# Un logiciel d’extorsion (ransomware) utilise un simple fichier batch


Un logiciel d’extorsion (ransomware) utilise un simple fichier batch
Informatique

**Des chercheurs de Symantec ont récemment identifié une menace d’extorsion qui fonctionne avec un script et une ligne de commande en utilisant le programme de chiffrement Open Source GnuPG.**

Pour extorquer de l’argent aux utilisateurs, des pirates ont mis au point un nouveau programme capable de chiffrer les fichiers sur l’ordinateur cible. Ce nouveau type de malware indique que les attaquants n’ont plus besoin de compétences pointues en programmation pour créer de dangereux programmes d’extorsion (ransomware) très efficaces, surtout quand les technologies de chiffrement avancé sont accessibles gratuitement. Des chercheurs du fournisseur d’antivirus Symantec sont récemment tombés sur un logiciel malveillant de ce type, d’origine russe, dont le composant principal se limite à un simple fichier batch, c’est à dire un script avec une ligne de commande. Cette stratégie de développement permet à l’attaquant de contrôler et de mettre facilement à jour le malware, explique dans un billet le chercheur Kazumasa Itabashi.

Le fichier batch télécharge une clef publique RSA en 1024 bits depuis un serveur et l’importe dans GnuPG, un programme de chiffrement gratuit qui fonctionne également par ligne de

commande. GnuPG est une implémentation Open Source de la norme de chiffrement OpenPGP. Il est utilisé pour chiffrer les fichiers de la victime avec la clé téléchargée. « Si l'utilisateur veut déchiffrer les fichiers concernés, ils a besoin de récupérer la clé privée de l'auteur du malware », indique le chercheur.

**Une rançon de 150 € pour déchiffrer ses propres données**

Dans le chiffrement à clé publique sur lequel est basé OpenPGP, les utilisateurs génèrent une paire de clés associées, l'une rendue publique et l'autre qui reste privée. Le contenu chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante. La nouvelle menace représentée par le ransomware que Symantec appelle Trojan.Ransomcrypt.L chiffre les fichiers avec les extensions suivantes: .xls, .xlsx, .doc, .docx, .pdf, .jpg, .cd, .jpeg, .1cd, .rar, .mdb et .zip. Les victimes sont invitées à payer une rançon de 150 € pour récupérer la clef privée.

Ce qui distingue le Trojan.Ransomcrypt.L des autres malwares ne tient pas à l'usage du chiffrement à clé publique – d'autres menaces adoptent la même technique – mais à sa simplicité et au fait que l'auteur a choisi d'utiliser un programme de chiffrement légal et Open Source, au lieu de créer sa propre mise en oeuvre, ce que font souvent les auteurs de malwares.

**Les chercheurs prévoient une augmentation des menaces**

Il existe certains programmes d'extorsion complexes avec des fonctionnalités avancées, développés essentiellement pour être vendus à d'autres cybercriminels qui n'ont pas les compétences nécessaires. Mais Trojan.Ransomcrypt.L montre qu'il est devenu possible de développer ce type de logiciels malveillants à peu de frais et sans connaissance de programmation avancée. Si bien que les chercheurs de Symantec s'attendent à une augmentation du nombre de menaces de ce type dans l'avenir.

Article de Jean Elyan avec IDG News Service

**Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)**

**Références :**
http://www.lemondeinformatique.fr/actualites/lire-un-logiciel-d-extorsion-utilise-un-simple-fichier-batch-58248.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter