

Les Ransomwares se multiplient

Ces codes malveillants, traduisibles en français par "rançongiciels", ont pour but de crypter des fichiers puis d'exiger une rançon en échange du mot de passe ou d'une clef de chiffrement permettant d'en déverrouiller l'accès.

Ces prises d'otage numériques ciblent principalement les extensions de fichiers .doc, .xls, .xml, c'est-à-dire les plus susceptibles de contenir des informations importantes.

Initialement construit autour d'un chiffrement faible, les plus récents ransomwares comme Gpcode était crypté sur 660 bits. Un chiffrement qui pour être cassé réclamerait 30 ans d'un labeur interrompu à un ordinateur dont le processeur est cadencé à 2,2GHz.

Alors que les ransomwares étaient initialement réservés aux entreprises, de plus en plus de virus de ce genre font leur apparition sur les bureaux de monsieur et madame Tout-le-Monde. Pour rappel, un ransomware et un fichier malicieux qui prend en otage vos données, généralement en les cryptant par un mot de passe et vous demande d'envoyer de l'argent en échange de la clé qui vous rendra vos données.

Ces fichiers peuvent être effacés sans problème, puisque ce sont ceux créés par le ransomware. Il est, enfin, conseillé aussi de mettre à jour son antivirus et son pare-feu. Vous pouvez aussi payer la somme de 10,99\$ aux auteurs du désagrément.