No More Ransom : coordination européenne contre les ransomwares

Tous les acteurs de la sécurité s'accordent à dire qu'actuellement les ransomwares sont la plaie numéro 1. Ces applications malveillantes se propagent rapidement et surtout évoluent rapidement au gré de l'imagination des cybercriminels. Rappelons que le rançongiciel a pour objectif de cadenasser des fichiers sur l'ordinateur d'un utilisateur. Ces fichiers peuvent être déverrouillés contre le paiement d'une somme d'argent, en bitcoin.

Face à cette montée en puissance, la riposte ou tout du moins la défense s'organise. La police nationale néerlandaise, Europol, Intel Security et Kaspersky Lab se sont associés pour lancer l'initiative « No More Ransom ».

Elle se traduit par l'ouverture d'un portail www.nomoreransom.org dont l'objectif est double. Il a d'abord une vocation informative à travers un onglet de questions-réponses sur les ransomwares, ainsi que des conseils de prévention. On notera par exemple l'importance de la sauvegarde. « backup ! backup ! backup ! », peut-on lire sur le site, tout comme la déconnexion du réseau immédiate en cas d'attaque pour éviter la propagation du malware.

4 outils de déchiffrement

Deuxième objectif du portail, l'aide aux victimes pour récupérer les données sans avoir à verser d'argent aux cybercriminels. Pour débuter, il fournit 4 outils de déchiffrement adaptés à différents types de ransomwares. On retrouve, Coinvault qui a été développé par la police nationale néerlandaise et qui a vocation à déchiffrer les rançongiciels Coinvault et Bitcryptor. Il y a également Rannoh, qui vient à bout d'Autoit, Fury, Crybola, Cryakl et CryptXXX versions 1 et 2. Autre outil : RakhniDecryptor capable de traiter, Rakhni, Agent.iih, Aura, Autoit, Pletor, Rotor, Lamer, Lortok, Cryptokluchen, Democry et Bitman (TeslaCrypt) versions 3 et 4. Et enfin, le dernier outil se nomme Shade Decryptor et s'attaque à une variante du programme Shade.

Cette initiative en est à ses débuts et chacun veut croire qu'elle va s'étoffer avec le temps. « *Nous espérons voir ce projet s'étoffer avec l'arrivée de renforts supplémentaires au fur et à mesure que d'autres entreprises et représentants de forces de l'ordre d'autres pays se joindront à notre combat* », explique Jornt van der Wiel chercheur en sécurité au sein de la l'équipe globale de recherche et d'analyse (GReAT) de Kaspersky Lab.

Cet effort de sensibilisation est donc un premier pas. Il gagnerait à décliner le portail dans les différentes langues de l'UE. Il n'est pas sûr que pour le grand public, la langue de Shakespeare soit la plus adaptée pour faire passer des messages de prévention. Ensuite, la vitesse d'évolution des rançongiciels est telle que la liste d'outils de déchiffrement apparaît bien pauvre. Reste qu'il fait saluer tous les efforts pour combattre ce fléau.

A lire aussi :

Satana, un ransomware pire que Petya

Un ransomware inonde des millions d’utilisateurs d’Office 365

Crédit Photo : Bacho-Shutterstock