Le ransomware Petya verrouille complétement le disque dur

Symantec en avait cerné la montée en puissance dans l'édition 2015 de son rapport Security Threat; BitDefender, comme AVG et Fortinet, y entrevoyait l'une des tendances de la cybersécurité en 2016 : la menace **rançongiciel** se fait plus tangible.

En France, la vigilance s'est véritablement accrue avec **Locky**, objet d'une campagne de diffusion massive qui a visé plusieurs organisations, dont l'AFP à au moins deux reprises. La rédaction de *Silicon.fr* (groupe NetMediaEurope, éditeur d'*ITespresso.fr*) a également été prise pour cible.

Ces derniers mois, on a également vu émerger le premier « vrai » ransomware pour les systèmes Mac OS X (KeRanger). Et le phénomène s'est décliné sur mobile (Zitmo, Lockerpin, Fakedefender…), forçant certaines victimes – au rang desquelles un hôpital californien – à verser une rançon pour restaurer rapidement l'accès à leurs fichiers.

Mais les cybercriminels rivalisent d'ingéniosité pour faire évoluer les ransomwares comme le montre le dernier en date : Petya.

Une prise directe avec le disque dur

Principal canal de propagation : la messagerie électronique, avec un e-mail semblant émaner d'une personne en recherche d'emploi. Les documents associés sont dits « trop gros » pour être mis en pièce jointe. L'expéditeur, apparemment légitime, les a donc placés dans un partage Dropbox (depuis Dropbox a supprimé le dossier virtuel contenant le logiciel ainsi que les comptes liés à la diffusion du malware).

Parmi ces fichiers figurent 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. Dans le cas présent, l'opération ne consiste pas à vérifier le volume, mais à chiffrer la table de fichiers… voire plus.

Un haut degré de chiffrement

Les versions divergent sur les forums du média allemand Heise. Ainsi un utilisateur a-t-il pu procéder à une réparation via un simple CD de Windows 7, quand un autre a constaté que tout son disque était chiffré (en RSA 4096 bits et AES-256) et qu'il n'était même plus reconnu comme un volume NTFS.

Dans tous les cas, il est demandé à la victime de verser 0,9 bitcoin (environ 340 euros au cours actuel) en échange de la clé qui lui permettra de récupérer ses fichiers. La transaction ne peut se faire que via le *darkweb* ; plusieurs liens sont fournis à cet effet, avec des consignes pour télécharger le navigateur Web du projet Tor, précise ITespresso.

La première soumission d'une souche de Petya sur VirusTotal remonte au 23 mars 2016. Selon les définitions du 29 mars 2016, plusieurs antivirus de renom ne détectent toujours pas le *malware*. Notamment ceux de Microsoft, Avast et DrWeb.

Pour une analyse détaillée du programme d'encodage et des secteurs infectés (routine de déchiffrement, de vérification du mot de passe, etc.), on se référera au forum Kernel Mode, où se trouvent par ailleurs des « échantillons » de Petya.

A lire aussi :

Johanne Ulloa, Trend Micro : « La v2 du ransomware est déjà là »
Ransomware : un tiers des Français prêts à payer et seulement 188 €

crédit photo © Green Jo – shutterstock