juventud rebelde
www.juventudrebelde.cu

Secuestro, nueva práctica de los cibercriminales **Autor:** El Mundo **Publicado:** 21/09/2017 | 06:11 pm

Secuestros digitales

Los virus informáticos conocidos como ransomware se han perfeccionado en los últimos tiempos, convirtiéndose en una seria amenaza para todos

Publicado: Miércoles 10 junio 2015 | 09:21:25 pm.

Publicado por: Yurisander Guevara

Joseph Edward, un estudiante británico de 17 años de edad, se suicidó el 22 de enero de este año porque recibió un correo electrónico que afirmaba ser de la policía de Chesire, la cual lo investigaría por «fotos indecentes» encontradas en su computadora.

El joven, que padecía autismo, tomó literalmente la amenaza contenida en el correo y se quitó la vida, sin advertir que era víctima de una estafa, pues la falsa misiva afirmaba que para evitar una investigación tendría que pagar en un plazo de 72 horas la cifra de 150 dólares, según reportó en esa fecha el diario The Telegraph.

Joseph, sin saberlo, recibió una variedad del virus informático secuestrador de información, conocido en inglés como ransomware, una de las más serias amenazas utilizadas por los cibercriminales contra empresas e individuos.

Aunque este es un caso que terminó en fatalidad por el padecimiento del joven —y que abre un debate paralelo sobre la necesidad de educar a las nuevas generaciones en el uso de las tecnologías, para que no sean víctimas de cibercriminales—, las sutiles maneras con que este tipo de software dañino afecta actualmente a Cuba y el mundo invitan a una reflexión sobre cómo mantenemos la seguridad en nuestros equipos informáticos.

Alerta Nacional

Justamente a una semana del suicidio de Joseph en Reino Unido, la empresa cubana de consultoría y seguridad informática, Segurmática, alertó en su web que circulaba por la red nacional el virus Win32.Onion, alias CBT-Locker.

Este ransomware encripta y bloquea los ficheros de la PC y de las carpetas de los recursos de red en las que tenga permisos de escritura, para luego pedir un «rescate»

monetario a cambio del acceso.

Explica la web de Segurmática (www.segurmatica.cu), que la principal vía de llegada de este virus es a través de correos electrónicos con el fichero malicioso como archivo adjunto.

Y no es solo un tipo de virus, pues tiene dañinas variantes, afirma el portal en línea.

«Dada la naturaleza polimórfica de los mismos (virus) es difícil la identificación por los antivirus, pues cambian constantemente en su comportamiento para evadir la detección», advierte Segurmática.

Abunda la empresa en su alerta que es casi impracticable el filtrado anticorreo basura, debido a que todos los virus de este tipo son distintos en cuanto a remitente, asunto, cuerpo, servidor de origen y fichero adjunto.

Eso se debe a que una buena parte del ransomware hoy se origina en la red Tor, conocida como la web profunda, de la cual se afirma contiene el 96 por ciento del contenido de Internet.

Como la red Tor está construida a partir de estrictos principios de anonimato, para las empresas que fabrican antivirus es muy difícil rastrear su origen.

CryptoLocker, CryptoDefence, CryptoWall, Accdfisa y GpCode son algunos de los ejemplos más difundidos en los mercados marginales de la web profunda.

Los datos afectados por los cibercriminales pueden incluir fotos personales, archivos, documentos, bases de datos, diagramas. Nada queda aislado de esta práctica que está creciendo, fundamentalmente, en América Latina, según afirma el sitio especializado en seguridad informática Safe and Savvy.

No obstante, existe un patrón para poder identificarlos. Miguel Gutiérrez Rodríguez,

director de la Oficina de Seguridad de Redes Informáticas (OSRI), explicó a **Juventud Rebelde** que estos virus casi siempre llegan adjuntos en formato .ZIP, el cual al descomprimirse contiene un archivo ejecutable con el ransomware.

Por eso Gutiérrez Rodríguez recomendó que lo principal es evitar abrir cualquier archivo adjunto en correos de remitentes desconocidos.

Al mismo tiempo sugirió no «pinchar» enlaces a sitios desconocidos y mantener actualizado el antivirus instalado en el ordenador.

Se deben hacer además de forma periódica, y mientras sea posible, respaldos de la información, pues un ransomware de última generación no detectado por el antivirus podría hacer que perdamos toda la información.

El directivo comentó que en caso de una infección, lo primero que debe hacer el usuario es no usar más el ordenador, evitar entrar en pánico y buscar ayuda con expertos del ramo antes de tomar la decisión que más rápido elimina estos virus y se lleva también nuestros datos: formatear la PC.

Informó Gutiérrez Rodríguez que el antivirus de Segurmática detecta y elimina la mayoría de los ransomwares conocidos, y en caso de no hacerlo puede el usuario contactar con la empresa a través del correo soporte@segurmatica.cu o a los teléfonos 7870-3536 al 38.

También pueden conectar con la OSRI al correo reportes@osri.gob.cu o a los teléfonos 7864-4041 al 44.

Consideró además el directivo que la colaboración de todos es importante. Si algún usuario detecta un nuevo tipo de virus o ve comportamientos extraños del software que utiliza es necesario que alerte a la empresa para su estudio, sentenció.

Los Pollos Hermanos

Uno de los ransomware más amenazantes de los últimos tiempos se conoce popularmente como Los pollos hermanos, nombre tomado por sus creadores de una cadena de comida rápida en la popular serie televisiva estadounidense **Breaking Bad**.

Nombrado Trojan.Cryptolocker.S, es uno de los más peligrosos virus secuestradores de información descubiertos hasta el momento. Aparecido en Australia, los usuarios afectados por este reciben un mensaje mediante un bloqueo en la pantalla de sus ordenadores donde se les indica que sus archivos han sido encriptados y que para liberarlos deben pagar 450 dólares australianos. Si no pagan, la cifra sube a mil dólares australianos.

Según Symantec, empresa que lo halló, el virus se distribuye a través de ingeniería social, haciéndose pasar como una descarga de otro archivo. De hecho, el paquete .ZIP que incluye el malware viene con un archivo .PDF para que el usuario no detecte que la descarga es falsa.

Como vemos, es el mismo comportamiento descrito por Miguel Gutiérrez Rodríguez para el ransomware encontrado en Cuba.

En todo caso, lo mejor será tomar las recomendaciones para evitar que se infesten nuestros equipos informáticos. A fin de cuentas pagar un secuestro digital solo contribuirá con el financiamiento de los cibercriminales, los que en la mayoría de los casos jamás desbloquean las terminales encriptadas.

Móviles en la mira

Desde 2002 y hasta el pasado 5 de junio en Cuba se han reportado 6 907 programas malignos, indican estadísticas de Segurmática.

Estos se dividen en 422 virus, 4 811 caballos de troya, 1625 gusanos, 24 jokes (crean efectos «humorísticos» molestos en los ordenadores) y 25 exploits, los que se aprovechan de vulnerabilidades de seguridad.

Estos datos, disponibles en la web de Segurmática, al ser desglosados por año muestran una tendencia global a la reducción en la cantidad de virus detectados. Empero, no significa que los mismos desaparezcan. De hecho han comenzado a tener como objetivo a los móviles, advierte la empresa de seguridad Symantec.

Durante mucho tiempo libre de virus, los terminales con sistema operativo Android comienzan a sufrir la aparición de este molesto software que puede encriptar la información o bloquear el aparato, afirma Symantec.

Por lo general el ransomware dedicado a Android se disfraza de aplicación y se sube a las tiendas en línea como una descarga legítima. Una vez activado por el usuario pasa un tiempo robando información personal hasta que actúa y daña el equipo.

Al igual que en los ordenadores, las empresas de seguridad informática aconsejan que los datos siempre tengan un respaldo y se evite instalar aplicaciones de origen desconocido. Al mismo tiempo, añaden, existen aplicaciones antivirus que pueden ser instaladas para proteger los terminales.

http://www.juventudrebelde.cu/suplementos/informatica/2015-06-10/secuestros-digitales