¡CUIDADO! ALERTA DE RANSOMWARE

Instituto Politécnico Nacional
Coordinación General de Servicios Informáticos
Dirección de Cómputo y Comunicaciones

Usted ha escuchado en los últimos días que empresas, organizaciones o personas han sufrido pérdida de información, que ésta ha sido encriptada y que muchas veces optan por pagar para que sus archivos sean desbloqueados. Si su respuesta fue sí, entonces Usted ha escuchado noticias sobre **Ransomware.**

(**Fuente**: http://blog.fortinet.com/post/10-steps-for-protecting-yourself-from-ransomware)

¿Qué es Ransomware?

Ransomware es un tipo de malware que infecta dispositivos, redes y centros de datos e impide su uso hasta que el usuario u organización pague para que el sistema sea desbloqueado. Este ataque cibernético ha ido en aumento en los últimos años, pero no es un ataque de reciente creación. El **Ransomware** surgió desde el año de 1989 y hoy es conocido como medio de extorsión.

Este ataque cibernético, generalmente trabaja de diversas formas. Por ejemplo, **Crypto Ransomware**[1] puede infectar un sistema operativo hasta que el dispositivo es incapaz de realizar el inicio del sistema. Otro tipo de **Ransomware,** pueden encriptar un disco o conjunto de archivos; algunas versiones maliciosas tienen un contador de tiempo, que comienza a borrar archivos hasta que un **"rescate"** (ransom), haya sido pagado. **Pagar el rescate no garantiza que los archivos sean descifrados, lo único que garantiza es que los "atacantes" reciban dinero de la víctima, y en algunos casos, su información bancaria**. Además, desencriptar o rescatar los archivos no significa que la infección de malware en sí, se haya eliminado.

(**Fuente**: http://blog.fortinet.com/post/10-steps-for-protecting-yourself-from-ransomware)

¿Cómo funciona?

Busca archivos: Todos aquellos como Word, Excel, Power Point, PDF, Archivos de texto, Audio, Video, Correos electrónicos.

Busca Accesos del usuario donde tenga alojada mayor información como capetas compartidas.

Reemplaza y cifra estos archivos, lo que impide leer su contenido e incluso su ejecución.

Solicita pago en Bitcoins[2], muestra en la pantalla un mensaje indicando que la información está cifrada y pide el pago para la recuperación de los accesos.

Impacta a Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS X.

(**Fuente**: http://blog.smartekh.com/)

¿Cómo se realiza la infección?

Ransomware puede ser distribuido de diversas maneras, pero la más común es a través de falsos correos electrónicos, es decir **Phishing**[3], que contienen archivos adjuntos con contenido malicioso.

Otra forma, es a través de la descarga de software, drivers, música, etc., donde el usuario visita sitios web infectados y el malware es descargado e instalado sin conocimiento del usuario.

El Ransomware también puede propagarse en redes sociales, a través de aplicaciones basadas en web, tales como la mensajería instantánea.

(**Fuentes**: http://blog.fortinet.com/post/10-steps-for-protecting-yourself-from-ransomware
https://www.us-cert.gov/ncas/alerts/TA16-091A)

[1] Crypto Ransomware es una variante de malware que encripta archivos.
[2] Bitcoin: moneda digital y es un medio de intercambio similar a los billetes y monedas físicos.
[3] Phishing: modo de robo de información personal y/o financiera hacia el usuario, mediante la falsificación de un sitio de confianza haciéndole creer que es un sitio legítimo.

¿Por qué es tan efectivo?

¡Su computadora ha sido bloqueada!

Los creadores de Ransomware infunden miedo y pánico en sus víctimas, haciendo que el usuario haga clic en un enlace o pague un rescate. Ransomware muestra mensajes intimidatorios similares a los siguientes:

"Su computadora ha sido infectada con virus. Clic aquí para resolver el problema".

"La computadora ha sido utilizada para visitar sitios web con contenido ilegal. Para desbloquear el equipo, deberá pagar una multa de $100 USD".

"Todos los archivos en su computadora han sido encriptados. Usted debe pagar el rescate en menos de 72 horas para recuperar el acceso a sus datos".

(**Fuente**: https://www.us-cert.gov/ncas/alerts/TA16-091A)

Para más información:
https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

¿Qué debe hacer para prevenirlo?

A continuación, se encuentran algunos consejos que pueden ayudarlo a protegerse de los efectos de Ransomware:

1. **Mantenga actualizado su cliente de antivirus**.

2. Al momento de recibir un correo electrónico **revise más de una vez la dirección origen y el asunto del correo**. Si no conoce el emisor del correo o el asunto no lo abra.

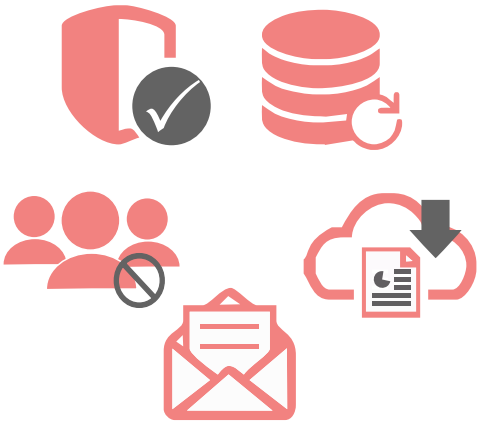
3. Si el correo electrónico contiene **un archivo adjunto, lea primero el contenido del correo** si viene en un idioma que no domine o maneje en su área de trabajo o el texto es incoherente, no abra el archivo.

4. **No abra directamente archivos adjuntos desde su correo**; primero descárguelo en su equipo de cómputo y escanéelo con el antivirus. Haga lo mismo con aquellos en una USB.

5. **Realice respaldos continuos de su información** es un esquema 3-2-1: 3 respaldos de su información, en 2 diferentes medios de almacenamiento, 1 de éstas copias en un lugar seguro.

6. **Limite los privilegios** a los usuarios en caso de manejar carpetas compartidas.

(**Fuente**: http://blog.smartekh.com/)



Referencias Bibliográficas

http://blog.fortinet.com/post/10-steps-for-protecting-yourself-from-ransomware
https://www.us-cert.gov/ncas/alerts/TA16-091A
http://blog.smartekh.com/