Boletín mensual de seguridad para todos

Evita el malware

Resumen

Probablemente has escuchado algunos términos como virus, troyano, *ransomware* o *rootkit* cuando la gente habla de ciberseguridad. Estos son diferentes tipos de códigos maliciosos llamados *malware* que los cibercriminales utilizan para infectar computadoras y dispositivos. Una vez instalado, ellos pueden hacer lo que quieren. Aprende qué es el malware, qué tan peligroso es y, lo más importante, qué puedes hacer para protegerte.

¿Qué es malware?

En pocas palabras, malware es un software (un programa de computadora) utilizado para realizar acciones maliciosas. Este término es la combinación de dos palabras en inglés: *malicious* y *software*. Los cibercriminales instalan malware en tus computadoras o dispositivos para obtener control de ellos. Una vez instalado, este permitirá a los criminales espiar tus actividades en línea, robar tus contraseñas, archivos o utilizar tu sistema para atacar a otros. El malware puede incluso tomar control de tus propios archivos exigiendo que pagues un rescate para recuperarlos. Mucha gente piensa que el malware es un problema exclusivo de equipos con sistema operativo Windows. Desafortunadamente, el malware puede infectar cualquier dispositivo, desde computadoras Mac y teléfonos inteligentes hasta DVR y cámaras de seguridad. Cuantas más computadoras y dispositivos cibercriminales infecten, más dinero podrán ganar. Por lo tanto, todos son un blanco, incluyéndote a ti.

Protégete a ti mismo – Detén el malware

Puedes pensar que lo único que tienes que hacer es instalar un programa de seguridad como un antivirus para estar a salvo de infecciones. Desafortunadamente, los antivirus no pueden detener todo el malware. Los cibercriminales están desarrollando constantemente malware nuevo y más sofisticado que puede evadir la detección. A su vez, los proveedores de antivirus actualizan constantemente sus productos con nuevas capacidades para detectar malware. Dado que no puedes confiar solo en el antivirus, aquí hay algunos pasos adicionales que puedes tomar para protegerte:

Los cibercriminales frecuentemente infectan computadoras y dispositivos explotando vulnerabilidades en el software. Cuanto más actual sea tu software, menos vulnerabilidades tendrán tus sistemas y será más difícil para los cibercriminales infectarlos. Asegúrate de que tu sistema operativo, aplicaciones, navegadores y sus complementos, además de tus dispositivos estén siempre actualizados con la última versión. La manera más sencilla de asegurarse de esto es habilitar las actualizaciones automáticas siempre que sea posible.

Una forma común en la que los cibercriminales infectan computadoras y dispositivos móviles es creando programas falsos o aplicaciones móviles, publicándolos en Internet, y luego engañándote para descargar e instalar alguno de ellos. Descarga e instala únicamente programas o aplicaciones desde tiendas en línea de confianza. También, mantente alejado de aplicaciones móviles que son nuevas, tienen pocas críticas positivas, rara vez se actualizan o han sido descargadas por un número reducido de personas. ¿Ya no utilizas un programa o una aplicación móvil? Bórralo.

Los cibercriminales suelen engañar a las personas para que instalen malware por ellos. Por ejemplo, podrían enviarte un correo electrónico que parezca legítimo y contenga un archivo adjunto o un enlace. Quizás el correo parezca provenir de un banco o un amigo. Sin embargo, si abrieras el archivo adjunto o dieras clic en el enlace, se activaría el código malicioso que instala malware en tu sistema. Si un mensaje crea un sentido fuerte de urgencia o parece demasiado bueno para ser verdad, podría ser un ataque. Sospecha de todo, el sentido común es a menudo la mejor defensa.

Respalda periódicamente tu sistema y archivos en la nube o almacena tus copias de seguridad fuera de línea, como en discos externos. Esto protege tus respaldos en caso de que el malware intente cifrarlos o borrarlos. Los respaldos son críticos, a menudo son la única forma de recuperarse de una infección de malware.

En última instancia, la mejor forma de defenderse del malware es mantener todos tus dispositivos actualizados, instalar antivirus confiables cuando sea posible y mantenerte alerta ante cualquier persona que intente engañarte para infectar tu sistema. Cuando todo lo demás falla, los respaldos suelen ser la única forma de recuperación.

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Editor Invitado

Lenny Zeltser *combate malware creando productos de seguridad para equipos de punto final en Minerva Labs y es instructor del Instituto SANS. Puedes encontrar a Lenny en Twitter como @lennyzeltser y en su blog de seguridad zeltser.com.*

Recursos

Ransomware:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201608_sp.pdf
Respaldos:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201708_sp.pdf
Evita el phising:	https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Spanish.pdf
Por qué instalar un antivirus:	https://www.seguridad.unam.mx/por-que-instalar-un-antivirus

 Consejo editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traductores: Célica Martínez Aponte y Raúl Abraham González Ponce