Forum: Sécurité

Topic: Hameçonnage (Phishing) via IDN Punycode

Subject: Hameçonnage (Phishing) via IDN Punycode

Publié par: Lotesdelere
Contribution le : 20/04/2017 12:49:26

Punycode est un système utilisé par nos navigateurs pour utiliser des noms de domaines internationalisés (IDN):
https://fr.wikipedia.org/wiki/Punycode

Et ce afin d'utiliser et d'afficher des URLs avec charactères non ASCII: cyrillique, grec, chinois, etc, ou encore lettres accentuées.
Les noms de domaine internationalisés sont convertis dans un nom de domaine ASCII commençant par xn--.

Seulement voilà, des petits malins ont compris qu'ils pouvaient détourner cet avantage à leur profit en vous faisant croire que vous êtes sur un site légitime et de confiance alors que vous êtes sur un autre. C'est la technique du hameçonnage ou phishing en anglais.

Car la plupart des navigateurs afficheront par défaut l'URL "reconstituée" à partir du punycode, ce qui peut être détourné, par exemple:
https://www.xn--e1awd7f.com vous fera croire que vous êtes sur https://www.epic.com
https://www.xn--80ak6aa92e.com vous fera croire que vous êtes sur https://www.apple.com

Parade pour afficher l'URL réelle, mais "moche", dans Firefox et ses clones:
Taper dans about:config dans la barre d'adresse
Oui, oui, je vais faire attention
Taper "puny", sans les guillemets, dans la barre Rechercher
Faire un double click sur network.IDN_show_punycode afin de modifier sa valeur en "true"
C'est fait, fermer la fenêtre about:config

Pour Chrome et ses clones il semble qu'il n'existe pas de parade manuelle pour l'instant. Solutions possibles:
Utiliser l'extension Punycode Alert: https://chrome.google.com/webstore/det ... fghekidjibckjmhbhhjeomlda
Utiliser la version de développement 58.0.3029.81
Faire très attention aux URLs en attendant la release de la version 58

Sources (en anglais):
https://www.xudongz.com/blog/2017/idn-phishing/
https://en.wikipedia.org/wiki/IDN_homograph_attack
https://www.wordfence.com/blog/2017/04 ... firefox-unicode-phishing/
https://www.ghacks.net/2017/04/17/puny ... e-hard-internet-veterans/