VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Marzo 2016

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- ¿Qué es el malware?
- ¿Quién crea el malware?
- Protégete a ti mismo

¿Qué es el malware?

Resumen

Es posible que hayas oído hablar de términos como virus, troyanos, ransomware o rootkits cuando la gente discute de ciberseguridad. Todas estas palabras describen lo mismo, los tipos de programas utilizados por los criminales para infectar computadoras y dispositivos. Un término común usado para describir a todos estos diferentes programas es la palabra malware. En este boletín vamos a explicar qué es el malware, quién lo crea y por qué y, lo más importante, qué puedes hacer para protegerte contra él.

Editor Invitado

Lenny Zeltser se encarga de salvaguardar las operaciones de los clientes de TI en NCR Corp y enseña a combatir el malware en el Instituto SANS. Puedes encontrar a Lenny en Twitter como **@lennyzeltser** y en su blog de seguridad **zeltser.com**.

¿Qué es el malware?

En pocas palabras, el malware es software (un programa de computadora) usado para llevar a cabo acciones maliciosas. De hecho, el término malware es una combinación de las palabras en inglés malicious y software. Los ciberdelincuentes instalan malware en tu computadora o dispositivos para obtener el control sobre ellos y tener acceso a su contenido. Una vez instalados, estos atacantes pueden usar software malicioso para espiar tus actividades en línea, robar las contraseñas o archivos e incluso utilizar el sistema para atacar a otros. El malware puede incluso negar el acceso a tus propios archivos, exigiendo que se pague al atacante un rescate para recuperar el control de ellos.

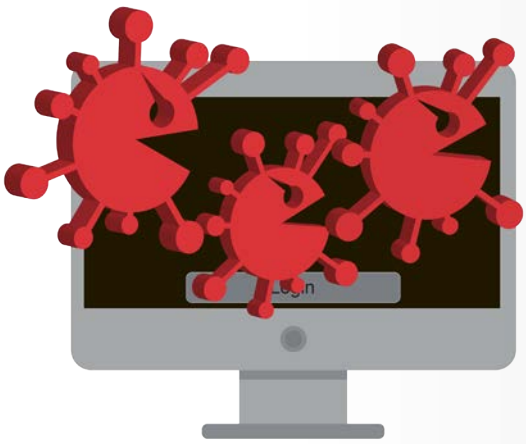
Muchas personas tienen la idea errónea de que el malware es un problema sólo para los equipos con Windows. Si bien Windows es ampliamente utilizado, volviéndolo un gran objetivo, el malware puede infectar a cualquier dispositivo, incluyendo equipos Mac, teléfonos inteligentes o tabletas. Entre más computadoras y dispositivos los cibercriminales infecten, mayor será el dinero que podrán obtener. Por lo tanto, todo el mundo es un objetivo, incluyéndote.

¿Quién crea el malware?

El malware ya no es creado por los aficionados curiosos o hackers amateurs, sino por sofisticados criminales cibernéticos. Su objetivo es hacer dinero desde la computadora o dispositivo infectado, tal vez mediante la venta de datos que te han robado, el envío de correos electrónicos de spam, ataques de denegación de servicio o la extorsión. Las personas que crean, distribuyen y se benefician de programas maliciosos pueden ir desde individuos que actúan por su cuenta, grupos criminales bien organizados o incluso organizaciones gubernamentales. Las personas que están creando hoy en día

¿Qué es el malware?

malware sofisticado se dedican a menudo a ese propósito, desarrollan software malicioso como trabajo de tiempo completo. Además, una vez que desarrollaron el malware, lo venden a otros individuos u organizaciones, incluso proporcionando a sus "clientes" actualizaciones regulares y soporte.



Protégete del malware, sé escéptico de mensajes sospechosos y mantén tus dispositivos actualizados y con un antivirus instalado.

Protégete a ti mismo

Un paso sencillo para protegerte consiste en instalar software antivirus de proveedores confiables. Dichas herramientas, algunas veces llamadas software antimalware, son diseñadas para detectar y detener al malware. Sin embargo, los antivirus no pueden bloquear o remover todos los programas maliciosos. Los cibercriminales están constantemente innovando, desarrollando malware nuevo y más sofisticado para evadir la detección. En respuesta, los proveedores de soluciones antivirus están constantemente actualizando sus productos con nuevas capacidades para detectarlo. En cierta manera, esto se ha convertido en una carrera armamentista, con ambos lados intentando vencer al contrario. Desafortunadamente, los atacantes están frecuentemente un paso adelante. Dado que no puedes confiar sólo en el antivirus, aquí hay algunos pasos que deberías tomar en cuenta para protegerte a ti mismo:

- Los ciberdelincuentes regularmente infectan computadoras o dispositivos para explotar vulnerabilidades en su software. Mientras más actualizados estén tus programas, menor cantidad de vulnerabilidades tendrán y será más difícil infectarlos. Por lo tanto, asegúrate de que tus sistemas operativos, aplicaciones y dispositivos estén habilitados para instalar actualizaciones automáticamente.
- Un medio común que los criminales usan para infectar dispositivos móviles es crear aplicaciones móviles falsas, las colocan en Internet y luego engañan a la gente para que las descarguen e instalen. Por ello, sólo descarga e instala aplicaciones de tiendas en línea confiables. Adicionalmente, sólo instala aplicaciones que hayan estado en línea por un largo tiempo, hayan sido descargados por una gran cantidad de personas y tengan numerosas reseñas positivas.
- En las computadoras, usa una cuenta estándar con privilegios limitados, en lugar de una cuenta con privilegios como "Administrador" o "root". Esto proporciona una protección adicional impidiendo que distintos tipos de malware sean capaces de instalarse por sí mismos.
- Los cibercriminales regularmente engañan a personas para que instalen ellos mismos el malware. Por ejemplo, podrían enviarte un correo electrónico simulando ser legítimo y contener un archivo adjunto o un vínculo. Tal vez el correo parezca provenir de tu banco o de un amigo. Sin embargo, si abrieras el archivo adjunto o dieras clic sobre el vínculo, activarías un código malicioso capaz de instalar malware en tu equipo. Si un mensaje trata de

¿Qué es el malware?

provocarte un fuerte sentido de urgencia, es confuso o parece demasiado bueno para ser verdad, podría tratarse de un ataque. Sé precavido, regularmente el sentido común es tu mejor defensa.

- Realiza periódicamente respaldos de tu equipo y archivos en servicios de almacenamiento en la nube o almacena tus respaldos en medios no conectados a Internet, como discos duros externos; así proteges tus respaldos en caso de que algún malware intente cifrarlos o borrarlos. Los respaldos son importantes, con frecuencia son la única forma de recuperarte de una infección de malware.

Finalmente, la mejor forma de defenderte contra el malware es mantener tus programas actualizados, instalar un software antivirus confiable de proveedores reconocidos y estar alerta en caso de que alguien intente engañarte o confundirte para infectar tu sistema.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

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

Recursos

¿Qué es malware?:	http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=193
Códigos maliciosos:	http://revista.seguridad.unam.mx/numero-01/c%C3%B3digos-maliciosos
Malware a través de correo electrónico:	http://revista.seguridad.unam.mx/numero-03/malware-traves-del-correo-electronico
Proyecto Malware:	http://www.malware.unam.mx/

Antivirus, una herramienta para nuestra seguridad:

http://revista.seguridad.unam.mx/numero-04/antivirus-una-herramienta-indispensable-para-nuestra-seguridad

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción: Mario Vasquez, Oscar Flores, Katia Rodríguez