Contents

Introduction

This document describes the use of homoglyph characters in advanced phishing attacks and how to be aware of these when using message and content filters on the Cisco Email Security Appliance (ESA).

Homoglyph Advanced Phishing Attacks

In advanced phishing attacks today, phishing emails may contain homogyph characters. homoglyph is a text character with shapes that are near identical or similar to each other. There may be

An example scenario may be as follows: Customer wants to block an email that had contains the URL of

Customer received example of an email containing: www.pypal.com

Content filter as configured contains: www.paypal.com

If you take a look at the actual URL via DNS you will notice they resolve differently:

The first URL uses a homoglyph of the letter “a” of the unicode format.

If you look closely, you can see that the first “a” in paypal is actually different than the second “a”.

Please be aware when working with message and content filters to block URLs. The ESA cannot tell the difference between homoglyphs and standard alphabet characters. One way to properly detect and prevent the use of homoglyphic phishing attacks is to configure and enable OF and URL Filtering.

Irongeek provides a method for testing homoglyphs and creating test malicious URL(s): Homoglyph Attack Generator

Detailed introduction into homoglyph phishing attacks, also from Irongeek: Out of Character: Use of Punycode and Homoglyph Attacks to Obfuscate URLs for Phishing