NÚMERO
2
FEBRERO
2015

BOLETIN
DE SEGURIDAD
DE LA INFORMACIÓN
BoS

Malware CryptoLocker

El **"CryptoLocker"** o "**CTB-Locker"** es un malware (Software dañino) que utiliza técnicas de cifrado para inutilizar los documentos contenidos en la computadora y dispositivos móviles del usuario. El cual se está propagando en Internet haciendo uso de enlaces engañosos, descargas de software, así como a través de correo electrónico en forma de archivos adjuntos infectados (generalmente con extensión .zip ver figura 1).

Figura 1

Cuando es ejecutado por el usuario, al abrir el adjunto infectado, comienza a encriptar todos los archivos personales detectados en la computadora, tanto en discos duros internos, como externos e incluso en las unidades de red (configuradas en la máquina del usuario, hacia otros servidores o computadores) con el objetivo de solicitar al usuario un pago o "rescate" para recuperar el acceso a su información.

¿Cómo se propaga?

Una vez que se ejecuta, se conecta a diversas URL´s (enlaces) para descargar el malware crypto-ransomware. Cuando la máquina o dispositivo móvil ya está infectado, muestra un mensaje pidiendo un "rescate" y solicitando un pago generalmente en "bitcoins" antes de que termine el tiempo señalado, o de lo contrario todos los archivos encriptados no podrán recuperarse.

Esta nueva variante utiliza 3 formas diferentes de infección:

- ✓ A través de correo electrónico (Spam) con el malware (archivos adjuntos) o enlaces maliciosos, lo que conduce a páginas que explotan las vulnerabilidades del sistema comunes.
- ✓ Mediante otro malware instalado previamente que lo descargue y ejecute automáticamente, viene con un archivo adjunto en forma de un archivo de Word o comprimido (.zip). El documento descargará el malware directamente en la máquina del usuario. Cuando se abre, el documento tratará de disfrazar como una advertencia de Microsoft Office válida indicando al usuario para habilitar macros.
- ✓ Explotando fallos en el navegador web o en el sistema operativo que permiten la ejecución de código remoto.

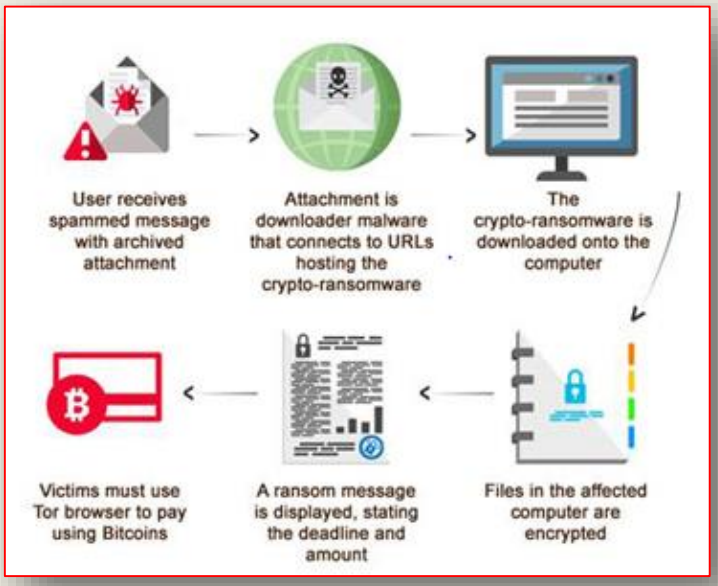

Figura 2

Se recomienda:

1) **Evite dar clic a links en un correo.** No seguir enlaces a sitios contenidos en correos no solicitados o descargar archivos adjuntos al recibir un correo relacionado a este tema. Es mejor visitar directamente el sitio al que hace referencia el link o bien asegúrese de que su navegador cuenta con reputación web para validar la veracidad del link.
2) **Asegurarse que el software antivirus de su computador está funcionando y actualizado**.
3) **Confíe en sus instintos**. Si un correo electrónico le parece sospechoso, no lo abra. Los atacantes están lanzando constantemente nuevos virus, para los cuales el software antivirus puede no tener una firma para identificarlo y bloquearlo. Si algo sobre un correo electrónico lo hace sentir incómodo, puede ser por una buena razón. No deje que la curiosidad ponga en peligro su equipo y sus datos personales.
4) **Valide siempre los remitentes de correo.** Si el correo lo envía un banco, valide con la institución si el correo que recibió es verídico. Si proviene de un remitente conocido, confirme con esa persona la validez del correo.
5) **Revise el contenido del mensaje.** Hay cosas que pueden indicar que algo está mal, una reclamación del banco o un amigo. Siempre es conveniente revisar los adjuntos con software antivirus antes de abrirlos.
6) **Respalde su información**. Desafortunadamente aún no hay una forma de desencriptar los archivos que cifra este malware. Una buena práctica es asegurar que tiene un respaldo de sus archivos de acuerdo al principio 3-2-1: tres copias – dos en diferentes medios y una en un lugar diferente. Windows tiene la característica llamada "*Volume Shadow Copy*" que permite recuperar archivos y está habilitada por defecto.
7) **Manténgase al tanto de los ataques de ingeniería social.**
8) **En caso de contagio**. De ser posible desconecte el cable de red o conexión a Internet, tan pronto se le presente la pantalla de CryptoLocker (ver ejemplo de Figura 3) y **contacte de forma inmediata a la Unidad de Informática de su Dirección o Dependencia.**

Figura 3

FUENTE

http://la.trendmicro.com
http://www.redeszone.net