Homoglyph a avancé des attaques par phishing

Contenu

Introduction

Ce document décrit l'utilisation des caractères de homoglyph dans des attaques par phishing avancées et comment se rendre compte de ces derniers en utilisant le message et le contenu filtre sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Homoglyph a avancé des attaques par phishing

Dans des attaques par phishing avancées aujourd'hui, les emails de phishing peuvent contenir des caractères de homogyph. Un homoglyph est un caractère des textes avec les formes qui sont près d'identique ou de semblable entre eux. Il peut y avoir d'URLs encastré dans les emails phising qui ne seront pas bloqués par des filtres de message ou de contenu configurés sur l'ESA.

Un exemple de scénario peut être comme suit : Le client veut bloquer un email qui a eu contient l'URL de www.pαypal.com. Afin de faire ainsi, on écrit un filtre satisfait d'arrivée qui recherchant l'URL contenant www.paypal.com. L'action de ce filtre satisfait serait configurée pour chuter et annoncer.

Le client a reçu l'exemple de contenir d'email : www.pαypal.com

Le filtre satisfait en tant que configuré contient : www.paypal.com

Si vous prenez à un regarder l'URL d'effectif par l'intermédiaire des DN vous noterez qu'ils les résolvent différemment :

```
$ 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
```

Le premier URL utilise un homoglyph de la lettre « a » du format d'unicode.

Si vous regardez étroitement, vous pouvez voir que le premier « a » dans paypal est réellement différent que le deuxième « a ».

Veuillez se rendre compte en fonctionnant avec des filtres de message et de contenu pour bloquer l'URLs. L'ESA ne peut pas faire la différence entre les homoglyphs et les caractères standard d'alphabet. Une manière correctement de détecter et empêcher l'utilisation des attaques par phishing homoglyphic doit configurer et enable DE et Filtrage URL.

Irongeek fournit une méthode pour tester des homoglyphs et créer l'URL malveillant de test : Générateur d'attaque de Homoglyph

Introduction détaillée dans des attaques par phishing de homoglyph, aussi d'Irongeek : Hors du caractère : Utilisation des attaques de Punycode et de Homoglyph d'assombrir l'URLs pour le phishing