IBM livre un malware avec ses systèmes de stockage Storwize

IBM a accidentellement envoyé des clés USB contenant un logiciel malveillant à certains clients ayant commandé ses systèmes de stockage flash IBM Storwize V3500, V3700 et V5000 Gen 1. Le logiciel malveillant est contenu dans le support renfermant l'outil d'initialisation de ces systèmes. Si cet utilitaire est lancé, le malware est copié sur le disque dur dans un dossier temporaire. L'application malveillante n'est donc pas lancée automatiquement, ce qui constitue un moindre mal. IBM n'a pas précisé quelles étaient les conséquences de l'installation de ce malware.

Dans une alerte, Big Blue exhorte ses clients à détruire les clefs immédiatement ou à les nettoyer avant toute réutilisation, via un formatage. Une copie de l'outil d'initialisation peut ensuite être téléchargée depuis le site d'IBM, décompressée et replacée sur le support USB, désormais débarrassé de toute souche infectieuse.

Effacer le répertoire où loge le virus

Si le support de stockage amovible a déjà été utilisé, IBM conseille aux entreprises de s'assurer que leurs antivirus sont bien à jour afin que le problème puisse être résolu. Big Blue a également placé en ligne une liste des différents fournisseurs d'antivirus qui identifient correctement le malware.

« *Si vous avez utilisé la clef USB d'initialisation d'un des produits IBM répertoriés et l'avez insérée dans un ordinateur de bureau ou un ordinateur portable pour initialiser un système Storwize, IBM vous recommande de vérifier que votre logiciel antivirus a déjà supprimé le fichier infecté ou de supprimer le répertoire contenant le fichier malveillant* », explique la société d'Armonk. Soit, sur Windows, %TMP%\initTool et sur Linux (ou Mac) /tmp/initTool. « *Ni les systèmes de stockage Storwize ni les données stockées sur ces systèmes ne sont infectés par ce code malveillant* », ajoute toutefois IBM. Pas plus que les supports USB utilisés pour la gestion des clés de chiffrement, qui sont également livrés avec l'équipement Storwize.

Bien qu'il s'agisse ici d'un accident, cet épisode permet de mettre l'accent sur les dangers des clefs USB, fréquemment utilisées comme vecteurs de logiciels malveillants. En 2016, un chercheur en sécurité, Elie Bursztein, montrait que la moitié des 297 clefs « abandonnées » dans des lieux variés sur un campus universitaire étaient par la suite raccordées à un PC par un utilisateur imprudent.

A lire aussi :

9 modems 3G/4G USB sur 10 sont très mal sécurisés

Une attaque via BadUSB publiée pour forcer les constructeurs à réagir