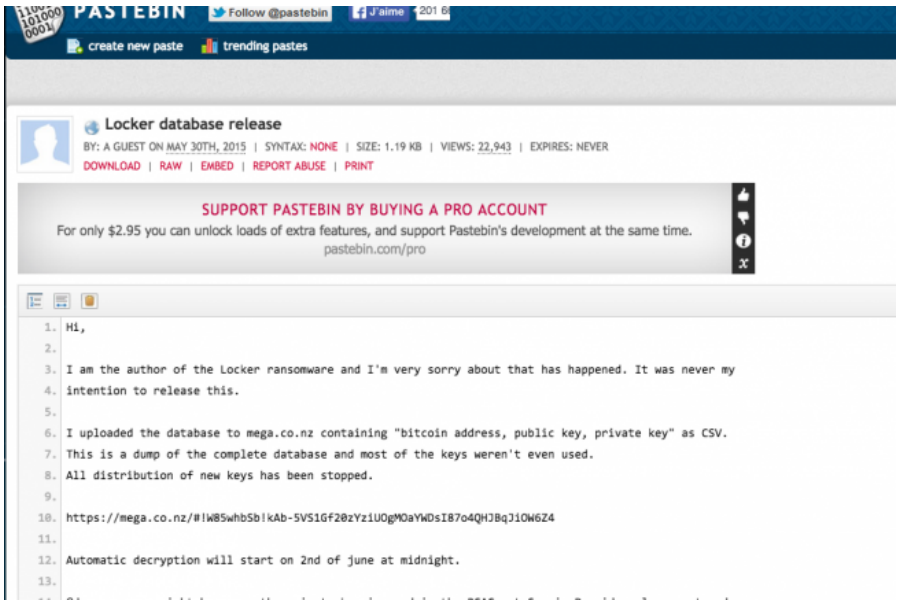
Des clés pour débloquer des milliers d’ordinateurs victimes d’un ransomware – Le Monde Informatique | Le Net Expert Informatique



Des clés pour débloquer des milliers d’ordinateurs victimes d’un ransomware

L'auteur présumé du ransomware Locker présente ses excuses pour les actions commises et affiche les clefs pour déchiffrer les fichiers verrouillés avec son outil.

Dans une sortie particulièrement étonnante sur Pastebin, l'auteur présumé du ransomware Locker, également connu sous le nom CryptoLocker V, a publiquement présenté ses excuses aux milliers de victimes du malware. Dans la foulée, il a publié une base de données avec les clés capables de déverrouiller les machines et les fichiers infectés. Ce geste est particulièrement rare dans le petit monde des développeurs de ransomwares qui sont parmi les plus impitoyables sur Internet.
Le nombre de victimes de Locker n'est pas très clair (le fichier .csv de clés / adresses Bitcoin semble avoir 62 000 entrées), mais les machines bloquées pourraient être beaucoup plus nombreuses. Pendant des mois, le programme avait discrètement infecté des utilisateurs en utilisant une version piégée de Minecraft. Les fichiers ciblés comportaient des extensions : .doc, .docx, .xlsx, .ppt, .jpg, cru, .odf, .rtf, .dbf, .odb et DBF.

Un déverrouillage complexe
Seul un petit pourcentage du nombre total de victimes aura payé la rançon, exigé en Bitcoins, mais le développeur a également publié des documents indiquant que les demandes de paiements pourraient être dix à vingt fois plus importantes. « Je suis l'auteur du ransomware Locker et je suis vraiment désolé de ce qui est arrivé. Il n'a jamais été dans mon intention de propager ceci », a annoncé quelqu'un se faisant appeler «Poka BrightMinds », dans un message sur Pastebin le jour de la publication des clefs de chiffrement.
Malheureusement, le processus de déverrouillage se révèle être particulièrement complexe. Pour toutes les personnes qui ont encore le malware sur leur PC, la commande de déblocage aurait été automatiquement envoyée le 2 juin, après quoi ils auront reçu le message suivant à travers le logiciel lui-même : « Je suis désolé pour le chiffrement, vos fichiers sont déverrouillés gratuitement. Soyez bon pour le monde et n'oubliez pas de sourire:). » Cependant, tous ceux qui ont désinstallé manuellement le logiciel malveillant en utilisant un utilitaire anti-virus devront utiliser l'outil Locker Unlocker développé par un chercheur qui peut être téléchargé à partir du site Bleeping Computer (http://www.bleepingcomputer.com/forums/t/577953/locker-developer-releases-private-key-database-and-3rd-party-decrypter-released).

Des intentions inconnues
Les chercheurs et les analystes en sécurité ont exprimé leur énorme surprise et leur perplexité quant aux dernières déclarations de l'auteur de ce logiciel malveillant. « Cela n'est jamais arrivé auparavant ! », a déclaré Stu Sjouwerman de KnowBe4, un cabinet de conseil américain qui a dressé une liste des victimes du ransomware. « L'auteur semble avoir soit gagné tellement d'argent qu'il se retire de cette campagne criminelle, ou bien il craint de se faire attraper par les forces de l'ordre, ou il aurait été menacé par une cybermafia locale », a-t-il dit. « Maintenant, tout cela semble assez plan-plan. Si vous écrivez ce type de code, vous savez très bien ce que vous faites. Le fait qu'il ait été conçu comme un malware dormant dénote une planification minutieuse étalée sur de longs mois. »
Il y a un point indiscutable. Tous les gens infectés ne verront pas le message indiquant qu'ils pourront inverser le processus, et tous ceux qui ont déjà payé une rançon en bitcoins doivent bien être conscient qu'ils ne seront jamais remboursés. Le mal a déjà été fait.

Source : http://www.lemondeinformatique.fr/actualites/lire-des-cles-pour-debloquer-des-milliers-d-ordinateurs-victimes-d-un-ransomware-61394.html
Par Serge Leblal