Homoglyph усовершенствованные фишинговые атаки

Содержание

Введение

Этот документ описывает использование homoglyph символов в усовершенствованных фишинговых атаках и как знать о них при использовании сообщения и фильтров контента на Cisco Email Security Appliance (ESA).

Homoglyph усовершенствованные фишинговые атаки

В усовершенствованных фишинговых атаках сегодня, электронные почты фишинга могут содержать homogyph символы. homoglyph является текстовым символом с формами, которые почти идентичны или подобны друг другу. Могут быть URL, встроенные в электронные почты фишинга, которые не будут заблокированы сообщением или фильтрами контента, настроенными на ESA.

Пример сценария может быть следующие: Клиент хочет заблокировать электронную почту, которая имела, содержит URL www.pαypal.com. В заказе для этого входящий фильтр контента записан, который будет , ища URL, содержащий www.paypal.com. Действие этого фильтра контента было бы настроено, чтобы отбросить и уведомить.

Клиент получил пример почтового, содержащего: www.pαypal.com

Фильтр контента согласно конфигурации содержит: www.paypal.com

Если вы будете смотреть на фактический URL через DNS, то вы заметите, что они решают по-другому:

```
$ 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
```

Первый URL использует homoglyph буквы формата unicode.

Если вы смотрите близко, вы видите, что первое в PayPal является фактически другим, чем второй “a”.

Знайте при работе с сообщением и фильтрами контента для блокирования URL. ESA не может сказать различие между homoglyphs и стандартными символами алфавита. Один способ должным образом обнаружить и предотвратить использование homoglyphic фишинговых атак состоит в том, чтобы настроить и включить OF и Фильтрацию URL-адресов.

Irongeek предоставляет метод для тестирования homoglyphs и создания теста злонамеренный URL: [Генератор Атаки Homoglyph]

Подробное введение в homoglyph фишинговые атаки, также от Irongeek: [Из Символа:]

Использование Punycode и Homoglyph Attacks для Запутывания URL для Фишинга