Le ransomware Petya trébuche sur un bug de chiffrement

Il y a quelques semaines, Petya faisait son apparition dans le catalogue des menaces à prendre au sérieux. Le rançongiciel se démarquait de ses congénères en s'attaquant au disque dur des ordinateurs. Concrètement, un fichier (transmis par mail) contient un exécutable 32 bits autoextractible (.exe) représenté par l'icône du programme de décompression WinRAR. C'est lui qui contient la charge utile nécessaire à l'implantation de Petya.

L'ouverture déclenche le redémarrage de la machine (via la commande *ExitWindowsEx* ou *NtRaiseHardError*). Auparavant, du code a été écrit sur les secteurs d'amorçage du disque, grâce à une élévation de privilèges. Petya simule alors l'exécution de l'outil *chkdsk*, qui se lance habituellement sur les PC Windows lorsque des erreurs ont été détectées sur le disque. Il en profite pour écraser le Master Boot Record (MBR) du disque dur et chiffrer la Master File Table (MFT) sur les partitions NTFS (contenant le nom, la taille et la localisation des fichiers).

Extraire des données pour les déchiffrer

Difficile de trouver une parade à ce fléau numérique. Et pourtant, le salut est venu de Twitter via un utilisateur, connu sous le pseudo Leostone. Son tweet est assez sybillin :

« #petya #ransomware #defeated. Get your disks back here: https://petya-pay-no-ransom.herokuapp.com ».

Le lien renvoie vers un outil, disponible sur GitHub, qui agit comme un générateur de mot de passe pour Petya en s'appuyant sur une méthode dite d'algorithme génétique.

Pour l'utiliser, il est nécessaire de placer le disque dur infecté dans un PC sain sous Windows. La victime doit alors extraire certaines données : 512 octets débutant au secteur 55 (0x37h) avec un offset de 0 (0x0) et 8 octets encodé en 64 bits au secteur 54 (0x36) avec un offset de 33 (0x21). Ces données doivent être encodées en Base64 et placées dans l'application web de Leostone ; l'utilisateur peut alors trouver le mot de passe Petya pour débloquer ses fichiers sans payer de rançon. Cette technique s'appuie sur un défaut de chiffrement du ransomware. Simple négligence des créateurs ?

Efficace jusqu'à quand ?

Toujours est-il que la méthode développée par Leostone est efficace. Bleeping Computer, société spécialisée dans la sécurité informatique, confirme son bon fonctionnement et même sa rapidité. Un des responsables a mis 7 secondes pour trouver la clé de déchiffrement. Par contre, la manipulation peut s'avérer problématique pour la plupart des utilisateurs. Un chercheur en sécurité d'Emisoft, Fabian Wosar, a donc développé un module gratuit baptisé Petya Self Extractor. Il permet d'extraire facilement les données citées ci-dessus. Il est par contre toujours nécessaire de placer le disque dur infecté dans un environnement sain.

Selon nos confrères d'*Ars Technica*, des experts allemands avaient pointé du doigt la semaine dernière le fait que Petya, dans sa première mouture, utilisait un niveau de chiffrement assez

basique (XOR). Une faiblesse que Leostone a réussi à exploiter. Il reste maintenant à savoir quelle sera la réaction des développeurs de Petya qui, fort de cette connaissance, peuvent assez simplement adapter et renforcer le chiffrement. Les solutions présentées ci-dessus seront alors inopérantes.

A lire aussi :

Les ransomwares s'engouffrent dans la faille zero day de Flash
Les ransomwares prennent le chemin des écoliers