Un ransomware inonde des millions d'utilisateurs d'Office 365

Des millions d'utilisateurs de Microsoft Office 365, la version Saas de la suite bureautique, ont été exposés à une attaque d'un ransomware appelé Cerber au cours de la semaine dernière. Dans un billet de blog, Steven Toole, un chercheur de la société Avanan, explique avoir détecté la première attaque de ce type le 22 juin au matin. Selon lui, si on se fie aux statistiques observées sur la base de clients d'Avanan, pas moins de 57 % des utilisateurs d'Office 365 ont reçu au moins un e-mail renfermant une pièce jointe infectée. C'est l'ouverture d'une macro incluse dans cette pièce jointe qui déclenche l'infection, se traduisant par le chiffrement de données clefs des utilisateurs touchés.

Récemment, lors de ses résultats trimestriels, Microsoft a revendiqué 18,2 millions d'abonnés à son service Office 365. Selon Steven Toole, Microsoft a mis plus de 24 heures à réagir et à bloquer les e-mails renfermant les pièces jointes infectieuses.

Le ransomware échappe aux outils d'Office 365

Cerber réclame à ses victimes 1,24 bitcoin, soit environ 720 euros, pour leur restituer l'accès aux données qu'il a chiffrées. De façon originale, le ransomware avertit ses victimes de son forfait tant via un message affiché à l'écran que par la lecture d'un fichier audio.

« *Cette attaque semble être une variante d'un virus détecté à l'origine sur des serveurs de mail en mars dernier*, écrit Steven Toole. *Cette fois, Cerber a été distribué massivement après que son auteur a pu avoir la confirmation que le virus était à même de passer au travers des outils de sécurité d'Office 365 via un compte mail privé ouvert sur ce service.* » C'est cette capacité des pirates à passer au travers des capacités de détection du premier éditeur mondial qui rend ce type d'attaques redoutable. « *De nombreux utilisateurs de services de messagerie dans le Cloud pensent qu'ils externalisent toute la chaîne chez Microsoft ou Google, y compris la sécurité* », rappelle Gil Friedrich, le Pdg de la firme de sécurité Avanan.

A lire aussi :

Ransomware : Locky reprend du service

Créer des ransomwares, une petite entreprise qui rapporte

CryptXXX : le ransomware qui vole aussi les mots de passe

crédit photo : ra2studio-Shutterstock