Maritime Security + Cyber Alert

Chrome and Firefox Phishing Attack Uses Domains Identical to Known Safe Sites

This entry was posted in General Security on April 14, 2017 by Mark Maunder 120 Replies

This is a Wordfence public service security announcement for all users of Chrome and Firefox web browsers:
There is a phishing attack that is receiving much attention today in the security community.

As a reminder: A phishing attack is when an attacker sends you an email that contains a link to a malicious website. You click on the link because it appears to be trusted. Merely visiting the website may infect your computer or you may be tricked into signing into the malicious site with credentials from a site you trust. The attacker then has access to your username, password and any other sensitive information they can trick you into providing.
This variant of a phishing attack uses unicode to register domains that look identical to real domains. These fake domains can be used in phishing attacks to fool users into signing into a fake website, thereby handing over their login credentials to an attacker.

This affects the current version of Chrome browser, which is version 57.0.2987 and the current version of Firefox, which is version 52.0.2. This does not affect Internet Explorer or Safari browsers.

The real epic.com is a healthcare website. Using our unicode domain, we could clone the real epic.com website, then start emailing people and try to get them to sign into our fake healthcare website which would hand over their login credentials to us. We may then have full access to their healthcare records or other sensitive data.

We even managed to get an SSL certificate for our demonstration attack domain from LetsEncrypt. Getting the SSL certificate took us 5 minutes and it was free. By doing this we received the word ‘Secure’ next to our domain in Chrome and the little green lock symbol in Firefox.

How is this possible?

The xn-- prefix is what is known as an ‘ASCII compatible encoding’ prefix. It lets the browser know that the domain uses ‘punycode’ encoding to represent Unicode characters. In non-techie speak, this means that if you have a domain name with Chinese or other international characters, you can register a domain name with normal A-Z characters that can allow a browser to represent that domain as international characters in the location bar.

What we have done above is used ‘e’ ‘p’ ‘i’ and ‘c’ unicode characters that look identical to the real characters but are different unicode characters. In the current version of Chrome, as long as all characters are unicode, it will show the domain in its internationalized form.

How to fix this in Firefox:

In your firefox location bar, type ‘about:config’ without quotes.

Do a search for ‘punycode’ without quotes.

You should see a parameter titled: **network.IDN_show_punycode**
Change the value from **false** to **true.**

Can I fix this if I use Chrome?

Currently we are not aware of a manual fix in Chrome for this. Chrome have already released a fix in their ‘Canary’ release, which is their test release. This should be released to the general public within the next few days.

Until then, if you are unsure if you are on a real site and are about to enter sensitive information, you can copy the URL in the location bar and paste it into Notepad or TextEdit on Mac. It should appear as the https://xn--….. version if it is a fake domain. Otherwise it will appear as the real domain in its unencoded form if it is the real thing.

Spread the word

The concept of an IDN homograph attack has been around since 2001 when Israeli researchers Evgeniy Gabrilovich and Alex Gontmakher first wrote about it.
Web browsers have attempted various fixes but the current implementations in Chrome and Firefox are clearly not doing a good enough job. To Chrome’s credit, they are about to fix that. Thankfully there is a manual fix for Firefox.

We would like to encourage you to spread the word. This new twist on phishing is getting a lot of attention today, Friday April 14th and is making the rounds currently in the security community. Xudong Zheng wrote about this earlier today and it is also being discussed on the netsec subreddit.
We think here is a high possibility that this may be exploited in phishing attacks before the Chrome fix is released to the general public, which is why we are posting this public service announcement.