호모글리프 고급 피싱 공격

목차

소개

이 문서에서는 지능형 피싱 공격에서 호모글리프 문자를 사용하는 방법과 Cisco ESA(Email Security Appliance)에서 메시지 및 콘텐츠 필터를 사용할 때 이를 인식하는 방법에 대해 설명합니다.

호모글리프 고급 피싱 공격

오늘날의 지능형 피싱 공격에서는 피싱 이메일에 호모형 문자가 포함될 수 있습니다. 상형 문자는 모양이 서로 같거나 비슷한 텍스트 문자입니다. 피싱 이메일에 포함된 URL이 있을 수 있으며, 이는 ESA에 구성된 메시지 또는 콘텐츠 필터에 의해 차단되지 않습니다.

예제 시나리오는 다음과 같습니다.고객이 www.pypal.com의 URL이 포함된 전자 메일을 차단하려고 합니다. 이를 위해 www.paypal.com이 포함된 URL을 찾는 인바운드 콘텐츠 필터가 작성됩니다. 이 콘텐츠 필터의 작업은 삭제 및 알림으로 구성됩니다.

고객이 다음을 포함하는 이메일의 예를 받았습니다. www.pɑypal.com

구성된 콘텐츠 필터에는 다음이 포함됩니다.www.paypal.com

DNS를 통해 실제 URL을 살펴보면 다음과 같이 다르게 확인됩니다.

```
$ 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
```

첫 번째 URL은 유니코드 형식의 문자 "a"의 홈 상형 문자를 사용합니다.

자세히 살펴보면, 페이팔의 첫 번째 "a"가 실제로 두 번째 "a"와 다르다는 것을 알 수 있습니다.

메시지 및 콘텐츠 필터로 URL을 차단할 때 유의하십시오. ESA는 홈 글리프 및 표준 알파벳 문자의 차이를 구별할 수 없습니다. 동성애 피싱 공격을 올바르게 탐지하고 방지하는 한 가지 방법은 OF 및 URL 필터링을 구성하고 활성화하는 것입니다.

Irongeek는 홈 글리프를 테스트하고 악성 URL을 테스트하는 방법을 제공합니다.[호모글리프 공격 생성기]

Irongeek에서도 제공하는 호모글리프 피싱 공격에 대한 자세한 소개: [Out of Character:피싱용 난독 URL에 Punycode 및 Homoglyph 공격 사용]