Advanced Notification of Punycode Phishing Attack

Security Advisory             AE-Advisory 17-22
Criticality                   Critical
Advisory Released On          18 April 2017
CVE Reference ID              -

Impact
Trick users into entering a phishing website

Affected Software
- Google Chrome
- Mozilla Firefox
- Opera

Solution
Refer to the “Solution” section below

Summary
As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a new critical Phishing attack that is almost impossible to detect on known web browsers such as: Google Chrome, Mozilla Firefox and Opera. The attack deceives users with phishing websites that appear as legitimate and known domains from looking at the URL by utilizing a known vulnerability in the web browsers mentioned above. Further information is explained in the Threat Details section below.
**Threat Details**

**Origin:**
The vulnerability within the web browsers that allow this Phishing attack to happen was discovered back in January 2017. The security researchers who found this vulnerability have reported it to the affected vendors however some of them have still not fixed the vulnerability and it is critical for all entities to be aware of this.

**Vulnerability Details:**
What is the best defense against a phishing attack? Usually it’s checking the address bar after the page has been loaded and if it is being served over a valid HTTPS connection, however, for this case it’s different. It is impossible to detect the vulnerability without carefully inspecting the site’s URL or SSL certificate. The researcher who was able to find this vulnerability managed to spoof (for proof-of-concept reasons) the website of “Apple” which is a known company for selling hardware and software. Refer to the screenshot below:

![Screenshot of Apple website with secure connection](image1)

However, the researcher has put up a message saying that this is a website for demonstration of a vulnerability as shown in the screenshot below:

![Message explaining the demonstration](image2)
Technical Details:

Homograph attacks have been known since 2001. It’s a spoofing attack where a website address and content look legitimate but it is really not because a character/s have been replaced with Unicode characters. Unicode characters represent alphabets like Greek, Cyrillic, and Armenian in internationalized domain names and the letters look the same to the normal eye but they are treated differently by computers as each character has a different value. For example, Cyrillic “а” (U+0430) and Latin “a” (U+0041) are both treated different by web browsers but are displayed as an “a” in the web browser address making it almost impossible for humans to know.

By default, many web browsers use “Punycode” encoding to represent Unicode characters in the URL to defend against Homograph attacks. Punycode is a special encoding used by web browsers to convert Unicode characters to ASCII (A-Z, 0-9) which is supported by the International Domain Names (IDNs) system. For example, a Chinese domain with Chinese characters such as “短.co” is represented in Punycode as “xn--s7y.co”. According to the researcher who found the vulnerability, web browsers render only Punycode URLs in one language as Unicode (for example only Chinese or Japanese) but they fail if a domain name contains characters from multiple languages.

This loophole allowed the researcher who discovered the vulnerability to be able to register a domain name “xn--80ak6aa92e.com” and bypass protection and make it appear as “apple.com” in all the vulnerable web browsers mentioned above. Fortunately, Internet Explorer, Microsoft Edge, Apple Safari, Brave and Vivaldi are not vulnerable.

The “xn--” prefix in the domain name mentioned above is known as an ASCII compatible encoding prefix, which shows the web browser that domain uses ‘Punycode’ encoding to represent Unicode characters, and because the researcher
used a Cyrillic “а” (U+430) rather than an ASCII “a” (U+0041), the defense approach implemented by the web browser failed.

Solution

- Google has already patched the vulnerability in its experimental Chrome Canary 59 and will come up with a permanent fix with the release of Chrome Stable 58 set to be launched later this month (April 2017)

- Users are recommended to disable Punycode support in their web browsers to temporarily mitigate this attack and identify phishing domains. Refer to your web browser vendor for guides on how to disable Punycode support.

- It is always recommended to manually type website URLs in the address bar for important/known websites like Google, Facebook, Twitter, Yahoo, banking websites and so on

Firefox users work-around:

For Mozilla Firework users, fortunately there is a way to disable Punycode support.

1. Type `about:config` in the address bar and press Enter on your keyboard

2. Type “Punycod” in the search bar

3. The list will be filtered so that it will show a parameter called: “network.IDN_show_punycod”. Double click or right-click and select Toggle to change the value from false to true.

4. Restart your browser and Punycode support should be disabled.
Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae