyo objetivo principal son los

Servidores Web. Así pues, los atacantes cifran todos los Sitios Web asociados al servidor, como resultado de la mayoría de ataques están diseñadas para el Sistema Operativo Windows (Symantec, 2016).

Tabla2: Ataques a servidores web

Servidor Web	Descripción	Ataque Ransomware
WINDOWS		
Apache	Servidor web con administrador de contenido Wordpress	CTB-loker
JBoss	los servidores de aplicaciones	SamSam
JRE y Flash	Sitios web donde instala un Exploit Kit	CryptoWall 4.0
LINUX		
Apache	Servidor web con administrador de contenido Wordpress	Linux.enconder1,2,3
Redis	Herramienta de código abierto utilizado por los desarrolladores de aplicaciones web.	FairWare

Fuente:(Chilán, 2016)

CONCLUSIONES

Con la realización de este trabajo se ha podido caracterizar los ataques ransomware en Servidores Web, basados en Sistemas Operativos Linux y Windows, frecuentemente dirigidas al sector Salud, Educación y Gobierno por la criticidad del negocio, para los cibercriminales es rentable por la cantidad BITCOIN que puede recaudar por el rescate. Asimismo, el rescate en cuotas periódicas para obtener la clave para descifrar y recuperar la información de los directorios del Servidor Web y sitios web asociados. Cabe destacar el tipo de ransomware Samsam para el sistema operativo Windows es crítico ya que la red de la organización por medio de SSH se autentica ingresando al servidor JBoos.

En definitiva, con el análisis se pretende informar de las vulnerabilidades de Servidores web en Sistemas Operativos Linux y Windows, por los casos revisados de servicios y herramientas que utilizan los desarrolladores para la implementación de los servidores Apache, JBoss y Estructura de base de datos Redis, por medio de un listado de herramientas de alerta temprana contra ataques ransomware. Así mismo con listado de análisis comparativo de ataques ransomware entre Windows y Linux, visto que cifra los archivos y directorios, pertenecientes a los Servidores y Sitios Web.

Las limitaciones del presente trabajo, por ser análisis de revisión no se ha realizado una investigación estructurada, para realizar simulación de ataques ransomware, mediante herramientas para la prevención de ataques o alerta temprana. Además, no existen publicaciones de revistas académicas o científicas por ser un tema nuevo de ransomware en Servidores Web basados en Sistemas Operativos Linux y Windows. Sin embargo, se pudo realizar un análisis de

tipos de ransomware, CTB-loker, SamSam, CryptoWall 4.0, Linux.Enconder y FairWare, dirigidosa Servidores Web.

Teniendo en cuenta, como trabajo futuro se recomienda realizar investigación científica de nuevos tipos ataques de la familia ransomware. Asimismo, una simulación con las herramientas para la prevención futura y alerta temprana de ataques ransomware en Servidores web.

REFERENCIAS BIBLIOGRÁFICAS

Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016). Ransomware Digital Extortion: A Rising New Age Threat. *Indian Journal of Science and Technology, 9*, 5.

Bhushan, B., & Singh, Y. (2016). Review on Cryptovirology. *International Journal of All Research Education and Scientific Methods (IJARESM), 4*.

Bitdefender. (2016). Ransomware: How to tackle extortion attacks in 2016. Retrieved from http://www.pcadvisor.co.uk/feature/security/ransomware-how-tackle-extortion-attacks-in-2016-3633788/

Bonderud, D. (2016). New PHP Ransomware Looks to Websites for Windfall. Retrieved from https://securityintelligence.com/news/new-php-ransomware-looks-to-websites-for-windfall/

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*.

CABAJ, K., GAWKOWSKI, P., GROCHOWSKI, K., & OSOJCA, D. (2015). Network activity analysis of CryptoWall ransomware. *Warsaw University of Technology*.

Constantin, L. (2015). File-encrypting ransomware starts targeting Linux web servers. Retrieved from http://www.pcworld.com/article/3003098/business-security/file-encrypting-ransomware-starts-targeting-linux-web-servers.html

Kansagra, D., Kumhar, M., & Jha, D. (2016). Ransomware: A Threat to Cyber security. *IJCSC, 7*.

Kovalev, A., Otrashkevich, K., Sidorov, E., & Rassokhin, A. (2014). EFFUSION – A NEW SOPHISTICATED INJECTOR FOR NGINX WEB SERVERS. *VIRUS BULLETIN*.

