NotPetya : certaines victimes vont pouvoir récupérer leurs données

Déchiffrer les données prises en otage par NotPetya, ce malware qui, parti d'Ukraine, a dévasté de nombreuses entreprises (Saint-Gobain, Maersk, Mondelez, WPP…) à partir du 27 juin ? Des chercheurs ont en effet découvert une technique pour récupérer des fichiers chiffrés par l'attaque du mois dernier.

Le malware NotPetya, le nom donné par Kaspersky à la nouvelle menace, est basé sur un ransomware connu, Petya, mais son code a été modifié de telle sorte que les systèmes qu'il infecte ne peuvent pas être entièrement restaurés. Plus qu'un véritable ransomware, NotPetya est plutôt un 'wiper', une souche destructrice ; les assaillants n'ayant visiblement aucune intention de livrer la clef de déchiffrement aux utilisateurs, même après paiement de la rançon.

Un chiffrement trop faible avec Salsa20

La société Positive Technologies, spécialisée dans la cybersécurité, a constaté que, en raison d'erreurs dans la manière dont le logiciel malveillant effectue le chiffrement des données qu'il prend en otage, une récupération des fichiers peut parfois être effectuée sans avoir accès à la clé des assaillants.

Dans les cas où NotPetya a obtenu des privilèges d'administrateur, il chiffre les données de ses victimes à l'aide de l'algorithme Salsa20. Selon Positive, en raison d'une erreur de mise en œuvre de ce dernier, seule la moitié des octets de chiffrement sont utilisés, ce qui rend le système plus facile à casser.

Positive assure que cette erreur, combinée à quelques autres approximations dans la programmation, permet d'envisager la mise en place d'une technique de déchiffrement des données prise en otage. « *Beaucoup de données différentes sont chiffrées à l'aide des mêmes fragments clés* », écrit Dmitry Sklyarov, responsable de reverse engineering de Positive dans un billet de blog. « *Ce qui permet de mettre en œuvre une attaque triviale basée sur un texte en clair connu des victimes* », autrement dit de forcer le verrou mis en place par les assaillants.

NotPetya sans droit d'admin : peu d'espoirs

Si la technique manuelle que dessine Positive est hautement technique et ne serait pas accessible à la plupart des utilisateurs, Sklyarov explique que des outils pourraient être développés pour mener à bien cette opération de façon automatisée. « *Nous pouvons nous attendre à ce que les prestataires de services puissent récupérer plus de données que ce qui a été possible jusqu'à aujourd'hui* », écrit-il.

En revanche, si NotPetya n'a, lors de l'infection, pas obtenu de droits d'administrateur, il a chiffré les données à l'aide d'une technique différente. Une clé est alors nécessaire pour récupérer les fichiers pris en otage, assure Sklyarov, notant qu'il n'y a aucun moyen de savoir dans combien de cas Salsa20 a été utilisé. Donc la proportion d'utilisateurs pour qui il reste un espoir.

A lire aussi :

Une clef de déchiffrement pour Petya… mais pas pour NotPetya

NotPetya : une facture de plus de 110 M€ pour le groupe pharmaceutique Reckitt

Guillaume Poupard, Anssi : « NotPetya, c'est de la médecine de guerre »