VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Junio de 2013

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Entendiendo a las direcciones URL
- Acortadores de direcciones URL
- Códigos QR

Acortadores de URL y códigos QR

Antecedentes

Un Localizador de Recursos Uniforme (del inglés Uniform Resource Locator o URL) no es más que un término elegante para referirse a las direcciones web, tal como http://www.cert.org.mx. Una dirección URL es el nombre que escribes cuando visitas un sitio web o una página web.

Editor Invitado

El Dr. Eric Cole es un experto reconocido en la industria de la seguridad. Es el autor de varios libros, incluyendo Advanced Persistent Threat (Amenazas Avanzadas Persistenetes), Hackers Beware (Lo que ocupa a los hackers) y Network Security Bible (Biblia de seguridad en redes). El Dr. Cole también es el fundador de Secure Anchor Consulting, consultoría líder en servicios de seguridad de la información para empresas privadas y públicas, además, ejerce como profesor miembro y autor de cursos en la Facultad de SANS. Puedes consultar más información sobre él en **http://www.sans.org/instructors/dr-eric-cole**.

Cuando escribes una dirección URL en tu navegador web, éste toma el nombre y lo resuelve o traduce en una dirección IP, la dirección IP es donde está localizado el sitio web en Internet. Tu navegador, entonces, se conecta al sitio web y descarga la página, en ese momento tú ya la puedes ver. El problema es que los cibercriminales pueden jugarte una variedad de trampas con las direcciones URL, haciéndote pensar que estás visitando un sitio legítimo cuando realmente estás visitando un sitio web diferente, uno controlado por ellos, que muy probablemente, esté diseñado para robar tu información o hacer un ataque a tu navegador e infectar tu computadora.

Hay una gran diferencia entre a dónde piensas que te diriges y a dónde realmente te diriges. Repasemos cómo funciona una dirección URL, cómo suceden varios ataques comunes a las direcciones URL y de qué forma puedes protegerte de ellos.

Entendiendo las direcciones URL

Una dirección URL no es más que un destino compuesto de tres partes. La primera parte es el protocolo, cómo tú estás conectado al sitio web. Normalmente es HTTP (información enviada en claro o legible) o HTTPS (utiliza una conexión cifrada para que la información sea ilegible). La segunda parte es el dominio, que es el sitio web al que te diriges. La tercera parte es la página de destino, la página que visitarás en el sitio web. Revisemos un ejemplo de una dirección URL:

https://www.securingthehuman.org/ouch

Esta dirección URL comienza con HTTPS, la cual indica una conexión cifrada. La segunda parte www.securingthehuman.org es el sitio web que puedes visitar si das clic en la liga. Finalmente, la tercera parte es

Acortadores de URL y códigos QR

la '/', cualquier cosa que siga después de la diagonal indica qué parte del sitio vas a visitar. En este ejemplo, irás al sitio web del Instituto SANS, directamente a la página del boletín OUCH! La parte más importante a examinar es la segunda parte, el dominio. ¿Es realmente el sitio web que intentas visitar? Veamos cómo podrían los atacantes jugarte un truco y enviarte a los sitios web controlados por ellos mismos.

Para mantenerte seguro, antes de dar clic, primero hay que verificar el destino real de los códigos QR y de las direcciones URL.

Acortador de direcciones URL

Probablemente habrás visto un acortador de direcciones URL, no es más que un servicio que toma una dirección URL larga y compleja y la compacta en una dirección URL corta y sencilla. Con este tipo de servicios es más fácil compartir una dirección URL en medios de comunicación tradicionales, como el correo electrónico. También se utiliza cuando nos vemos limitados en la cantidad de caracteres que podemos publicar, como en Twitter o en mensajes SMS. Algunos sitios que ofrecen este tipo de servicio son: tinyurl.com, goo.gl y bit.ly. El riesgo que presenta utilizar un servicio acortador de direcciones URL es que no se puede conocer el verdadero destino. Por lo tanto, los atacantes pueden publicar URL acortadas, que en última instancia redirigen a sitios web que son controlados por ellos.

Una manera de protegerse contra este tipo de amenazas es verificar a dónde redirige la liga acortada antes de dar clic en ella. Muchos sitios web ofrecen el servicio para identificar el destino de un enlace acortado (para más ejemplos ver la sección Recursos). Además, algunos acortadores de direcciones URL brindan la opción de ver antes el destino. Por ejemplo, para una dirección URL acortada desde el servicio bit.ly, solo se necesita agregar al final el símbolo "+" para conocer el verdadero destino de la dirección URL, por ejemplo:

http://bit.ly/19HtqVH+

Códigos QR

Un código QR es similar al concepto de acortadores de direcciones URL, pero está diseñado para ser usado por smartphones. Su funcionamiento es sencillo, convierte una dirección URL en una imagen digital, esto se logra utilizando una aplicación dentro del dispositivo móvil, se toma la foto del código QR y se abre un navegador web dentro del dispositivo para redirigir a la dirección URL almacenada en el código QR. Se corre el mismo riesgo que con los acortadores de direcciones URL, ya que se está confiando ciegamente en el código QR sin conocer

Acortadores de URL y códigos QR

el verdadero destino. Por ejemplo, supongamos que te encuentras en una estación de tren o en una terminal de aeropuerto y ves un cartel promocionando una nueva película. Si utilizas un smartphone para leer el código QR, el cartel promete mostrar los avances de la nueva película. Si bien, es muy probable que el cartel sea legítimo, también puede ser que algún criminal haya caminado hasta el cartel y pegado un código QR malicioso sobre el código QR legítimo. De esta manera, cualquier dispositivo que intente leer la imagen QR no será redirigida al trailer de la película sino a un sitio web controlado por el atacante.

Al igual que con el acortador de direcciones URL, lo primero que debes hacer para protegerte es verificar el destino del código QR. Hay que asegurarse de que la aplicación utilizada para leer los códigos QR tenga la capacidad de, primero mostrar el destino al cual redirige y, después, dar la opción de decidir si se quiere acceder al sitio web o no. Si la aplicación para la lectura de códigos QR no tiene habilitada esta característica, lo recomendable es conseguir una nueva aplicación, hay muchas opciones disponibles de forma gratuita.

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 en Cómputo en México reconocido ante FIRST, es una referencia en seguridad de la información en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Recursos

Más sobre códigos QR:	http://es.wikipedia.org/wiki/C%C3%B3digo_QR
Previsualizadores de ligas acortadas:	http://unfurlr.com/ http://urlxray.com/
10 acortadores de URL:	http://preview.tinyurl.com/89sjx2c
Términos comunes de seguridad:	http://preview.tinyurl.com/6wkpae5
Tip del día de seguridad del SANS:	http://preview.tinyurl.com/6s2wrkp

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