Un expert en sécurité français trouve une parade à WannaCry… sous XP

Adrien Guinet, chercheur en sécurité chez Quarkslab, a trouvé une parade pour le ransomware **WannaCry**. Mais qui n'est valable que pour les machines fonctionnant sous **Windows XP**.

Après le processus de chiffrement des données par le malware, la clé utilisée pour crypter les données reste en effet présente en mémoire sous XP. Ce n'est pas une erreur de la part des pirates, explique l'expert. Ces derniers ont en effet utilisé correctement **l'API de cryptographie de Windows**, qui efface les clés de la mémoire lorsque CryptReleaseContext est appelé. Mais pas sous Windows XP.

À bien des égards, c'est donc une faille de sécurité de Windows XP qui permet de récupérer la clé de chiffrement utilisée par WannaCry. Et ainsi de disposer du précieux sésame permettant de récupérer ses données.

Un outil Open Source pour repérer la clé de chiffrement

Adrien Guinet propose Wannakey, un outil Open Source permettant de retrouver la clé utilisée par WannaCry. Une fois la clé détectée en mémoire, il sera possible d'utiliser Wannafork (depuis un autre PC) pour déchiffrer les fichiers.

Notez que cet outil n'a pas été testé intensivement, et qu'il pourrait donc ne pas fonctionner sur certaines machines. De plus, la technique qu'il emploie **ne sera pas transposable** sur les PC pourvus de Windows 7, 8, 8.1 ou 10.

À lire aussi :
WannaCry : du code nord-coréen… dans un malware américain
WannaCry met en lumière le phénomène des anti-updates
La parade n'existe pas pour contrer les futures affaires WannaCry