Attention aux fausses mises à jour de Windows 10 dissimulant des Ransomware ! | Le Net Expert Informatique

Attention aux fausses mises à jour de Windows 10 dissimulant des Ransomware !

Il n'a pas fallu longtemps pour voir apparaitre les premières tentatives d'escroquerie autour de la mise à jour vers Windows 10 proposée par Microsoft depuis le 29 juillet 2015. Une première campagne de Ransomware vient d'être détectée.

Cette campagne s'appuie sur l'actualité brulante du moment, à savoir le lancement de la version finale de Windows 10 par Microsoft. L'objectif est de tromper les utilisateurs au sujet du téléchargement de la mise à jour gratuite. Il télécharge en réalité des fichiers malveillants sur leurs ordinateurs.

Définition d'un Ransomware selon Wikipédia:
Un Ransomware ou rançongiciel, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Windows 10, un contexte idéal pour les Ransomware
Disponible depuis quatre jours seulement, Windows 10 est désormais installé sur des dizaines de millions d'ordinateurs et Microsoft entrevoit une accélération de la demande. Windows 10 est l'actualité du moment et surtout un contexte idéal pour des campagnes de Ransomware. L'équipe Cisco Talos vient d'en détecter une.
Ses créateurs utilisent une adresse IP attribuée à la Thaïlande. Ils sont à l'origine d'un envoi massif d'emails soigneusement construits afin d'inviter leurs destinataires à installer Windows 10.
Ces e-mails s'accompagnent d'une pièce jointe, une archive ZIP, qui contient un exécutable qui lance CTB-Locker. Si l'antivirus présent sur la machine ne le détecte pas ou si l'archive en question n'a pas été vérifiée par un système web comme VirusTotal, le résultat est peu glorieux avec un verrouillage de données et l'apparition d'un message.
Celui-ci demande de payer une somme afin de rendre de nouveau accessible les données de l'ordinateur. Voici le message en question.

L'équipe Cisco explique qu'il s'agit ici d'une méthode
« standard […], en utilisant un cryptage asymétrique qui permet aux adversaires de crypter les fichiers de l'utilisateur sans avoir la clé de déchiffrement présente sur le système infecté. »
Les utilisateurs ont seulement quatre jours pour payer la «rançon». Les pirates se cachent au travers de « Tor » et de la monnaie « Bitcoin » afin d'être anonymes. Ils profitent ainsi de leur campagne de logiciel malveillant avec un risque minimal. L'équipe Cisco Talos recommande de créer des sauvegardes régulières de son PC et de stocker les archives en dehors de tous services en ligne.

Source : http://www.appy-geek.com/Web/ArticleWeb.aspx?regionid=2&articleid=45798024&source=hootsuite
Par GINJFO