Koolova, un ransomware donneur de leçons

Considérés comme la plaie de la sécurité informatique en 2016, les auteurs de ces rançongiciels n'hésitent pas à jouer avec leurs victimes. On connaissait Popcorn Time demandant à la victime d'envoyer un lien malveillant à plusieurs personnes. Et si au moins deux utilisateurs étaient infectés à leur tour, le ransomware déverrouillait gratuitement les fichiers de l'expéditeur contraint.

Mais Michael Gillepsie, chercheur en sécurité, a découvert une variante d'un rançongiciel, nommé Koolova au comportement pour le moins étrange. En effet, il propose de déchiffrer gratuitement les fichiers en échange de la lecture de 2 articles concernant…les ransomwares. Encore au stade de développement, le spécialiste a réussi à mettre la main sur la page de revendication de Koolova. Sur cet écran, on peut lire qu'il se considère comme étant le jumeau gentil de Jigsaw. Ce dernier est un ransomware particulièrement vicieux en installant un compte à rebours et en effaçant progressivement les fichiers verrouillés tant que la personne ne s'est pas acquittée de la rançon.

Lire ou périr, telle est la question

Cette parentèle se retrouve chez Koolova avec l'obligation de lire deux articles sinon un compte à rebours s'enclenche avec la perspective de la suppression de fichiers. Les articles en question sont un message issu du blog de l'équipe de sécurité de Google intitulé, « Stay Safe, While Browsing » et un papier de BleepingComputer (qui s'est fait l'écho de Koolova) nommé « Jigsaw Ransomware Decrypted: Will delete your files until you pay the Ransom ». Une fois lu ces deux articles, un bouton sur la page de verrouillage, « *déchiffrer mes fichiers* » est activé. Quand on appuie dessus, Koolova se connecte au serveur de commande et contrôle pour récupérer la clé de déchiffrement et l'afficher dans un pop-up. Il suffit alors de la copier et de la coller dans le champ ad hoc.

L'absence de rançon est un peu étrange dans le comportement de Koolova. Traditionnellement, les auteurs de ce type de malware réclament le paiement d'une compensation en général en bitcoin.

Certains demandent une rétribution en cartes iTunes ou clament que les « *dons* » seront reversés à des associations caritatives. Mais dans ce cas-là, rien de financier, juste une volonté de donner une leçon aux internautes en les exhortant « *d'arrêter de télécharger des applications non sécurisées sur Internet* ». Quel cynisme !

A lire aussi :

Comment le ransomware est devenu le gagne-pain des cybercriminels

RansomFree, l'application qui leurre les ransomwares