.Seguridad
Cultura de prevención para TI
Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

RANSOMWARE, ¿QUIÉN SECUESTRA NUESTRA INFORMACIÓN?

Miguel Ángel Mendoza López

numero-30

*Este texto es una actualización del artículo “La evolución del *ransomware*: del ochentero PC Cyborg a un servicio en venta”, publicado el 21 de agosto de 2015 en https://www.welivesecurity.com/la-es/2015/08/21/evolucion-del-ransomware/

En mayo pasado una noticia recorrió el mundo entero. Por primera vez, una nota relacionada con la

ciberseguridad acaparó los titulares, debido a un código malicioso conocido como *WannaCry*. Se trataba de otra familia de ransomware. Aunque el secuestro y la extorsión en el ámbito digital a través del software malicioso no es un tema nuevo, este *malware* contaba con la característica de gusano informático, es decir, la facultad de propagarse de forma automática a través de la explotación de vulnerabilidades en el software, algo que podemos denominar *ransomworm*.

Los propósitos por los cuales se desarrollan y propagan los códigos maliciosos han cambiado; desde modificar la funcionalidad de los sistemas y dar reconocimiento a sus creadores, hasta causar daños, corromper la información y conseguir algún otro tipo de beneficio para sus desarrolladores (principalmente ganancias económicas) en un periodo cada vez menor. En esta publicación haremos un recuento de la evolución del ransomware, desde sus primeras versiones hasta casos más recientes y los pronósticos relacionados con esta amenaza informática.

EL INICIO DEL SECUESTRO DE INFORMACIÓN

Mucho se ha hablado de las distintas campañas de propagación a nivel global. Aunque no se trata de una idea nueva, el secuestro de la información ha tomado relevancia debido al impacto que ha representado para los usuarios y empresas que se han visto afectadas negativamente. Los primeros casos de ransomware se remontan a 1989, cuando apareció el troyano PC Cyborg, un programa que ocultaba los directorios y cifraba los nombres de los archivos de la unidad de almacenamiento. Posteriormente solicitaba al usuario “renovar su licencia” con un pago en dólares. Su propagación se presentó principalmente en Europa y Estados Unidos.

En los siguientes años se identificaron nuevas versiones de programas que buscaban extorsionar a los usuarios, que a diferencia del cifrado simétrico de PC Cyborg, utilizaban algoritmos de cifrado asimétrico con claves cada vez de mayor tamaño. Por ejemplo, en 2005 se conoció GPCoder y, más tarde, sus variantes, que luego de cifrar archivos con extensiones específicas pedía un pago como rescate de la información codificada.

BLOQUEO DE PANTALLA, NUEVAS VARIANTES DEL RANSOMWARE

Eventualmente, aparecieron más códigos maliciosos que funcionaban bajo el principio de la inaccesibilidad a la información, a partir de bloquear los sistemas. Estas variantes son las denominadas LockScreen, que en lugar de modificar los archivos mediante el cifrado, se enfocaban en bloquear el acceso al equipo y la información.

Dentro de esta categoría aparece Winlock, programa malicioso que se conoció en 2010 y que luego de infectar el equipo, lo bloqueaba desplegando un mensaje en la pantalla, al tiempo que se demandaba un pago. Para obtener el código de desbloqueo, el usuario afectado debía enviar un mensaje SMS con un costo aproximado de 10 dólares.

Bajo este mismo principio, en 2012 se conoció a Reveton, el denominado “virus de la policía” que bloqueaba el acceso al sistema del usuario afectado. El programa malicioso permitía mostrar un falso mensaje supuestamente del cuerpo policiaco del país donde se propagaba la amenaza, que indicaba al

usuario haber infringido una ley, por lo que debía pagar una “multa” para restaurar el acceso normal.

AUMENTO DE LA CANTIDAD Y COMPLEJIDAD DEL RANSOMWARE

En años recientes, comenzó a observarse la proliferación de los códigos maliciosos creados de forma específica para generar ganancias económicas a sus desarrolladores. El crecimiento es tal que diariamente los Laboratorios de ESET a nivel mundial reciben alrededor de 200 mil nuevas variantes. El aumento puede identificarse en tres variables: cantidad, complejidad y diversidad.

