Homoglyph avançou ataques do phishing

Índice

Introdução

Este documento descreve o uso de caráteres do homoglyph em ataques avançados do phishing e como estar ciente destes ao usar a mensagem e o índice filtra na ferramenta de segurança do email de Cisco (ESA).

Homoglyph avançou ataques do phishing

Em ataques avançados do phishing hoje, os email do phishing podem conter caráteres do homogyph. Um homoglyph é um caráter do texto com formas que estão perto de idêntico ou de similar entre si. Pode haver URL encaixadas nos email phising que não serão obstruídos pelos filtros da mensagem ou do índice configurados no ESA.

Um exemplo de cenário pode ser como segue: O cliente quer obstruir um email que tenha contenha a URL de www.pɑypal.com. A fim fazer assim, um filtro satisfeito de entrada é escrito que procurando a URL que contém www.paypal.com. A ação deste filtro satisfeito seria configurada para deixar cair e notificar.

O cliente recebeu o exemplo de uma contenção do email: www.pɑypal.com

O filtro satisfeito como configurado contém: www.paypal.com

Se você olha a URL real através do DNS você observará que resolvem 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
```

A primeira URL usa um homoglyph da letra “a” do formato do unicode.

Se você olha proximamente, você pode ver que o primeiro “a” em paypal é realmente diferente do que o segundo “a”.

Esteja por favor ciente ao trabalhar com os filtros da mensagem e do índice para obstruir URL. O ESA não pode dizer a diferença entre homoglyphs e caráteres padrão do alfabeto. Uma maneira de detectar e impedir corretamente o uso de ataques homoglyphic do phishing é configurar e permitir DE e Filtragem URL.

Irongeek fornece um método testando homoglyphs e criando o teste URL maliciosa: Gerador do ataque de Homoglyph

Introdução detalhada em ataques do phishing do homoglyph, também de Irongeek: Fora do caráter: Uso de ataques de Punycode e de Homoglyph confundir URL para o phishing