Homoglyph提前网络钓鱼攻击

目录

简介

本文描述使用在先进的网络钓鱼攻击的homoglyph字符和如何知道这些，当使用消息时，并且在思科的内容过滤器给安全工具(ESA)发电子邮件。

Homoglyph提前网络钓鱼攻击

在先进的网络钓鱼攻击今天，网络钓鱼电子邮件可能包含homogyph字符。 homoglyph是与彼此在相同或类似附近的形状的一个文本字符。 可能有在不会由消息阻塞或内容过滤已配置的在ESA的phising的电子邮件嵌入的URL。

示例情形可能如下：客户要阻塞有包含www.paypal.com URL的电子邮件。 为了执行如此，寻找包含www.paypal.com的URL的一个入站内容过滤器写入。 此内容过滤器的操作将配置下降和通知。

电子邮件包含的客户已接收示例： www.paypal.com

内容过滤器作为已配置的包含：www.paypal.com

如果看一看在实际URL通过DNS您注意他们不同地解决：

```
$ 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
```

第一个URL使用字母“a”的homoglyph unicode格式。

如果仔细地看，您能看到第一个“a”在paypal跟第二个“a”实际上不同。

当工作用消息和内容过滤器阻塞URL时，请注意。 ESA不能说出homoglyphs和标准的字母表字符之间的差别。 一种方式适当地检测和防止使用homoglyphic网络钓鱼攻击配置和enable (event)和URL过滤。

Irongeek为测试homoglyphs和创建测验有恶意的URL提供一个方法：Homoglyph攻击生成器

详细的介绍到homoglyph网络钓鱼攻击里，也来自Irongeek ： 在字符外面：使用Punycode和Homoglyph攻击弄暗淡网络钓鱼的URL