Attacchi di phishing avanzati omoglifi

Sommario

Introduzione

Questo documento descrive l'uso di caratteri omoglitici in attacchi di phishing avanzati e come esserne consapevoli quando si usano i filtri messaggi e contenuti su Cisco Email Security Appliance (ESA).

Attacchi di phishing avanzati omoglifi

Negli attacchi di phishing avanzati di oggi, le e-mail di phishing possono contenere caratteri omogotici. Un omoglifo è un carattere di testo con forme simili o identiche. Potrebbero esserci URL incorporati in e-mail phishing che non verranno bloccati dai filtri messaggi o contenuti configurati sull'ESA.

Uno scenario di esempio può essere il seguente: Il cliente desidera bloccare un'e-mail che contiene l'URL di www.pɑypal.com. A tale scopo, viene scritto un filtro dei contenuti in arrivo che cercherà l'URL contenente www.paypal.com. L'azione di questo filtro contenuti verrà configurata per l'eliminazione e la notifica.

Il cliente ha ricevuto un esempio di e-mail contenente: www.pɑypal.com

Il filtro contenuti configurato contiene: www.paypal.com

Se si guarda l'URL reale tramite DNS, si noterà che si risolvono in modo diverso:

```
$ 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
```

Il primo URL utilizza un omoglifo della lettera "a" del formato unicode.

Se guardate attentamente, potete vedere che la prima "a" in paypal è in realtà diversa dalla seconda "a".

Quando si utilizzano filtri messaggi e contenuti per bloccare gli URL, occorre tenerli in considerazione. L'ESA non riesce a distinguere tra omoglifi e caratteri alfabetici standard. Un modo per rilevare e prevenire correttamente l'uso di attacchi di phishing omoglifi è configurare e abilitare il filtro URL e di.

Irongeek fornisce un metodo per verificare gli omoglifi e creare URL dannosi per i test: Generatore di attacchi omoglifo

Introduzione dettagliata agli attacchi di phishing omoglifi, sempre da Irongeek: Fuori carattere: Utilizzo di attacchi Punycode e Homoglyph per offuscare gli URL per il phishing