Quand les malwares se cachent dans les journaux Windows

Injecter du code malveillant dans des journaux Windows ? Kaspersky a constaté, en début d'année, l'utilisation de cette technique. Il vient d'en rendre compte publiquement. Ce n'est pas là le seul élément remarquable de l'attaque que relate l'éditeur russe. Mais c'est, à l'en croire, le plus « innovant ».

Parmi les autres éléments remarquables, il y a diverses méthodes d'évasion. Dont :

– Manipulation d'API Windows de traçage et d'analyse *antimalware*
– Recours à de multiples compilateurs et couches de chiffrement
– Signature d'une quinzaine de modules

L'attaque implique plusieurs briques issues des boîtes à outils SilentBreak et Cobalt Strike. Au bout de la chaîne se trouvent deux chevaux de Troie communiquant sur HTTP et SMB. Tout en amont se trouve une archive RAR que la victime est censée avoir téléchargée.

À un stade de l'attaque, WerFault (fonction de rapport d'erreurs de Windows) entre en jeu. Ou plus précisément une copie, placée dans le dossier des tâches Windows. Elle fait appel à un chargeur – déguisé en DLL – qui intercepte les *logs* du service de gestion de clés (KMS). Et donc le code malveillant, qu'il reconstitue… et qui s'exécute avec plusieurs paramètres dont l'adresse mémoire des chevaux de Troie.

Kaspersky affirme ne pas avoir détecté de similitudes avec du code exploité dans de précédentes attaques. Il insiste toutefois sur la prédominance de modules issus de SilentBreak.

Photo d'illustration © Pavel Ignatov – Shutterstock