You Think You Can’t Be Phished?

Originalartikel

Backup

<html> Well, think again. At least if you are using Chrome or Firefox. Don’t believe us? Well, check out Apple new website then, at https://www.apple.com . Notice anything? If you are not using an affected browser you are just seeing a strange URL after opening the webpage, otherwise it’s pretty legit. This is a page to demonstrate a type of Unicode vulnerability in how the browser interprets and show the URL to the user. Notice the valid HTTPS. Of course the domain is not from Apple, it is actually the domain: “https://www.xn--80ak6aa92e.com/“. If you open the page, you can see the actual URL by right-clicking and select view-source. So what’s going on? This type of phishing attack, known as IDN homograph attacks, relies on the fact that the browser, in this case Chrome or Firefox, interprets the “xn–” prefix in a URL as an ASCII compatible encoding prefix. It is called Punycode and it’s a way to represent Unicode using only the ASCII characters used in Internet host names. Imagine a sort of Base64 for domains. This allows for domains with international characters to be registered, for example, the domain “xn–s7y.co” is equivalent to “短.co”, as [Xudong Zheng] explains in his blog. Different alphabets have different glyphs that work in this kinds of attacks. Take the Cyrillic alphabet, it contains 11 lowercase glyphs that are identical or nearly identical to Latin counterparts. These class of attacks, where an attacker replaces one letter for its counterpart is widely known and are usually mitigated by the browser: <blockquote> In Chrome and Firefox, the Unicode form will be hidden if a domain label contains characters from multiple different languages. It is possible to register domains such as “xn–pple-43d.com”, which is equivalent to “аpple.com”. It may not be obvious at first glance, but “аpple.com” uses the Cyrillic “а” (U+0430) rather than the ASCII “a” (U+0041). The “аpple.com” domain as described above will appear in its Punycode form as “xn–pple-43d.com” to limit confusion with the real “apple.com”. </blockquote> So far so good, the browsers filters these types of counterpart character substitution. But there’s a catch. It appears that the mitigation fails when all characters in the URL use the same alphabet. The domain “аррlе.com” as in the website shown before, registered as “xn–80ak6aa92e.com”, bypasses the filter by using only Cyrillic characters. One can understand why a developer may have chosen this behaviour, nevertheless it presents a problem, as demonstrated. 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. If you are using Firefox, you can switch off the Punycode translation in about:config by changing network.IDN_show_punycode to true. If you are using Chrome, you’ll have to wait for the update. Or manually check the HTTPS certificate in HTTPS enabled websites. Aren’t you just tempted to register a domain to go and phish the phishers? [Thanks chrisatomix] </html>