Un vaccin pour enrayer le ransomware Petya

Depuis hier, le monde a subit une nouvelle vague de ransomware. Au centre de cette menace, le rançongiciel Petya est le principal protagoniste avec des appellations différentes en fonction des éditeurs : NotPetya, Petna ou SortaPetya. Une variante très virulente qui a déjà fait beaucoup de victimes.

Comme dans le cas de WannaCry, les spécialistes de sécurité informatique se sont penchés sur ce rançongiciel avec l'espoir de trouver un killswitch. Ce processus d'autodestruction du malware avait été découvert par hasard par un jeune chercheur, connu sous le pseudo Malware Tech. Il avait enregistré un domaine apparaissant dans le code du malware, bloquant l'exécution et la diffusion de WannaCry. D'après le chercheur, le domaine libre qu'il a enregistré correspondrait en réalité à une sécurité imaginée par les développeurs du malware, afin d'éviter les analyses par les systèmes de sécurité basée sur des sandbox. Dans le cas de Petya, les chercheurs ont tenté de trouver cette même procédure, en vain.

Créer un fichier « perfc » dans Windows

La réponse est venue d'une autre voie découverte par Amit Serper, chercheur chez Cybereason, société de sécurité. Il a analysé le fonctionnement du ransomware et a découvert qu'il cherchait en local le fichier « perfc » et qu'il abandonnait son processus de chiffrement si ce fichier était déjà présent sur le disque. Cette trouvaille a été validée par d'autres éditeurs de sécurité, comme PT Security, TrustedSec et Emsisoft, rapporte nos confrères de *Bleepingcomputer*. Ces derniers ont même mis en ligne un fichier bat pour faciliter la mise en place de procédé (à condition d'avoir les droits administrateurs).

L'astuce est donc de créer un fichier du nom « perfc », en lecture seule, dans le dossier C: \ Windows. Attention, le chercheur précise que cette méthode s'apparente à une vaccination et non pas à un remède miracle. Elle vise à éviter l'infection des PC et des serveurs, pas de les guérir.

A lire aussi :

Petya : 5 questions pour comprendre le ransomware qui terrorise les entreprises

Le ransomware GoldenEye infecte plusieurs entreprises, dont Saint-Gobain

Photo credit: Dr PS Sahana * Kadamtala Howrah via Visualhunt.com / CC BY