目录

简介
Homoglyph提前网络钓鱼攻击
相关的思科支持社区讨论

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

示例情形可能如下：客户要阻塞有包含

电子邮件包含的客户已接收示例： www.p ？ypal.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：

第一个URL使用字母的homoglyph ？a ？unicode格式。

如果仔细地看，能看到第一？a ？在paypal跟第二实际上不同？a ？。

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