Outil de déchiffrement du rançongiciel (ransomware) PyLocky versions 1 et 2

cybermalveillance.gouv.fr/nos-articles/outil-dechiffrement-rancongiciel-ransomware-pylocky-v1-2/

Publié le 11 juin 2019

decrypter ransomware | pylocky | ransomware | ransomware decryptor

13544 Temps de lecture : 6 min

Le ministère de l'Intérieur met à disposition du public sur la plateforme Cybermalveillance.gouv.fr, dont il est membre fondateur, un outil gratuit de déchiffrement du rançongiciel PyLocky.

1. Qu'est-ce que le rançongiciel PyLocky ?

PyLocky est un programme malveillant (appelé communément « virus ») de la catégorie des rançongiciels (ou *ransomware* en anglais). Il rend inaccessible les fichiers de la victime en les chiffrant et lui réclame une rançon en échange de la clef qui pourrait permettre d'en recouvrer l'accès.

PyLocky se propage généralement par message électronique (email) et se déclenche à l'ouverture d'une pièce jointe ou d'un lien piégés. Il est très actif en Europe et on compte de nombreuses victimes en France tant dans un cadre professionnel (entreprises, collectivités, associations, professions libérales) que particuliers.

2. Un outil de déchiffrement du rançongiciel PyLocky

Cet outil est le fruit de la collaboration des services du ministère de l'Intérieur, en particulier de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) de la Direction régionale de la police judiciaire de Paris qui a pu récolter dans le cadre de ses investigations des éléments techniques en association avec des chercheurs en sécurité bénévoles. Ces éléments ont permis au Service des technologies et des systèmes d'information de la sécurité intérieure ST(SI)², rattaché à la Gendarmerie nationale, de réaliser ce programme.

Programme de déchiffrement PyLocky

Pour télécharger le programme de déchiffrement PyLocky versions 1 et 2 et sa documentation, téléchargez le dossier ci-joint.

Publié le 20/07/2020ZIP 1 MoTélécharger

Cet utilitaire permet le déchiffrement des fichiers chiffrés avec les version 1 (fichiers chiffrés avec l'extension .lockedfile ou .lockymap) et version 2 (fichiers chiffrés avec l'extension .locky) de PyLocky. Il nécessite un ordinateur équipé du système d'exploitation Microsoft Windows 7 ou supérieur et l'environnement d'exécution Java JRE (Java Runtime Environnement) version 8.

Ce programme est fourni gracieusement « tel quel », sans support, ni garantie expresse ou implicite. Les auteurs ne pourront en aucun cas être tenus responsables d'éventuels dommages qui pourraient découler de l'utilisation de cet outil. Des déclinaisons de PyLocky peuvent avoir été réalisées et pourraient rendre cet utilitaire inopérant.

À noter que le déchiffrement des fichiers ne décontamine pas pour autant la machine infectée par le rançongiciel.

<img src="/medias/2019/11/Fiche-reflexe_rancongiciels.jpg" alt="Les rançongiciels (ransomwares
Les rançongiciels (*ransomwares*)

Apprenez à vous prémunir des rançongiciels grâce à notre fiche réflexe consacrée au sujet.

Publié le 08/04/2021PDF 117 KoTélécharger

D'autres outils de déchiffrement de rançongiciels (ransomware) sont disponibles sur le site Nomoreransom.org. Cette plateforme est une initiative issue de la coopération des polices européennes, d'Europol et de sociétés privées spécialisées en cybersécurité.

A lire aussi

Comment identifier et supprimer un virus ?

Voir l'actualité

Inscrivez-vous à la newsletter

Tenez-vous informé(e) de l’actualité de la cybermalveillance et des nouvelles menaces

Détail de l'abonnement :