Petya, le nouveau ransomware qui chiffre l’ensemble du disque

Petya, le nouveau ransomware qui chiffre l’ensemble du disque

Le G DATA Security Labs a détecté les premiers fichiers ce jeudi 24 mars, en Allemagne, d'un nouveau type de ransomware nommé Petya.

A la différence des codes actuels, tels que Locky, CryptoWall ou TeslaCrypt, qui chiffrent certains fichiers du système, Petya chiffre l'ensemble des disques durs installés.

.

La campagne actuellement en cours vise les entreprises

Dans un email au service des ressources humaines, il y a une référence à un CV se trouvant dans Dropbox. Le fichier stocké dans le partage Dropbox est un exécutable. Dès son exécution, l'ordinateur plante avec un écran bleu et redémarre. Mais avant cela, le MBR est manipulé afin que Petya prenne le contrôle sur le processus d'amorçage. Le système démarre à nouveau avec un message MS-Dos qui annonce une vérification CheckDisk. A défaut d'être vérifié, le système est chiffré et plus aucun accès n'est possible.

Le message est clair : le disque est chiffré et la victime doit payer une rançon en se connectant à une adresse disponible sur le réseau anonyme TOR. Sur la page concernée, il est affirmé que le disque dur est chiffré avec un algorithme fort. Après 7 jours, le prix de la rançon est doublé. Il n'y a pour le moment aucune certitude sur le fait que les données soient irrécupérables.

Il est donc recommandé aux entreprises et particuliers de redoubler de vigilance quant aux emails reçus… [Lire la suite]

Réagissez à cet article

Source : *Petya : un nouveau ransomware qui chiffre l'ensemble du disque*