VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Abril 2014

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Editor invitado
- ¿Por qué eres un objetivo?
- Protégete

Sí, en realidad sí eres un objetivo

Introducción

Un concepto erróneo que muchas personas tienen, es no creer que sean el objetivo de los criminales cibernéticos, que ellos mismos o sus equipos no tengan algún valor. Nada podría estar más lejos de la verdad. Si tienes un equipo, dispositivo móvil, una cuenta asociada a un correo electrónico, tarjeta de crédito o cualquier otro tipo de actividad en línea, tú tienes un valor monetario para los criminales cibernéticos. En este boletín te explicamos por qué eres un objetivo, cómo estás siendo atacado y qué puedes hacer para protegerte.

Editor Invitado

Eric Conrad es Presidente y Director General de Tecnología (CTO) de Backshore Communications, autor de la segunda edición del libro CISSP Study Guide y de Eleventh Hour CISSP. Participó como coautor del sexto día del curso Monitoreo Continuo y Operaciones de Seguridad (SEC511) del SANS.

¿Por qué eres un objetivo?

Delitos como fraudes, robo de identidad o extorsiones han existido desde que surgieron las civilizaciones; son parte de nuestro día a día. El objetivo de los criminales siempre ha sido el mismo, hacer tanto dinero como sea posible de la manera más sencilla y con el menor riesgo. Anteriormente era difícil porque los delincuentes estaban limitados por su ubicación y tenían que interactuar físicamente con sus víctimas. Esto no sólo los limitaba en cuanto a quiénes podían elegir como blancos, también los exponía a un gran riesgo. Sin embargo, el crimen ha cambiado radicalmente con la aparición de Internet y la tecnología en línea. Ahora los criminales cibernéticos pueden llegar fácilmente a cualquier persona en el mundo, a un bajo costo o inclusive sin costo alguno y con muy poco riesgo. Actualmente, los criminales cibernéticos se han vuelto altamente organizados y eficientes, lo que les permite ser más efectivos que nunca.

Los criminales cibernéticos saben que entre más tarjetas de crédito roben, más cuentas logren hackear o más contraseñas obtengan, mayor dinero harán. Literalmente intentan hackear a cualquier persona conectada a Internet, incluyéndote. Hackear a millones de personas alrededor del mundo quizás pueda parecer mucho trabajo, pero es sorprendentemente fácil, ya que utilizan herramientas automatizadas que realizan todo el trabajo. Por ejemplo, pueden diseñar una base de datos con millones de correos electrónicos y usar una herramienta automática para enviar mensajes de phishing a cada una de las direcciones de correo. El costo por enviar correos electrónicos es casi nulo, ellos simplemente usan otro equipo comprometido (incluso podría ser el tuyo), para realizar el trabajo sucio. Éste es otro ejemplo del porqué tus dispositivos tienen valor, ya que como mínimo, pueden ser usados para comprometer o dañar a otros. Finalmente, los delincuentes

Sí, en realidad sí eres un objetivo

no saben quiénes serán las víctimas que caerán en los ataques por correo electrónico, pero están conscientes de que entre más correos masivos envíen, más personas eventualmente caerán en sus ataques. Tal vez, los delincuentes literalmente monitoreen cada equipo en Internet (una vez más, a través de equipos comprometidos para monitorear), en busca de cualquier dispositivo que pueda ser hackeado. Recuerda, no eres elegido porque seas especial. Más bien, los delincuentes tienen como objetivo a todas las personas posibles, también tú.

Tal vez no te des cuenta, pero tus dispositivos y tu información tienen un gran valor para los criminales cibernéticos alrededor del mundo.

Protégete

Cuando los criminales cibernéticos intentan comprometer personas alrededor del mundo, regularmente utilizan métodos relativamente sencillos. Afortunadamente, siguiendo algunos simples pasos, puedes hacer mucho por protegerte . Algunos de los pasos recomendados a seguir son los siguientes:

- **Tú mismo**. Finalmente, tú eres el primero en la línea de defensa ante un ataque cibernético. Muchos ataques inician con un intento de engañarte, como abrir el archivo adjunto de un correo electrónico que se encuentra infectado o engañándote para dar tu contraseña a través del teléfono. El sentido común es la mejor defensa, si algo parece extraño, sospechoso o muy bueno para ser verdad, seguramente se trata de un ataque.

- **Actualización**. Asegúrate de que el equipo o los dispositivos móviles que usas se encuentren actualizados y cuenten con los últimos parches. Esto no sólo es importante para el sistema operativo, también para cualquier aplicación o complemento que utilices. Mantener siempre tu sistema y aplicaciones actualizadas ayuda a protegerte de los ataques más comunes.

- **Contraseñas**. Utiliza una contraseña fuerte y única para cada una de tus cuentas. De esta manera, si el sitio web que utilizas es hackeado y todas las contraseñas son comprometidas (incluida la tuya) tus otras cuentas están a salvo. También asegúrate de que todos tus dispositivos se encuentren protegidos por una contraseña, PIN o cualquier otro mecanismo de protección que sea fuerte y único. Para mantener seguras todas tus contraseñas te recomendamos utilizar un administrador de contraseñas.

- **Tarjetas de crédito**. Revisa tus estado de cuenta regularmente, te recomendamos hacerlo semanalmente (mensualmente no es suficiente). Tan pronto como veas una transacción no autorizada en tu tarjeta de crédito,

Sí, en realidad sí eres un objetivo

repórtalo inmediatamente al emisor de tu tarjeta. Si tu banco permite configurar alertas de correo electrónico o mensajes de texto para transacciones inusualmente grandes o extrañas, utilízalo para tener notificaciones de actividades sospechosas más rápidamente.

- **Tu red**. Asegura el acceso de la red inalámbrica de tu hogar con una contraseña de administrador fuerte y asegúrate que la requiera cuando alguien quiera acceder. También asegúrate de que conoces los dispositivos que se encuentran conectados a la red de tu hogar y que todos los dispositivos estén actualizados.

- **Redes sociales**. Cuanta más información publiques en línea, es más probable que puedas ponerte en riesgo. No sólo la información que publicas hace más fácil que seas un objetivo de los criminales cibernéticos para tratar de engañarte, esta información también puede identificarte como un objetivo más valioso.

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

OUCH! Administrador de Contraseñas:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Asegurando la red de tu hogar:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Ataques Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Poster: Tú eres un objetivo:	http://www.securingthehuman.org/resources/posters

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Erika Ródriguez e Israel Rubí