同形高級網路釣魚攻擊

目錄

簡介

本文檔介紹在高級網路釣魚攻擊中使用同形字元，以及在思科郵件安全裝置(ESA)上使用郵件和內容過濾器時如何識別這些同形字元。

同形高級網路釣魚攻擊

在當今的高級網路釣魚攻擊中，網路釣魚電子郵件可能包含同型字元。 同形字是形狀幾乎相同或相似的文本字元。 ESA上配置的郵件或內容過濾器不會阻止加密電子郵件中嵌入的URL。

示例場景可能如下所示：客戶想要阻止包含www.pypal.comURLα的電子郵件。 為此，會編寫入站內容過濾器，以查詢包含www.paypal.com的URL。 此內容過濾器的操作將被配置為丟棄並通知。

客戶收到的電子郵件示例包括： www.pαypal.com

配置的內容過濾器包含：www.paypal.com

如果您檢視透過DNS的實際的URL，會發現其解析方式不同：

```
$ 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
```

第一個URL使用unicode格式字母「a」的同形字。

如果你仔細看你會發現貝寶中的第一個a實際上不同於第二個a。

使用郵件和內容過濾器阻止URL時，請注意。 ESA無法區分同形文字和標準字母字元之間的差異。 正確檢測和防止使用同型網路釣魚攻擊的一種方法是配置並啟用OF和URL過濾。

Irongeek提供了一種測試同形字形和建立測試惡意URL的方法：同形攻擊生成器

同形網路釣魚攻擊的詳細介紹，也來自Irongeek:Out of Character:使用Punycode和同形碼攻擊對網路釣魚的URL進行模糊處理