VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Julio de 2013

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- ¿Qué es spear phishing?
- Efectividad del spear phishing
- Medidas de protección

Spear phising

¿Qué es spear phishing?

Seguramente estás familiarizado con los ataques de phishing, esos correos electrónicos diseñados para engañar y estafar a millones de víctimas potenciales alrededor del mundo. Por lo general, estos mensajes parecen venir de una fuente confiable, como puede ser un banco o alguna persona que conozcas. Los correos electrónicos a menudo tienen un mensaje urgente o una oferta demasiado buena para dejarse pasar. Si haces clic en la liga de un correo electrónico phishing, corres el riesgo de ser llevado a un sitio web malicioso que obtenga acceso a tu computadora o que busque almacenar tu usuario y contraseña. También es posible que el correo electrónico phishing tenga un archivo adjunto infectado, el cual, si lo abres, intentará infectar o tomar el control de tu computadora. Los cibercriminales envían estos mensajes de correo electrónico a la mayor cantidad de gente posible, sabiendo que, entre más personas reciban el correo electrónico, más víctimas pueden caer.

Editor Invitado

Lenny Zeltser es el invitado para esta edición. Lenny se enfoca en salvaguardar las operaciones de TI de los clientes de NCR Corp y enseña a combatir el software malicioso en el SANS Institute. Encuentra a Lenny en Twitter como **@lennyzeltser** o en su blog de seguridad como **blog.zeltser.com**.

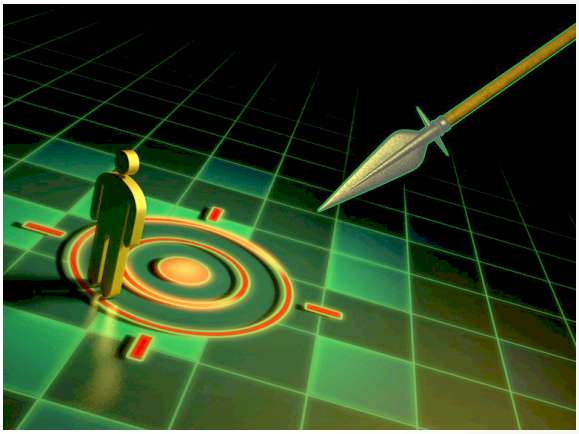
Aunque el phishing sigue siendo efectivo, se ha desarrollado un tipo de ataque relativamente nuevo llamado spear phishing. El concepto es el mismo, los ciberatacantes envían correos electrónicos a sus posibles víctimas, haciéndose pasar por una organización o una persona de confianza. Sin embargo, a diferencia de los correos electrónicos phishing tradicionales, los mensajes de spear phishing son muy específicos. En lugar de que se envíe un correo electrónico a millones de víctimas potenciales, los ciberatacantes envían un correo electrónico a unos cuantos individuos previamente seleccionados, tal vez cinco o diez personas específicas. A diferencia del phishing tradicional, con el spear phishing, los ciberatacantes se ven obligados a investigar a sus objetivos, revisando sus cuentas de Facebook o LinkedIn o leyendo los mensajes que publican en foros o blogs públicos. Con base en este rastreo de datos, los atacantes crean un correo electrónico altamente personalizado, el cual pretende causar un impacto real en los posibles blancos. De esta manera, las personas son mucho más propensas a caer en los ataques.

Efectividad del spear phishing

El spear phishing se utiliza cuando el ciberdelincuente quiere atacar a una persona o a una organización en particular. En lugar de simplemente robar dinero, los atacantes que utilizan spear phishing tienen objetivos muy particulares, por lo general, obtener acceso a información altamente confidencial, como secretos comerciales

Spear phising

corporativos, planes estratégicos de tecnología o comunicaciones confidenciales del gobierno. Tal vez, tu organización es un simple trampolín para obtener acceso a otra organización. Por lo mucho que ambicionan ganar, estos atacantes están dispuestos a invertir todo el tiempo y el esfuerzo necesario en investigar a sus objetivos.



La mejor forma de protegerte contra el spear phishing es tener en cuenta que podrías ser el blanco. Limita la información que publicas sobre ti y reporta correos electrónicos sospechosos.

Por ejemplo, supongamos que un gobierno extranjero decide que tu organización desarrolla un producto o tecnología que es clave para su éxito económico. En ese momento, te conviertes en el blanco. Los atacantes investigan el sitio web de tu organización e identifican tres individuos clave. Posteriormente, investigan las páginas de Facebook, Twitter y LinkedIn de estos tres individuos para crear un expediente completo de ellos. Después de analizar a estos individuos, los atacantes crean un correo electrónico spear phishing pretendiendo ser un proveedor de tu organización. El correo electrónico tiene un archivo adjunto que pretende ser una factura por ejemplo, cuando en realidad es un documento infectado. Dos de las tres personas seleccionadas son engañadas por el correo electrónico spear phishing y abren el archivo adjunto infectado, dando acceso total a gobiernos extranjeros en sus equipos y, en última instancia, a todos los secretos de los productos de su empresa, que ahora van a producir ellos mismos.

El spear phishing es una amenaza mucho más peligrosa que los simples ataques de phishing, ya que los ciberdelincuentes elaboran un ataque muy específico para una organización o una persona. Esto no solo aumenta las posibilidades de éxito de los atacantes, sino que son más difíciles de detectar.

Medidas de protección

El primer paso para protegerse contra estos ataques dirigidos es comprender que tú puedes ser un objetivo. Después de todo, tú y tu organización probablemente posean información sensible que otra persona pudiera desear o que pudiera ser usada para acceder a otra organización. Una vez que comprendas que puedes ser el blanco, toma las siguientes precauciones para protegerte a ti mismo y a tu compañía:

- Limita la información que publicas sobre ti en foros públicos, en Facebook, LinkedIn, o en sitios similares en sitios similares. Entre más detalles personales compartas, más fácil es para los ciberatacantes elaborar un correo electrónico de spear phishing que parezca un correo relevante y genuino.

Spear phising

- Si un correo electrónico te pide que abras un archivo adjunto, que hagas clic en un vínculo que parezca sospechoso o te solicita información sensible, verifica el mensaje. Si el correo electrónico parece provenir de una empresa o de una persona que conozcas, usa los datos de contacto que aparecen para comunicarte con el remitente y comprobar que él te envió el mensaje.

- Mantén los esfuerzos de seguridad de tu empresa siguiendo las políticas de seguridad apropiadas y haciendo uso de herramientas de seguridad como antivirus, cifrado y actualizaciones que estén disponibles para ti.

- Recuerda que la tecnología no puede filtrar y detener todos los ataques de correo electrónico, especialmente los correos electrónicos de spear phising. Si un correo electrónico parece un poco extraño al principio, léelo con cuidado. Si te preocupa que puedas haber recibido un correo electrónico de spear phishing o incluso si has sido víctima de ataque de se puede omitir spear phishing, contacta al servicio de asistencia técnica o al equipo de seguridad informática de tu empresa de inmediato.

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

Cómo evitar ataques de spear phishing: http://mx.norton.com/spear-phishing-scam-not-sport/article

Evitar la ingeniería social: http://revista.seguridad.unam.mx/numero-03/ingenierí-social-técnica-de-ataque-eficaz-en-contra-de-la-seguridad-informática

Evitar los ataques de phishing: http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=166

Phising: http://www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

Términos comunes de seguridad: http://www.securingthehuman.org/resources/security-terms

Tip del día de seguridad del SANS: https://www.sans.org/tip_of_the_day.php

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Paulo Contreras, Jonathan Banfi, Nora Cozaya, Célica Martínez