# Victime du ransomware Petya ? Décryptez gratuitement les fichiers | Denis JACOPINI


Victime du ransomware Petya ? Décryptez gratuitement les fichiers

**Il est possible de récupérer gratuitement ses fichiers après une infection par le ransomware Petya. Pas forcément simple à mettre en œuvre, une méthode a vu le jour.**

Petya bloque totalement l'ordinateur. Pour cela, il écrase le Master Boot Record du disque dur et chiffre la Master File Table sur les partitions NTFS (système de fichiers de Windows). Cette MFT contient les informations sur tous les fichiers et leur répartition.
La procédure malveillante laisse croire à une vérification du disque dur après un plantage et un redémarrage. La victime aura au final droit à une tête de mort en caractères ASCII et une demande de rançon (0,9 bitcoin) pour espérer récupérer ses fichiers et déchiffrer le disque dur prétendument chiffré avec un algorithme dit de niveau militaire.
Un bon samaritain (@leostone) a mis en ligne un outil pour se dépêtrer de Petya (https://petya-pay-no-ransom-mirror1.herokuapp.com) sans devoir payer une rançon. La procédure nécessite de récupérer des données d'un disque dur affecté pour obtenir une clé de déchiffrement promise en quelques secondes. Manifestement, il était simplement question d'un encodage en Base64.
Pour BleepingComputer.com, l'expert en sécurité informatique Lawrence Abrams a confirmé la validité de l'outil. Chercheur en sécurité chez Emisoft, Fabian Wosar a de son côté développé un outil Petya Sector Extractor (http://download.bleepingcomputer.com/fabian-wosar/PetyaExtractor.zip) permettant d'extraire facilement les données à fournir à l'outil de Leostone.
Bien évidemment, le disque dur infecté doit être connecté à un autre ordinateur afin de pouvoir y accéder (extraire les données pour l'outil de Leostone). Une fois la clé de déchiffrement obtenue, il est à replacer dans l'ordinateur d'origine et il faudra saisir la clé sur l'écran affiché par Petya.
L'existence de cette faille pour se débarrasser de Petya sans payer de rançon sera nécessairement portée à la connaissance de l'auteur du ransomware. Le code du nuisible pourrait dès lors être prochainement modifié en fonction.

---



Source : *Petya : une échappatoire contre le ransomware agressif*