Por ello, han aparecido nuevas oleadas de programas maliciosos que operan bajo el principio del cifrado de la información, también conocido como *criptoransomware* o FileCoders, ya que su principal propósito es codificar los archivos mediante algoritmos de cifrado. Para 2013 conocimos la relevancia de CryptoLocker, en gran medida debido a la cantidad de infecciones generadas en distintos países. Entre sus principales características se encuentra el cifrado a través de algoritmos de clave pública, enfocado únicamente de algunos tipos de extensiones de archivos y el uso de comunicaciones con el comando y control (C&C) del atacante a través de la red anónima Tor.

Casi de manera simultánea, hizo su aparición CryptoWall (una variante de Cryptolocker), que logró superar a su predecesor en el número de infecciones, en cierta medida, debido a los vectores de ataque empleados: desde *exploit kits* en navegadores y ataques *drive-by-download*, hasta el más común mediante archivos maliciosos adjuntos en correos electrónicos.

A principios de 2015 se identificaron nuevas campañas con la aparición de CTB-Locker, mismo que podía ser descargado al equipo de la víctima utilizando un TrojanDownloader; el término *downloader* se aplica para programas maliciosos cuyo propósito (generalmente único) es descargar y ejecutar software malicioso adicional e infectar un sistema. Entre sus distintas versiones, una estaba enfocada a los usuarios hispanohablantes, con mensajes escritos completamente en español.

Entre sus peculiaridades, el malware también conocido como Citrioni cifraba los archivos en el disco, unidades extraíbles y unidades de red, utilizando un algoritmo de curva elíptica no reversible para el cifrado de la información. Para mantener el anonimato del creador, se conecta a través de Tor y solicita un rescate en *bitcoins*, una de las criptomonedas más conocidas.

Posteriormente, durante 2016 nuevas familias de ransomware comenzaron a propagarse por Latinoamérica, tal es el caso de Cerber, Locky o TeslaCrypt, con importantes repercusiones en las empresas y usuarios de la región. Durante 2017, el código malicioso de mayor renombre sin duda ha sido WannaCry, también conocido como WannaCryptor que, a diferencia de sus predecesores, se puede propagar automáticamente a través de la explotación de vulnerabilidades en el sistema operativo, lo que aumenta su potencial de infección.

El caso más reciente fue el brote del malware Diskcoder.C, también conocido como ExPetr, PetrWrap, Petya, o NotPetya, el cual tiene como objetivo sobrescribir los archivos, sin cobrar el dinero del rescate.

De hecho, no brinda información de contacto de los cibercriminales ni puede proveer una clave de descifrado. Por ello, las nuevas familias de malware son diseñadas para causar daño, corromper la información y afectar de forma negativa a objetivos de interés y con un alcance global.

LA DIVERSIDAD DEL RANSOMWARE EN AUMENTO

En los últimos años, hemos visto el desarrollo de una mayor cantidad de ransomware, con mecanismos cada vez más complejos, que hacen casi imposible la recuperación la información, ya que los intentos por obtener las claves de descifrado requieren de mucho tiempo y procesamiento, debido a que los algoritmos de cifrado tienen como base la resolución de problemas matemáticos complejos.

Por ello, la última alternativa que tienen las víctimas de ransomware es el pago del rescate al cibercriminal, sin embargo no se recomienda por dos razones principales. En primer lugar, al realizar el pago del rescate no se tiene garantía ni la certeza de recuperar la información, puesto que es probable que el ciberdelincuente no realice la entrega de las claves de descifrado y por otro lado, con el pago se financia una industria cibercriminal que con más recursos puede generar más amenazas informáticas.

Aunado al crecimiento en la cantidad y complejidad del ransomware, su diversidad también ha ido en aumento. Por ejemplo, en 2014 conocimos el primer caso de malware de la familia FileCoder para Android. SimpLocker apareció en escena; su función consistía en escanear la tarjeta de almacenamiento del dispositivo móvil en busca de archivos con extensiones específicas. Del mismo modo, aparecieron más códigos maliciosos como AndroidLocker, que suplantaba soluciones de seguridad y aplicaciones legítimas para Android, con el propósito de ganar la confianza de los usuarios.

