Locky revient à travers une nouvelle campagne de spam

Après plusieurs semaines de silence, la propagation du ransomware Locky reprend du service à travers une nouvelle campagne de spam, alerte My Online Security qui reproduit le contenu d'un message reçu le 21 avril dernier. Les PME sont particulièrement visées alors que l'objet de l'e-mail évoque un reçu de paiement qui se présente sous les intitulés « Receipt », « Payment » ou encore « Payment Receipt » suivi d'un nombre généré aléatoirement.

L'e-mail s'accompagne d'un fichier PDF dont l'intitulé ne fournit aucun indice quant à son contenu (P2724.pdf, par exemple). Si le destinataire de la missive a la mauvaise idée de cliquer sur la pièce jointe, le document qui s'affiche invite ce dernier à ouvrir un document Word ou Excel embarqué. Un mode opératoire des plus suspects pour le moins. Surtout lorsque s'affiche un message invitant à autoriser le logiciel à éditer le contenu du document (en cliquant sur le bouton qui apparait alors en haut de la page) sous prétexte que celui-ci a été créé avec une version plus récente de l'éditeur que celle installée sur la machine. Microsoft a en effet mis en place cette demande d'exécution pour justement lutter contre l'exécution automatique de macro malveillante. Une étape supplémentaire qui nécessite une interaction de l'utilisateur censée limiter les risques d'infection (sauf si l'exécution des macros est configurée pour démarrer automatiquement).

Paiement incontournable

Effectivement, le fichier Office contient une macro qui télécharge le fichier exécutable redchip2.exe qui n'est autre que Locky. Le fichier est en tout cas qualifié comme tel par une quarantaine d'éditeurs d'antivirus sur les 60 référencés par VirusTotal. Une fois téléchargé, le script s'exécute automatiquement et commence le chiffrement des fichiers du disque dur qui héritent alors de l'extension .OSIRIS. Espérons que cette suite de manipulations datant d'une époque antédiluvienne dans l'histoire de l'informatique aura mis la puce à l'oreille de l'utilisateur qui évitera ainsi de tomber dans le panneau.

Si, malgré l'ensemble des obstacles qui se dressent sur sa route Locky parvient à ses fins, sa victime en est alors informée par un message qui indique que *« tous vos fichiers ont été chiffrés en RSA-2048 et AES-128. […] Le décryptage de vos fichiers n'est possible qu'avec la clé privée et le programme de décryptage qui se trouvent sur notre serveur secret »*. Suit un mode d'emploi pour installer le navigateur Tor et une adresse du réseau d'anonymisation qui demande le paiement d'une rançon en bitcoins en échange de la clé de déchiffrement. A moins d'avoir fait une sauvegarde de ses données, l'utilisateur n'aura d'autre choix que de payer s'il veut espérer les récupérer (sans aucune garantie de service pour autant). Il n'existe, pour l'heure, aucun outil gratuit de déchiffrement de Locky.

Lire également
Ransomwares : 38 % des victimes paient leur rançon
Le ransomware Locky s'invite sur Facebook

Ransomware : Locky active le mode pilotage automatique