L’antivirus Webroot classe les fichiers Windows comme des malwares

Sortie de route pour Webroot : les utilisateurs se sont en effet aperçus d’un comportement bizarre de leur antivirus. Suite à une mise à jour des signatures de malwares, le logiciel a identifié plusieurs fichiers systèmes clé de Windows comme étant des programmes malveillants. Les premiers échos de ce comportement étrange ont eu lieu sur Twitter où des utilisateurs écrivaient que Webroot classait des fichiers Windows en tant que W32.Trojan.Gen. Suite à cette identification, l’antivirus plaçait les fichiers systèmes en quarantaine avant, in fine, de bloquer complètement l’OS.

D’autres messages ont indiqué que les effets néfastes de la mise à jour de Webroot ne s’arrêtaient pas aux fichiers Windows, mais qu’elle interdisait aussi l’accès à des sites web tels que Bloomberg et Facebook en les cataloguant comme des sites de phishing.

Et la Berezina va même plus loin. S’il est difficile de recenser le nombre de personnes touchées, le problème touche non seulement le grand public, mais également les éditions commerciales et diffusées par des prestataires aux entreprises et organisations. Des salariés ont twitté à propos des désagréments au sein de leur société. Ainsi, un utilisateur explique qu’une centaine de fichiers ont été mis en quarantaine dont ceux servant à Windows Insider Preview ou des logiciels de suivi de rendez-vous et de gestion d’équipements.

Pas de piratage et système D

En mode pompier, un porte-parole de l’éditeur a fait une déclaration sur le forum de support de Webroot pour préciser que les équipes travaillent pour résoudre le problème. Afin de rassurer les utilisateurs, il explique : « *Webroot n’a pas été piraté et il n’y aucun risque pour les clients* ». Et d’ajouter : « *les vrais fichiers malveillants sont identifiés et bloqués normalement. Une solution a déjà été trouvée pour résoudre le problème de Facebook, elle est en cours de déploiement auprès des clients* ».

Ces derniers n’ont pas attendu les conseils de Webroot et proposent leurs propres solutions. Un client propose de supprimer Webroot, de restaurer les fichiers depuis une sauvegarde, puis de réinstaller l’antivirus. Avec cette méthode, « *les fichiers n’ont pas été à nouveau mis en quarantaine* », assure-t-il. Un autre est plus radical et s’arrête à la première étape, c’est-à-dire l’exclusion pure et simple de Webroot.

A lire aussi :

Pour la Free Software Foundation, Windows… est un malware

DoubleAgent détourne les antivirus pour pirater les PC Windows

Photo credit: portalgda via VisualHunt / CC BY-NC-SA