Además, otras plataformas se han convertido en objetivo de los atacantes. Durante 2015 aparecieron los primeros casos de ransomware diseñado especialmente para sistemas operativos Linux, CTB-Locker o KillDisk. Durante 2016 apareció una muestra de ransomware conocida como KeRanger, un ransomware especialmente diseñado para OS X, así como otras familias enfocadas en macOS, como la familia de ransomware Patcher durante 2017.

¿ESTAMOS ANTE UNA AMENAZA QUE LLEGÓ PARA QUEDARSE?

Es evidente que la proliferación del ransomware va en aumento y es muy probable que continúe creciendo. Los hechos y los datos nos hacen pensar que estamos ante una amenaza que estará presente en los siguientes años, entre los principales motivos, por las ganancias ilícitas que representa para sus creadores, así como la cantidad de dispositivos y usuarios que podrán verse afectados.

Una tendencia de los últimos meses es el crecimiento de ransomware que tiene como foco el denominado Internet de las cosas (IoT). Distintos dispositivos como relojes o televisores inteligentes son susceptibles de ser afectados por software malicioso de esta naturaleza, en lo que se ha denominado ransomware de las cosas (RoT). Es probable que en el futuro próximo seamos testigos de ataques a dispositivos que se conectan a Internet, incluso se vislumbran nuevos conceptos, como el *jackware*

, es decir, el secuestro de automóviles que se conectan a Internet.

Aunque el escenario parece pesimista, sin duda existen cuestiones positivas dentro del conjunto de descalabros. Podemos destacar que la seguridad de la información fue el foco de atención en el orbe, a raíz de estos ataques, lo que debería traducirse es mayores iniciativas de protección en diferentes ámbitos, teniendo como punto de partida la prevención.

Ante este panorama, la ciberseguridad se convierte en un tema cada vez más relevante en distintos ámbitos y niveles, que involucra a la iniciativa privada, los gobiernos, instituciones académicas, y por supuesto, a los usuarios. Las buenas prácticas, la tecnología de protección y la educación en temas seguridad resultan necesarios en la actualidad, todo con un objetivo fundamental: disfrutar de la tecnología en un ambiente cada vez más seguro.

REFERENCIAS

- Cobb, S. (2017). Jackware: cuando los autos conectados conocen al ransomware. *WeLiveSecurity en español.* Recuperado el 23 de agosto de 2017, de https://www.welivesecurity.com/la-es/2016/07/21/jackware-autos-conectados-ransomware
- Lipovsky, R. (2017). KillDisk apunta a Linux: demanda $250K de rescate pero no descifra los archivos. *WeLiveSecurity en español.* Recuperado el 24 de agosto de 2017, de https://www.welivesecurity.com/la-es/2017/01/05/killdisk-linux-rescate-no-descifra
- Longstaff, T. (1989). Information about the PC CYBORG (AIDS) trojan horse. *SecurityFocus*. Recuperado el 24 de agosto de 2017, de http://www.securityfocus.com/advisories/700
- Mendoza M. (2017). Panorama de ransomware en México tras el impacto de WannaCryptor. *WeLiveSecurity en español.* Recuperado el 24 de agosto de 2017, de https://www.welivesecurity.com/la-es/2017/07/26/panorama-de-ransomware-m...
- M.léveillé, M. (2017). Nuevo ransomware criptográfico afecta a macOS. *WeLiveSecurity en español.* Recuperado el 20 de agosto de 2017, de https://www.welivesecurity.com/la-es/2017/02/22/nuevo-ransomware-criptografico-afecta-macos
- Pagnotta, S. (2016). Locky, un ransomware ya presente en Latinoamérica. *WeLiveSecurity en español.* Recuperado el 24 de agosto de 2017, de https://www.welivesecurity.com/la-es/2016/02/19/locky-nuevo-ransomware-latinoamerica

SI QUIERES SABER MÁS, CONSULTA:

- Wannacry: ataque mundial y consideraciones sobre ciberseguridad
- Macro malware, campañas de propagación vigentes en México
- Tendencias de seguridad 2017, ¿estás preparado?