Homoglyph 高度なフィッシング攻撃

目次

概要

この資料は高度 phishing 不正侵入でメッセージを使用するときこれらに気づく方法を homoglyph 文字の使用を記述したもので、コンテンツは Cisco E メール セキュリティ アプライアンス（ESA）でフィルタリングします。

Homoglyph 高度なフィッシング攻撃

今日高度 phishing 不正侵入では、電子メールを phishing は homogyph 文字が含まれているかもしれません。 homoglyph は同一か類似したの近くに互いにある図形のテキスト文字です。 ESA で設定されたメッセージまたはコンテンツ フィルターによってブロックされない phising 電子メールで組み込まれる URL があるかもしれません。

シナリオ例は次の通りであるかもしれません: 顧客は含まれている www.pαypal.com の URL が持っていた電子メールをブロックしたいと思います。 そうするために、受信コンテンツ フィルタは書かれ www.paypal.com が含まれている URL を探します。 このコンテンツ フィルタの操作は廃棄し、知らせるために設定されます。

顧客は電子メール含んでいる例を受け取りました: www.pαypal.com

設定されるとしてコンテンツ フィルタは含んでいます: www.paypal.com

DNS によって実際の URL の見てみればそれらが別様に解決することを注意します:

```
$ 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
```

最初の URL は unicode 形式の文字「a」の homoglyph を使用します。

よく見る場合、paypal の最初の「a」が実際に第 2 「a」と異なっていることがわかります。

URL をブロックするためにメッセージおよびコンテンツ フィルターを使用した場合わかっていてであって下さい。 ESA は homoglyphs と標準アルファベット文字の違いをわかります。 きちんと homoglyphic phishing 不正侵入の使用を検出する、防ぎ 1 つの方法は、イネーブルのおよび URLフィルタリング設定することです。

Irongeek は homoglyphs をテストし、テスト悪意のある URL を作成するために方式を提供します: Homoglyph 攻撃ジェネレーター

Irongeek からの homoglyph phishing 不正侵入への詳しい概要、また: 文字から: Phishing のための URL を混乱させる Punycode および Homoglyph 不正侵入の使用