Contenido

Introducción

Este documento describe el uso de los caracteres del homoglyph en los ataques avanzados del phishing y cómo ser consciente de éstos al usar el mensaje y los filtros del contenido en Cisco envían por correo electrónico el dispositivo de seguridad (ESA).

Homoglyph avanzó los ataques del phishing

En los ataques avanzados del phishing hoy, los correos electrónicos del phishing pueden contener los caracteres del homogyph. Un homoglyph es un carácter del texto con las dimensiones de una variable que están cerca de idéntico o de similar el uno al otro. Puede haber

Un ejemplo de escenario puede ser como sigue: ¿ www.p? ypal.com. Para

El cliente recibió el ejemplo de contener del correo electrónico: ¿www.p? ypal.com

El filtro contento como configurado contiene: www.paypal.com

Si usted hecha una ojeada el URL real vía el DNS usted notará que resuelven diferentemente:

¿El primer URL utiliza un homoglyph de la carta? ¿a? del formato del unicode.

¿Si usted mira de cerca, usted puede ver que el primer? ¿a? ¿en PayPal es realmente diferente que el segundo? a?.

Sea por favor consciente al trabajar con los filtros del mensaje y del contenido para bloquear los URL. El ESA no puede decir la diferencia entre los homoglyphs y los caracteres estándar del alfabeto. Una manera de detectar y de prevenir correctamente el uso de los ataques homoglyphic del phishing debe configurar y permiso DE y Filtrado de URL.

Irongeek proporciona un método para probar los homoglyphs y crear la prueba URL malévolo: Generador del ataque de Homoglyph

Introducción detallada en los ataques del phishing del homoglyph, también de Irongeek: Fuera del carácter: Uso de los ataques de Punycode y de Homoglyph de ofuscar los URL para el phishing