Le ransomware Locky s'invite sur Facebook

Les campagnes de ransomwares ne faiblissent pas et testent de nouveaux vecteurs de propagation. Bart Blaze, chercheur en malware, a été sollicité par un ami qui a reçu une image « étrange » sur son compte Facebook. Il s'agissait d'un spam utilisant le chat de Facebook pour diffuser une image (au format .svg) intégrant un outil de téléchargement de malware nommé Nemucod. Un premier point à souligner est que l'image est capable de passer sous les radars des filtres anti-spam de Facebook.

L'utilisation de fichiers SVG (Scalable Vector Graphics) est importante. SVG est basé sur XML, ce qui signifie qu'un pirate peut intégrer n'importe quel contenu, comme du JavaScript. Dans ce cas-là, l'analyse du code a montré qu'il s'agissait bel et bien de JavaScript.

Redirigé vers une fausse page YouTube

En cliquant sur l'image, l'internaute est redirigé sur une page qui ressemble à YouTube. Une fois le site téléchargé, l'utilisateur est invité à télécharger à un codec pour lire la vidéo. Si celui-ci, présenté comme une extension de Chrome, est installé, alors Nemucod débarque et Locky aussi. Le rançongiciel peut ensuite à sa guise chiffrer les fichiers de l'ordinateur et réclamer de l'argent (habituellement en bitcoin) à la victime.

Bart Blaze conseille donc de se méfier des images envoyées notamment par des connaissances, « *surtout quand il n'y a que l'image dans le message* ». Fraser Kyne, directeur technique chez Bromium, se veut plus inquiétant en soulignant le fait que « *pas mal de personne regarde Facebook au bureau, il y a alors un grand risque pour la diffusion du malware au sein de l'entreprise* ». Locky a été découvert en février 2016 par des équipes de Palo Alto Networks et a impacté beaucoup d'entreprises à travers le monde.

A lire aussi

Ransomware : Locky active le mode pilotage automatique

Une variante de Locky se fait passer pour un fichier système Windows