# Homoglyph avanzó los ataques del phishing

## 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 URL integrados en los correos electrónicos phising que no serán bloqueados por los filtros del mensaje o del contenido configurados en el ESA.

Un ejemplo de escenario puede ser como sigue: El cliente quiere bloquear un correo electrónico que tenía contenga el URL de www.pαypal.com. Para hacer así pues, se escribe un filtro contento entrante que buscando el URL que contiene www.paypal.com. La acción de este filtro contento sería configurada para caer y para notificar.

El cliente recibió el ejemplo de contener del correo electrónico: www.pαypal.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:

```
$ dig www.pypal.com

; <<>> DiG 9.8.3-P1 <<>> www.pypal.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 37851
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.p\201\145ypal.com. IN A

;; AUTHORITY SECTION:
com. 900 IN SOA a.gtld-servers.net. nstld.verisign-grs.com. 1440725118 1800 900 604800 86400

;; Query time: 35 msec
;; SERVER: 64.102.6.247#53(64.102.6.247)
;; WHEN: Thu Aug 27 21:26:00 2015
;; MSG SIZE rcvd: 106 $ dig www.paypal.com
```

```
; <<>> DiG 9.8.3-P1 <<>> www.paypal.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51860
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 8, ADDITIONAL: 8

;; QUESTION SECTION:
;www.paypal.com. IN A

;; ANSWER SECTION:
www.paypal.com. 279 IN CNAME www.paypal.com.akadns.net.
www.paypal.com.akadns.net. 9 IN CNAME ppdirect.paypal.com.akadns.net.
ppdirect.paypal.com.akadns.net. 279 IN CNAME wlb.paypal.com.akadns.net.
wlb.paypal.com.akadns.net. 9 IN CNAME www.paypal.com.edgekey.net.
www.paypal.com.edgekey.net. 330 IN CNAME e6166.a.akamaiedge.net.
e6166.a.akamaiedge.net. 20 IN A 184.50.215.128

;; AUTHORITY SECTION:
a.akamaiedge.net. 878 IN NS n5a.akamaiedge.net.
a.akamaiedge.net. 878 IN NS n7a.akamaiedge.net.
a.akamaiedge.net. 878 IN NS n2a.akamaiedge.net.
a.akamaiedge.net. 878 IN NS n0a.akamaiedge.net.
a.akamaiedge.net. 878 IN NS n1a.akamaiedge.net.
a.akamaiedge.net. 878 IN NS n4a.akamaiedge.net.
a.akamaiedge.net. 878 IN NS n6a.akamaiedge.net.
a.akamaiedge.net. 878 IN NS n3a.akamaiedge.net.

;; ADDITIONAL SECTION:
n0a.akamaiedge.net. 383 IN A 184.27.45.145
n1a.akamaiedge.net. 3142 IN A 184.51.101.8
n2a.akamaiedge.net. 6697 IN A 88.221.81.194
n3a.akamaiedge.net. 31 IN A 88.221.81.193
n4a.akamaiedge.net. 168 IN A 72.37.164.223
n5a.akamaiedge.net. 968 IN A 184.51.101.70
n6a.akamaiedge.net. 1851 IN A 23.220.148.171
n7a.akamaiedge.net. 3323 IN A 184.51.101.73

;; Query time: 124 msec
;; SERVER: 64.102.6.247#53(64.102.6.247)
;; WHEN: Thu Aug 27 21:33:50 2015
;; MSG SIZE rcvd: 470
```

El primer URL utiliza un homoglyph de la carta “a” del formato del unicode.

Si usted mira de cerca, usted puede ver que la primera “a” en PayPal es realmente diferente que la segunda “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