هجمات التصيد الاحتيالي المتقدم للحرف المتجانس

المحتويات

المقدمة

يصف هذا المستند إستخدام أحرف الحرف المتماثل في هجمات التصيد الاحتيالي المتقدمة وكيفية إدراك ذلك عند إستخدام عوامل تصفية الرسائل والمحتوى على جهاز أمان البريد الإلكتروني Cisco Email Security Appliance (ESA).

هجمات التصيد الاحتيالي المتقدم للحرف المتجانس

في هجمات التصيد الاحتيالي المتقدمة اليوم، قد تحتوي رسائل البريد الإلكتروني للتصيد الاحتيالي على أحرف مطابقة. الحرف المتماثل هو حرف نصي له أشكال قريبة من التطابق أو مشابهة لبعضها البعض. قد تكون هناك عناوين URL مضمنة في رسائل البريد الإلكتروني المستنسخة التي لن يتم حظرها بواسطة عوامل تصفية الرسائل أو المحتوى التي تم تكوينها على ESA.

قد يكون سيناريو المثال كما يلي: يريد العميل حظر بريد إلكتروني يحتوي على عنوان URL الخاص www.paypal.com. للقيام بذلك، تتم كتابة عامل تصفية محتوى وارد سيبحث عن عنوان URL الذي يحتوي على www.paypal.com. سيتم تكوين إجراء عامل تصفية المحتوى هذا للإفلات والإخطار.

تلقى العميل مثالا على رسالة بريد إلكتروني تحتوي على: www.paypal.com

يحتوي عامل تصفية المحتوى كما تم تكوينه على: www.paypal.com

إذا ألقيت نظرة على عنوان URL الحقيقي عبر DNS ستلاحظ أنه حل بشكل مختلف:

```
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 ;;
```

يستخدم عنوان URL الأول حرف "a" الخاص بتنسيق unicode.

إذا نظرت عن كثب، يمكنك أن ترى أن أول حرف "A" في باي بال هو في الواقع مختلف عن الثاني "A".

الرجاء أن تكون على دراية عند العمل باستخدام عوامل تصفية الرسائل والمحتوى لحظر عناوين URL. لا يمكن ل ESA تحديد الفرق بين الحروف الرسومية المتجانسة وحروف الأبجدية القياسية. تتمثل إحدى الطرق لاكتشاف هجمات التصيد الاحتيالي المتجانسة ومنع إستخدامها بشكل صحيح في تكوين تصفية URL و OF وتمكينها.

يوفر IronGeek طريقة لاختبار الحروف الرسومية المتماثلة وإنشاء عنوان (عناوين) URL ضار للاختبار: مولد هجوم Homoglyph

مقدمة مفصلة حول هجمات التصيد الاحتيالي على الحرف المتماثل، كذلك من IronGeek: خارج الحروف: إستخدام هجمات Punycode و Homoglyph إلى عناوين URL الخاصة بالتصيد الاحتيالي غير المشفرة

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).