Krebs, B. (2015). Ransomware Now Gunning for Your Web Sites. Retrieved from https://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/

Lawrence, A. (2016). New FairWare Ransomware targeting Linux Computers. Retrieved from https://www.bleepingcomputer.com/news/security/hacked-redis-servers-being-used-to-install-the-fairware-ransomware-attack/

Luo, X., & Liao, Q. (2016). Ransomware: A New Cyber Hijacking Threat to Enterprises.

Mark, W. (2016). Linux users targeted by new Linux.Encoder.1 encryption ransomware. Retrieved from http://www.markwilson.co.uk/

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

Shahzad, F., Shahzad, M., & Farooq, M. (2013). In-execution dynamic malware analysis and detection by mining information in process control blocks of Linux OS. *Information Sciences*.

Sharma, P., Zawar, S., & Patil, S. B. (2016). *RANSOMWARE ANALYSIS: INTERNET OF THINGS (IOT) SECURITY ISSUES, CHALLENGES AND OPEN PROBLEMS INTHE CONTEXT OF WORLDWIDE SCENARIO OF SECURITY OF SYSTEMS AND MALWARE ATTACKS*. Paper presented at the International conference on recent Innovation in Engineering and Management.

Shukla, M., Mondal, S., & Lodha, S. (2016). POSTER: Locally Virtualized Environment for Mitigating Ransomware Threat. *TCS Research*.

Sittig, D. F., & Singh, H. (2016). A Socio-technical Approach to Pre-venting, Mitigating, and Recovering from Ransomware Attacks.

Symantec, W. S. S. (2015). *Informe de Symantec sobre las amenazas para la seguridad de los sitios web 2015*. Retrieved from

Aziz, S. M. (2016). Ransomware in High-Risk Environments. *Department of Computing and Information Sciences*.

Beek, C. (2016). Los objetivos del ransomware en el sector salud. Retrieved from http://clustersalud.americaeconomia.com/los-objetivos-del-ransomware-en-el-sector-salud/

Beek, C., & Furtak, A. (2016). *Targeted Ransomware No Longer a Future Threat*. Retrieved from

Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016). Ransomware Digital Extortion: A Rising New Age Threat. *Indian Journal of Science and Technology, 9*, 5.

Bhushan, B., & Singh, Y. (2016). Review on Cryptovirology. *International Journal of All Research Education and Scientific Methods (IJARESM), 4*.

Bidefender. (2015). Linux Ransomware Debut Fails on Predictable Encryption Key. Retrieved from https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/

Bitdefender. (2016a). Ransomware: How to tackle extortion attacks in 2016. Retrieved from http://www.pcadvisor.co.uk/feature/security/ransomware-how-tackle-extortion-attacks-in-2016-3633788/

Bitdefender. (2016b). Third Iteration of Linux Ransomware Still not Ready for Prime-Time. Retrieved from https://labs.bitdefender.com/2016/01/third-iteration-of-linux-ransomware-still-not-ready-for-prime-time/

Bonderud, D. (2016). New PHP Ransomware Looks to Websites for Windfall. Retrieved from https://securityintelligence.com/news/new-php-ransomware-looks-to-websites-for-windfall/

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*.

Cabaj, K., Gawkowski, P., Grochowski, K., & Osojca, D. (2015). Network activity analysis of CryptoWall ransomware. *Warsaw University of Technology*.

Caragea, R. (2016). TeLeScope - real-time peering into the depths of TLS traffic from the hypervisor. *Bitdefender Labs*.

CISCO, T. (2016). SamSam: The Doctor Will See You, After He Pays The Ransom. Retrieved from http://blog.talosintel.com/2016/03/samsam-ransomware.html?m=1

Constantin, L. (2015). File-encrypting ransomware starts targeting Linux web servers. Retrieved from http://www.pcworld.com/article/3003098/business-security/file-encrypting-ransomware-starts-targeting-linux-web-servers.html

Constantin, L. (2016a). CTB-Locker ransomware hits over 100 websites. Retrieved from http://www.pcworld.com/article/3038207/security/ctb-locker-ransomware-hits-over-100-websites.html

Constantin, L. (2016b). FairWare ransomware infects servers through exposed Redis instances. *CIO (13284045)*, 9-9.

Di-Lorio, Ruiz, Alberdi, Curti, Greco, Podestá, . . . Trigo. (2015). Análisis Forense de Memoria: Malware y Evidencia Oculta.

DR.WED. (2016). Linux.enconder. Retrieved from http://vms.drweb.com/virus/?i=7910141&lng=en

Dubell, M. (2016). Building ransomware for fun and profit academic research purposes. *Language-Based Security*.

García, H. A. M., & Us, L. B. C. (2015). Hidden Tear: Análisis del primer Ransomware Open Source.

Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. *Australian Information Security Management Conference*.

Harshada, S., & Ravindra, K. (2015). Ransomware: A Cyber Extortion. *Special issues of Convergence in Computing, 2*.

Herzog, B., & Balmas, Y. (2016). Great Crypto Failures

Jasper, N. (2016). Ransomware - o uso maléfico da criptografia.

Kansagra, D., Kumhar, M., & Jha, D. (2016). Ransomware: A Threat to Cyber security. *IJCSC, 7*.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2014). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks.

Kiire, R., & Goto, S. (2016). Detecting Drive-by-Download Attacks based on HTTP Context-Types. *Proceedings of the APAN*.

Kirk, J. (2016). MedStar Health partially restores services after suspected ransomware attack. *CIO (13284045)*, 12-12.

Kovalev, A., Otrashkevich, K., Sidorov, E., & Rassokhin, A. (2014). EFFUSION – A NEW SOPHISTICATED INJECTOR FOR NGINX WEB SERVERS. *VIRUS BULLETIN*.

Krebs, B. (2015). Ransomware Now Gunning for Your Web Sites. Retrieved from https://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/

Largent, W. (2016). Ransomware: Past, Present, and Future. Retrieved from http://blog.talosintel.com/2016/04/ransomware.html

Lawrence, A. (2016). New FairWare Ransomware targeting Linux Computers. Retrieved from https://www.bleepingcomputer.com/news/security/hacked-redis-servers-being-used-to-install-the-fairware-ransomware-attack/

Lemos, R. (2016). Samsam Server-Side Ransomware Targets K-12 Schools, Hospitals. *eWeek*, 8-8.

Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention. *Information Systems Security, 16*(4), 195-202. doi:10.1080/10658980701576412

Luo, X., & Liao, Q. (2016). Ransomware: A New Cyber Hijacking Threat to Enterprises.

Maheswaran, J., Jackowitz, D., Wolinsky, D. I., Wang, L., & Ford, B. (2014). Crypto-Book: Bootstrapping Privacy Preserving Online Identities from Social Networks. *Yale University*.

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

Mehmood, S. (2016). Enterprise Survival Guide for Ransomware Attacks.

Moure, M. (2015). Secuestro de información por medio de Malware.

Nakamoto, S. (2014). Bitcoin: A Peer-to-Peer Electronic Cash System.

Pathak. (2016). A Dangerous Trend of Cybercrime: Ransomware

Growing Challenge. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*.

Pauli, D. (2016). Hospital servers in crosshairs of new ransomware strain. Retrieved from http://www.theregister.co.uk/2016/03/30/hospital_ransomware_samsam/

Salvi, H. U., & Kerkar, R. V. (2015). Ransomware: A Cyber Extortion. *Asian Journal of Convergence in Technology*.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *IEEE 36th International Conference on Distributed Computing Systems*.

Sgandurra, D., Muñoz, L., Mohsen, R., & Lupu, E. C. (2016). Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection. *Department of Computing, Imperial College London*.

Shahzad, F., Shahzad, M., & Farooq, M. (2013). In-execution dynamic malware analysis and detection by mining information in process control blocks of Linux OS. *Information Sciences*.

Sharma, P., Zawar, S., & Patil, S. B. (2016). *RANSOMWARE ANALYSIS: INTERNET OF THINGS (IOT) SECURITY ISSUES, CHALLENGES AND OPEN PROBLEMS INTHE CONTEXT OF WORLDWIDE SCENARIO OF SECURITY OF SYSTEMS AND MALWARE ATTACKS*. Paper presented at the International conference on recent Innovation in Engineering and Management.

Shillam, R. (2012). What If Your Business Was Held To Ransom?

Shukla, M., Mondal, S., & Lodha, S. (2016). POSTER: Locally Virtualized Environment for Mitigating Ransomware Threat. *TCS Research*.

Sittig, D. F., & Singh, H. (2016). A Socio-technical Approach to Pre-venting, Mitigating, and Recovering from Ransomware Attacks.

Symantec. (2016). Ransomware and Businesses 2016.

Thakkar, S. (2014). Ransomware - Exploring the Electronic form of Extortion. *Department of Computer Applications, 2*.

Thomson, I. (2016). SamSam ransomware shifts from hospitals to schools via JBoss hole. Retrieved from http://www.theregister.co.uk/2016/04/19/samsam_ransomware_in_hospitals_schools/

Wright, J. (2016). *Over 18,000 Redis Instances Targeted by Fake Ransomware*. Retrieved from https://duo.com/blog/over-18000-redis-instances-targeted-by-fake-ransomware