VERSIÓN EN ESPAÑOL

OUCH! | Febrero 2014

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Qué es malware
- Quién y por qué
- Medidas de protección

¿Qué es el malware?

Resumen

Es posible que hayas oído hablar de términos como virus, gusano, troyano o rootkit cuando la gente habla sobre seguridad cibernética. Estos términos describen los tipos de programas utilizados por los cibercriminales para infectar y tomar el control de computadores y dispositivos móviles. Hoy en día estos diferentes términos se refieren a malware. En este boletín vamos a explicar qué es el malware, quién lo desarrolla, sus vías de propagación y qué podemos hacer para protegernos.

Editor Invitado

Lenny Zeltser es especialista en la protección de TI de los clientes del corporativo NCR y enseña medidas para combatir malware en el Instituto SANS. Lenny está en Twitter como **@lennyzeltser** y escribe en el blog de seguridad **blog.zeltser.com**.

Qué es el malware

En pocas palabras, el malware es un software, un programa de computadora utilizado para llevar a cabo acciones maliciosas. El término malware es una combinación de las palabras software y malicioso. El objetivo final de la mayoría de los cibercriminales es instalar malware en las computadoras o dispositivos móviles. Una vez instalados, estos atacantes pueden obtener potencialmente el control completo sobre ellos. Mucha gente tiene la idea errónea de que el malware solo es un problema que se presenta en las computadoras Windows. Mientras que Windows es ampliamente utilizado, el malware puede infectar a cualquier dispositivo informático, incluyendo teléfonos inteligentes y tabletas. De hecho, la prevalencia de software malicioso que infecta los dispositivos móviles es cada vez mayor. Además, recuerda que todo el mundo puede ser blanco de este tipo de ataques. Para los ciberdelincuentes, entre más computadotas logran infectar, más ganancias obtendrán. Por lo general, a los atacantes no les importa a quién infectar, sino a cuántas personas puedan alcanzar.

Quién y por qué

El malware ya no es creado sólo por curiosos o hackers aficionados, sino por sofisticados criminales cibernéticos para ayudarles a alcanzar metas específicas. Estos objetivos pueden incluir el robo de datos confidenciales, nombres de usuarios y contraseñas, envío de correos electrónicos de spam, lanzamiento de ataques de denegación de servicio y la extorsión o el robo de identidad. Por ejemplo, el malware conocido como Cryptolocker es utilizado por los ciberdelincuentes para infectar y cifrar todos los archivos de las computadoras. Una vez infectado y cifrado el equipo, estos atacantes exigen un rescate a cambio de descifrar los archivos.

¿Qué es el malware?

Las personas que crean, implementan y se benefician de programas maliciosos, pueden variar desde individuos que actúan por su cuenta a grupos criminales bien organizados u organizaciones gubernamentales, incluso. Además, para las personas que crean el software malicioso sofisticado de hoy, es un trabajo de tiempo completo. De hecho, una vez que desarrollan programas maliciosos, frecuentemente los venden a otras personas u organizaciones y proporcionan actualizaciones y soporte de manera periódica a sus clientes. Una vez comprado, otros criminales ganan dinero mediante la instalación del malware en millones de sistemas de víctimas desprevenidas creando una botnet con los sistemas infectados. Esta red de computadoras infectadas se convierte en un ejército controlado de forma remota, el ciberdelincuente la utiliza para sus propios fines o vende las máquinas infectadas a otros criminales cibernéticos.

La mejor manera de protegerte contra el malware es asegúrandote de que tus dispositivos se mantengan actualizados, que tengan la última versión de antivirus y estar alerta sobre ataques.

Medidas de protección

El primer paso para la protección de tu computadora y dispositivos móviles contra el malware es instalar el software antivirus de proveedores de confianza. Un antivirus es un software de seguridad diseñado para detectar y detener el software malicioso. Sin embargo, un antivirus no puede bloquear o eliminar todo el malware. Los atacantes cibernéticos están constantemente innovando, desarrollando nuevas y más sofisticados ataques que podrían pasar por alto ante los programas antivirus. A su vez, los vendedores de antivirus están constantemente actualizando sus productos con nuevas capacidades para detectar nuevos tipos de malware. En muchos sentidos, se ha convertido en una carrera armamentista con ambos lados intentando burlar al otro. Por desgracia, los cibercriminales casi siempre tienen las de ganar. Por tal motivo, recuerda que mientras los antivirus detectan y bloquean una gran cantidad de malware, los atacantes están creando siempre nuevas versiones que pueden pasar desapercibidas. Como resultado de esto, no puedes confiar sólo en un antivirus para protegerte, es necesario tomar medidas adicionales.

En primer lugar, asegúrate de que tus sistemas operativos y aplicaciones estén habilitadas para instalar automáticamente las actualizaciones de seguridad. Mientras más actualizado esté tu software, más difícil es para los ciberdelincuentes infectar tu computadora o dispositivos móviles.

En segundo lugar, recuerda que tú eres una de las mejores defensas contra el malware. Comúnmente, las infecciones de malware implican ingeniería social, en donde los atacantes engañan a las víctimas para que instalen programas maliciosos. Un ejemplo común son los ataques de phishing, estos son mensajes de correo electrónico que parecen ser legítimos pero que en realidad son falsificaciones diseñadas para poder engañar e infectar computadoras. Por ejemplo, un atacante

¿Qué es el malware?

puede enviarte un correo electrónico simulando provenir de tu banco y pidiéndote que des clic en el enlace. Si lo haces, te lleva automáticamente a un sitio que intenta hackear o infectar tu computadora. Quizás recibas por correo una notificación de que tu paquete no pudo ser entregado, pidiéndote que abras el seguimiento de documentos adjuntos y, al hacerlo, tu computadora se infecta.

Los ataques de ingeniería social también ocurren por medio de otras tecnologías, como el teléfono. Por ejemplo, los atacantes pueden llamarte pretendiendo ser del soporte técnico de Microsoft e informarte que tu computadora está infectada. Su historia es una mentira, tu computadora está bien. Su objetivo es engañarte para creer que está infectada y luego hacer que les des acceso remoto a tu sistema o para que compres un software de seguridad falso. Utiliza el sentido común. Si un mensaje o llamada parece extraña, sospechosa o demasiado buena para ser verdad, probablemente se trate de un engaño.

La mejor manera de protegerte es mantener tu sistema actualizado, instalar un software antivirus confiable y estar alerta sobre personas que quieran engañarte para infectar tu computadora.

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

Más sobre phishing:

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_sp.pdf

Más sobre mantener tu equipo seguro:

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201212_sp.pdf

Poster Formas en las que eres vulnerable:

http://www.seguridad.unam.mx/noticia/?noti=806

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Miguel Bautista y Jazmín López