This Google Chrome and Firefox Phishing Scam Is 'Practically Impossible to Spot'

Ricardo Briones Cortés

March 14, 2018

1 Resumen

Los expertos en seguridad informatica advierten a las personas sobre una estafa muy engañosa que va en aumento y engañara incluso a los usuarios más atentos.

El ataque es una variedad de phishing, que consiste en engañar a las personas para que confíen en una pag web falsa para llevarlos a un link para robar informacion o para descargar un archivo que contiene diferentes tipos de virus.

Este ataque utiliza nombres de dominio llamadas direcciones web, que se ven casi idénticos a los reales. Este ataque es mejor que la versión habitual donde los estafadores engañan a las personas para que visiten una imitación de "gmail.com" como "gmail.co", "gmial.com", "gmai1.com", etc.

Esta estafa es mucho más sutil pues los estafadores pueden registrar dominios con caracteres extraídos de varios alfabetos que no sean el alfabeto latino. Cuando se muestra, es prácticamente imposible diferenciar una "O" griega de una "O" cirílica de una "O" latina.

Este ataque ya es algo viejo y se llama "ataque homógrafo de IDN". Uno de los primeros descubrimientos de estos ataques lo descubiro Bruce Schneier, un experto en ciberseguridad que trabaja en IBM, al darse cuenta de una pag falsa llamada "PayPaI" en lugar de "PayPal" cambiando la "l" por la "i".

Gracias a este ataque, Xudong Zheng creo una pagina para demostrar lo facil que era crearla y demostrar el potencial del ataque.

El dominio falso de Zheng es en realidad "xn–80ak6aa92e.com". Este gobbledygook alfanumérico se traduce como "apple.com" en el navegador web debido a una herramienta llamada "punycode", que traduce caracteres de Unicode.

Los navegadores usan punycode para mostrar nombres de dominio extranjeros en inglés. Entonces "xn–80ak6aa92e.com", que hace referencia a las letras cirílicas (en Unicode), se convierte en "apple.com" en ASCII.

Los navegadores web mas vulnerables son Google Chrome, Mozilla Firefox y Opera. Los navegadores Safari e Internet Explorer no se ven afectados.

En muchos casos, la única forma de detectar el engaño es verificar el certificado SSL de un sitio, un archivo digital que verifica criptográficamente la identidad de un sitio.

Al hacerlo, en el sitio de prueba de concepto de ataque de Zheng se recupera un certificado que debería verse: "xn—80ak6aa92e.com".

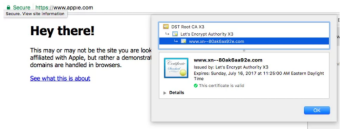

Figure 1: Imagen de como se muesta el certificado SSL de la pag web

Figure 2: Imagen de dos paginas distintas con aparentemente la misma direccion web

2 Ataque Homográfico

El ataque homográfico es la suplantación de caracteres alfanumericos por medio de Unicode en las direcciones de dominio de las paginas web, haciendo asi irreconocible para el usuario comun, los cambios de letras en el URL y redireccionando al usuario a una pagina falsa para robar sus datos personales.

3 Investigar y escribir las definiciones de los siguientes conceptos:

3.1 Phishing

Es un tipo de ataque que mediante el envió de correos electrónicos y páginas web falsas, trata de obtener números de cuenta y claves confidenciales para realizar operaciones fraudulentas, perjudicando de sobremanera a los legítimos dueños de la información.

3.2 Punycode

es una forma de representar Nombres de Dominio Internacionalizados (IDNs) con el conjunto limitado de caracteres (A-Z, 0-9) admitido por el sistema de nombres de dominio.

3.3 Certificado SSL

Un certificado SSL sirve para brindar seguridad al visitante de su página web, una manera de decirles a sus clientes que el sitio es auténtico, real y confiable para ingresar datos personales. Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que sus datos viajen de manera íntegra y segura

4 Referencias

Lance James, Phishing Exposed, Primera Edición, Syngress Publishing, Inc., USA 2005
https://www.dynadot.com/es/comunidad/ayuda/pregunta.html?aid=69
https://www.certsuperior.com/QueesunCertificadoSSL.aspx