Homoglyph Advanced Phishing-Angriffe

Inhalt

Einführung

Dieses Dokument beschreibt die Verwendung von Homoglyph-Zeichen bei komplexen Phishing-Angriffen und wie diese bei der Verwendung von Nachrichten- und Content-Filtern auf der Cisco E-Mail Security Appliance (ESA) beachtet werden.

Homoglyph Advanced Phishing-Angriffe

Bei hoch entwickelten Phishing-Angriffen enthalten Phishing-E-Mails möglicherweise Homogyph-Zeichen. Ein Homoglyph ist ein Textzeichen mit Formen, die einander nahezu identisch oder ähnlich sind. Möglicherweise sind in Phising-E-Mails eingebettete URLs vorhanden, die nicht durch auf der ESA konfigurierte Nachrichten- oder Content-Filter blockiert werden.

Ein Beispielszenario kann wie folgt aussehen: Der Kunde möchte eine E-Mail blockieren, die die URL www.pɑ ypal.com enthält. Dazu wird ein Content-Filter für eingehende Anrufe geschrieben, der nach der URL mit www.paypal.com sucht. Die Aktion dieses Content-Filters wird so konfiguriert, dass sie verworfen und benachrichtigt wird.

Der Kunde hat ein Beispiel für eine E-Mail erhalten, die Folgendes enthält: www.pɑ ypal.com

Der Content-Filter in der konfigurierten Form enthält: www.paypal.com

Wenn Sie sich die tatsächliche URL über DNS anschauen, werden Sie bemerken, dass diese anders aufgelöst wird:

```
$ 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
```

Die erste URL verwendet eine Homoglyph des Buchstabens "a" des Unicode-Formats.

Wenn Sie genau hinschauen, können Sie sehen, dass das erste "a" in PayPal tatsächlich anders ist als das zweite "a".

Beachten Sie, dass Sie beim Arbeiten mit Nachrichten- und Content-Filtern URLs blockieren. Die ESA kann den Unterschied zwischen Homoglyphen und Standardalphabetentzeichen nicht erkennen. Eine Möglichkeit, homoglyphische Phishing-Angriffe richtig zu erkennen und zu verhindern, besteht in der Konfiguration und Aktivierung von OF und URL-Filterung.

Irongeek bietet eine Methode zum Testen von Homoglyphen und zum Erstellen von schädlichen URL(s) zum Testen: Homoglyph Attack Generator

Detaillierte Einführung in Homoglyph-Phishing-Angriffe auch von Irongeek: Out of Character: Verwendung von Punycode und Homoglyph-Angriffen, um URLs für Phishing zu verschleiern