VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Enero 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- ¿Qué es la ingeniería social?
- Cómo detectar y detener los ataques de ingeniería social

Ingeniería social

Resumen

La mayoría de las personas tienen la idea errónea de que los ciberatacantes utilizan herramientas altamente avanzadas y técnicas para comprometer las computadoras o cuentas de los usuarios. Esto no es cierto. Los atacantes han aprendido que a menudo la forma más fácil de robar tu información es comprometer tus cuentas o infectar los sistemas engañándote para que cometas un error. En este boletín aprenderás cómo estos ataques, conocidos como ingeniería social, funcionan y lo que puedes hacer para protegerte.

Editor Invitado

James Lyne (**@jameslyne**) es un instructor certificado de SANS y líder global de investigación en Sophos. Usa ingeniería inversa y desmantela las últimas y más grandes creaciones de los cibercriminales. Es autor de las clases de Metasploit (SEC580) e Ingeniería Social (SEC567) en SANS.

¿Qué es la ingeniería social?

La ingeniería social es un ataque psicológico a través del cual el delincuente te engaña para realizar algo que no deberías hacer. El concepto no es nuevo, ha existido por cientos de años; piensa en los estafadores o los artistas del engaño, es la misma idea. Lo que hace a la tecnología actual más efectiva para realizar ciberataques es que físicamente no los puedes ver, los atacantes pueden pretender ser cualquier cosa o persona y dirigirse a millones de personas alrededor del mundo, incluyéndote. Además, los ataques de ingeniería social pueden evadir muchas tecnologías de seguridad. La forma más fácil de entender cómo funcionan estos ataques y cómo protegerte de ellos es dar un vistazo a los dos siguientes ejemplos.

Recibes una llamada telefónica de alguien que afirma ser una empresa de soporte informático, el proveedor de servicios de Internet (ISP) o tal vez el soporte técnico de Microsoft. La persona que llama explica que tu computadora está explorando activamente Internet, por lo cual creen que está infectada y fueron asignados para ayudarte con tu equipo. A continuación utilizan términos técnicos y te llevan a través de pasos confusos para convencerte que tu computadora está infectada. Por ejemplo, podrían pedirte que revises ciertos archivos en tu equipo y te explican cómo encontrarlos. Al localizar estos archivos, la persona que llama asegura que estos demuestran que la computadora está infectada, cuando en realidad son archivos de sistema comunes que se encuentran en casi todas las computadoras del mundo. Una vez que te han engañado, te presionan para que compres un software de seguridad que en realidad es un programa malicioso. Si lo compras y lo instalas no solo te habrán engañado para que infectes el equipo, sino que les pagaste para que lo hicieran.

Ingeniería social

Si les das acceso remoto a tu computadora, van a tomar control de ella y robar tu información o usarla en sus pujas.

Otro ejemplo es el ataque por correo electrónico conocido como la estafa del CEO, que ocurre frecuentemente en el trabajo. Un ciberatacante investiga tu organización en línea e identifica el nombre de tu jefe o compañero de trabajo. El atacante redacta un correo pretendiendo ser la persona que eligió y te lo envía. El correo te pide con urgencia que realices una acción, como realizar una transferencia o enviar información sensible sobre un empleado. Muy a menudo estos correos pretenden que hay una emergencia que requiere que omitas los procedimientos de seguridad estándar, por ejemplo, te pueden pedir que envíes información altamente sensible a una cuenta @gmail.com personal. Lo que hace que los ataques dirigidos como este sean peligrosos es que los atacantes investigan de antemano a su víctima. Además, las tecnologías de seguridad como los antivirus y los firewall no pueden detectar o detener estos ataques porque no hay un malware o vínculo malicioso involucrado.

El sentido común es tu defensa más poderosa para identificar y detener la mayoría de los ataques de ingeniería social.

Ten en cuenta que los ataques de ingeniería social no se limitan a llamadas telefónicas o correos electrónicos; estos pueden presentarse en cualquier forma, a través de mensajes de texto a tu teléfono, en tus redes sociales o incluso en persona. La clave es saber qué proteger, tú eres tu mejor defensa.

Cómo detectar y detener ataques de ingeniería social

Afortunadamente detener este tipo de ataques es más sencillo de lo que podrías imaginar, el sentido común es tu mejor defensa. Si ves algo sospechoso o no te sientes bien haciéndolo, puede ser un ataque. Las pistas más comunes son:

- Alguien crea un tremendo sentido de urgencia, tratando de engañarte para que cometas un error.
- Alguien te pregunta por información a la cual no deberían tener acceso o que ya debería saber, como los números de tus cuentas.
- Alguien te solicita tu contraseña, ninguna organización legítima te pediría eso.
- Alguien te presiona para que evadas o ignores los procedimientos de seguridad o procedimientos que se espera sigas en tu trabajo.

Ingeniería social

- Algo es demasiado bueno para ser cierto. Por ejemplo, te notifican que has ganado la lotería o un iPad sin siquiera haber concursado.
- Recibes un correo extraño de un amigo o colaborador de trabajo que contiene palabras que no utilizan comúnmente. Un ciberatacante puede haber entrado a sus cuentas y trata de engañarte. Para protegerte, debes verificar contactando a tu amigo por otros medios de comunicación, ya sea en persona o por teléfono.

Si sospechas que alguien intenta engañarte, no te comuniques más con esa persona. Si el ataque está relacionado con el trabajo, asegúrate de informar inmediatamente de la situación a la mesa de ayuda o el equipo de seguridad informática. Recuerda, el sentido común es a menudo tu mejor defensa.

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: securingthehuman.sans.org/ouch/archives

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

Ingeniería social: http://revista.seguridad.unam.mx/numero-03/ingenieria-social-tecnica-de-ataque

Evitando ataques de ingeniería social: http://www.seguridad.unam.mx/descarga.dsc?arch=191

Ingeniería social y privacidad en redes sociales:
https://revista.seguridad.unam.mx/numero-12/redes-sociales-ingenieria-social-riesgos-privacidad

Phishing: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_sp.pdf

Estafa del CEO: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201607_sp.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Katia Rodríguez y Célica Martínez

