CryptXXX : le ransomware qui vole aussi les mots de passe

La vague des ransomware qui se limitent à chiffrer les fichiers et à les libérer contre rançon semble laisser la place à des malwares multifonctions. Il en est ainsi de CryptXXX (Trojan-Ransom.win31.CryptXXX) dont la dernière version tente de voler les mots de passe en plus de rendre inaccessible les contenus du disque.

Découverte fin mai, la version 3.100 de CryptXXX renferme le module StillerX qui, comme son nom le suggère, se charge de dérober des informations confidentielles comme les identifiants de connexion et les mots de passe. Une double source de revenus en perspective pour les cybercriminels, qui peuvent espérer à la fois recueillir les fruits de la rançon tout cherchant à revendre les données confidentielles volées ou les exploiter pour de futures attaques.

StillerX, le voleur autonome de CryptXXX

StillerX est une bibliothèque logicielle (stiller.dll, stillerx.dll et stillerzzz.dll) qui accompagne CryptXXX sous la forme d'un plugin. Mais il peut aussi être utilisé comme un agent autonome, souligne Proofpoint. Ecrit en Delphi, comme le ransomware qui l'embarque, le malware voleur *« vise les identifiants d'une large gamme d'applications allant d'un logiciel de poker aux identifiants des VPN Cisco »*, indique le fournisseur de solutions de sécurité, qui liste notamment les services de messagerie, de FTP, les navigateurs, les outils d'administration à distance ou encore les données de Microsoft Credential Manager parmi les applications visées. *« Outre les informations d'identification des fonctions de saisie, nous avons trouvé des routines, inutilisées, propres aux systèmes d'empreintes digitales et des routines d'exfiltration de données. »*

StillerX n'est pas la seule nouveauté de CryptXXX. Le malware découvert en avril dernier a su déjouer les outils de déchiffrement que Kaspersky à développés et mis à disposition à deux reprises courant mai. De plus, la version 3.100 du malware concentre désormais son activité sur le scan du port 445 à la découverte des différentes composantes du réseau local (LAN) dans l'espoir de découvrir les disques partagés sous Windows. *« Cette nouvelle version de CryptXXX est capable de trouver des ressources partagées sur le réseau, listant les fichiers dans chaque répertoire partagé, et les cryptant un par un »*, écrit Proofpoint. Enfin, les auteurs de CryptXXX ont également introduit un système de blocage d'écran des PC infectés accentuant la difficulté à accéder au système de fichiers pour l'administrateur.

Des évolutions rapides

Les évolutions rapides de versions de CryptXXX (voire liste ci-dessous) montrent que ses auteurs n'ont pas l'intention de se laisser dépasser par les éditeurs de sécurité et entendent tirer un maximum de profit des infections qu'ils génèrent à partir d'un seul agent malveillant. Et l'arrêt de TeslaCrypt (lire ce télégramme) laisse penser qu'un certain nombre de ses utilisateurs se sont tournés vers CryptXXX *« qui est très répandu »*, s'inquiète Profpoint. Qui prévient : *« sans outil de*

décryptage disponible, les utilisateurs et les organisations doivent se concentrer sur la détection et la prévention ».

Les différentes versions de CryptXXX depuis sa découverte :

- 1.001 le 16 avril
- 2.000 le 29 avril
- 2.006 le 9 mai
- 2.007 le 11 mai
- 3.000 le 16 mai
- 3.002 le 24 mai
- 3.100 le 26 mai

Lire également

[Le ransomware Locky mute pour multiplier ses victimes en France]
[Créer des ransomwares, une petite entreprise qui rapporte]
[ZCryptor : le ransomware Windows qui progresse comme un ver]

Crédit Photo : Bacho-Shutterstock