Geavanceerde phishing-aanvallen

Inhoud

Inleiding

Dit document beschrijft het gebruik van homo-achtige tekens in geavanceerde phishing-aanvallen en hoe u deze bewust bent bij het gebruik van bericht- en contentfilters op Cisco Email Security Appliance (ESA).

Geavanceerde phishing-aanvallen

Vandaag de dag kunnen phishing e-mails homogyph tekens bevatten. Een homo-achtige tekst is een tekstteken met vormen die vrijwel identiek of soortgelijk zijn aan elkaar. Er kunnen URL's in phising-e-mails zijn ingebouwd die niet worden geblokkeerd door bericht- of inhoudfilters die in de ESA zijn ingesteld.

Een voorbeeldscenario kan als volgt zijn: De klant wil een e-mail blokkeren die de URL van www.pɑ ypal.com bevat. Om dit te doen, wordt een inkomende contentfilter geschreven dat naar de URL zal zoeken die www.paypal.com bevat. De actie van dit filter van de inhoud wordt zo ingesteld dat deze moet vallen en melden.

Door de klant ontvangen voorbeeld van een e-mail met: www.pɑypal.com

Content filter zoals ingesteld bevat: www.paypal.com

Als u de eigenlijke URL via DNS bekijkt, ziet u dat deze anders wordt opgelost:

```
$ 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
```

De eerste URL gebruikt een homoLyph van de letter "a" van het éénode formaat.

Als je goed kijkt, kun je zien dat de eerste "a" in paypal feitelijk anders is dan de tweede "a".

Houd hier rekening mee wanneer u met bericht- en contentfilters werkt om URL's te blokkeren. Het ESA kan het verschil niet zien tussen homoglypen en standaard alfabet tekens. Eén manier om homo-phishing aanvallen correct te detecteren en te voorkomen is om ATM en URL Filtering te configureren en in te schakelen.

Irongeek biedt een methode om homo's te testen en testkwaadwillige URL(s) te maken: [Homoglyph Attack Generator]

Gedetailleerde introductie van phishing phishing aanvallen vanaf homoglyph, ook vanuit Irongeek: [Out of Character: Gebruik van Punycode en Homoglyphaanvallen om URLs voor phishing te verduisteren]