Ransomware

Como es bien sabido, el universo de la Internet está plagado de peligros virtuales que suelen provocar daños muy reales. Virus informáticos, phising, netbots, robo de identidad o denegación de servicio son solo algunos ejemplos de amenazas latentes. Sin embargo, quizá una de las más deleznables sea el *ransomware* (relativo al rescate). Este es un tipo de *malware* que, una vez instalado en la computadora, despliega un mensaje de alguna agencia federal (como el FBI o la policía federal) señalando una violación a la ley, por lo que el equipo quedará bloqueado a menos que se pague una multa; o quizá muestra un *pop-up* indicando que los archivos se encriptarán permanentemente si no se paga algún rescate por ellos. Lo anterior significa simplemente que la información del usuario ha quedado secuestrada y para liberarla deberá cubrir alguna suma de dinero, en algunos casos mediante una moneda virtual llamada Bitcoin o por transferencia electrónica, y que generalmente fluctúa entre los 100 y 300 dólares.

Debido que las víctimas llegan a entrar en pánico por la potencial pérdida de su información, sobre todo si no poseen respaldos, pagan por el rescate, aunque en realidad no garantice que los delincuentes envíen la llave que permita el proceso de desencriptamiento o desbloqueo. Esto ha provocado la proliferación de distintas versiones de *malware*, pues sus creadores obtienen grandes beneficios financieros. De acuerdo con Symantec, durante 2012 y utilizando solo una variante de este virus llamada Trojan.Ransomlock.G (de 16 detectadas en un lapso de dos años), se estima que los delincuentes obtuvieron ganancias cercanas a los cinco millones de dólares. Al conocer el éxito que representa esta amenaza para los *black hat hackers*, en 2013 se desarrollaron versiones más peligrosas y destructivas como el CryptoLocker, que no solo cifra archivos de usuario, sino también unidades de red o compartidas; o el Cryptowall, creada en 2014, con funciones igualmente peligrosas y que llegó a infectar más de 250 mil sistemas solo en Estados Unidos.

Existen diferentes métodos en los cuales el *ransomware* actúa: (1) por correo electrónico, donde la virtual víctima recibe un mensaje con un archivo adjunto proveniente de un usuario, conocido o no. Al abrir este archivo se ejecuta un programa desplegando una ventana de advertencia mientras de forma paralela inicia el proceso de encriptamiento de archivos (documentos, hojas de cálculo, presentaciones, imágenes, etc.); (2) a través de la web, cuando el usuario accede a alguna página cuyo contenido alberga el *malware*, que al descargarse en el equipo se ejecuta, iniciando el proceso de bloqueo o cifrado de archivos.

Es por ello que, para minimizar la presencia de esta amenaza, se recomienda tomar las siguientes medidas preventivas:

1. Mantener instalado y actualizado el antivirus.
2. Actualizar continuamente el sistema operativo. Es importante recordar que estas corrigen posibles vulnerabilidades de seguridad.
3. En caso de recibir correos electrónicos de dudosa procedencia, hay que eliminarlos. No intentar abrir archivos adjuntos o presionar clic en vínculos contenidos en el mensaje.
4. Siempre tener al menos un respaldo de información actualizado en unidades externas (disco duro externo o memorias USB).

Si a pesar de las medidas preventivas se llegara a infectar el equipo, será recomendable:

1. Inmediatamente después de recibir el mensaje en pantalla apagar el equipo de cómputo. Esto logrará detener el proceso y evitará que al menos parte de la información no sea encriptada.
2. Comunicarse con el soporte técnico para realizar una revisión de posible daño.

A pesar que estas amenazas tienen algunos años flotando por la web, últimamente han cobrado fuerza, por lo que el usuario deberá estar atento a las recomendaciones realizadas por el área de soporte técnico.

REFERENCIAS

- Constantine, L. (2014). CryptoWall ransomware held over 600K computers hostage, encrypted 5 billion files, PC-World. Tomado de www.pcworld.com/article/2600543/cryptowall-held-over-halfamillion-computers-hostage-encrypted-5-billion-files.html.
- UNAM-CERT (2014). *Boletín de Seguridad UNAM-CERT-2014-011 Crypto Ransomware*. Tomado de www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=6521
- US-CERT (2014). Alert (TA14-295A). Crypto Ransomware. Tomado de www.us-cert.gov/ncas/alerts/TA14-295A.

ENLACES DE INTERÉS:

- http://oregonstate.edu/helpdocs/safety-and-security/computer-viruses-fraud/computer-viruses/cryptolocker-dangerous-ransomware.
- http://www.sophos.com/en-us/support/knowledgebase/119006.aspx.
- http://www.symantec.com/connect/articles/recovering-ransomlocked-files-using-built-windows-tools.
- http://blogs.sophos.com/2015/03/03/anatomy-of-a-ransomware-attack-cryptolocker-cryptowall-and-how-to-stay-safe-infographic/.
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.
- http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/.