Le ransomware Jigsaw lance son compte à rebours

En plus de chiffrer et verrouiller, Jigsaw supprime progressivement les fichiers, et ce une heure après la demande de paiement (l'équivalent de 150 dollars en crypto-monnaie Bitcoin), relève *InfoWorld*. Le ransomware augmente ensuite le nombre de fichiers supprimés après chaque cycle de 60 minutes. Si aucun paiement n'est effectué dans les 72 heures, tous les fichiers restants seront détruits.

« Tentez quelque chose d'amusant et l'ordinateur appliquera plusieurs mesures de sécurité pour effacer vos fichiers », alerte un message illustré du masque de Jigsaw, le personnage de tueur de la série de films d'horreur Saw…

D'après le site d'assistance informatique BleepingComputer.com, le ransomware détruit un millier de fichiers à chaque redémarrage du PC. *« C'est la première fois que nous constatons l'application d'une telle menace par un ransomware »*, a commenté son fondateur, Lawrence Abrams, dans un billet de blog.

Une parade provisoire ?

Des spécialistes en sécurité ont trouvé une solution pour déchiffrer les fichiers sans avoir à payer. L'utilisateur victime de Jigsaw doit ouvrir le gestionnaire de tâches de Windows et stopper les processus firefox.exe et drpbx.exe pour éviter d'autres suppressions de fichiers, rapporte Lawrence Abrams. Il faut ensuite lancer l'utilitaire de Windows msconfig et supprimer l'entrée de démarrage qui pointe vers %UserProfile%\AppData\Roaming\Frfx\firefox.exe. Cette opération devrait arrêter le processus de destruction de fichiers et empêcher le malware de se relancer.

Les utilisateurs devront ensuite télécharger l'utilitaire Jigsaw Decrypter hébergé sur BleepingComputer.com et déchiffrer les fichiers. Une fois cette opération effectuée, Abrams recommande de télécharger un logiciel anti-malware et de lancer un scan du système.

Lire aussi :

Le ransomware Petya trébuche sur un bug de chiffrement

Ransomware Locky : la France parmi les deux principaux pays ciblés

SamSam, le plus petit des grands ransomwares, analysé