Microsoft supprime Tor à distance pour bloquer un botnet

Jusqu'où peut-on aller pour assurer la sécurité des citoyens ? *« Ceux qui sacrifient la liberté pour la sécurité ne méritent ni l'un ni l'autre »*, avait résumé Benjamin Franklin. Cette question trouve aujourd'hui un nouvel écho dans le monde de l'informatique avec une **opération menée par Microsoft** « dans l'intérêt des utilisateurs », mais qui – dans la pratique – lui a probablement fait franchir la ligne rouge.

La firme a en effet décidé de **retirer à distance le système d'anonymisation Tor** de certaines machines, afin de bloquer le botnet Sefnit, explique *The Daily Dot*. L'opération est réalisée automatiquement **via les outils de sécurité de l'éditeur** (Security Essentials, Windows Defender, Safety Scanner, System Center Endpoint Protection et Malicious Removal Tool).

Prise de conscience

Sefnit se compose d'un malware installé sur le PC de l'utilisateur, qui 'calcule' des bitcoins pour le compte de deux pirates, lesquels récupèrent les informations via Tor, le client Tor étant installé sur les PC infectés.

Dans le but de casser ce réseau, Microsoft a retiré à distance le malware des deux pirates, mais également le client Tor. La firme s'est expliquée par la suite sur son geste : la version de Tor utilisée était trop ancienne et sujette à de nombreuses failles critiques de sécurité. *« Tor est une bonne application utilisée pour anonymiser le trafic et ne pose en général pas de problème »*, admet Geoff McDonald de Microsoft.

Le souci dans cette affaire est que les utilisateurs ont découvert que la firme de Redmond avait **le pouvoir de retirer des logiciels à distance** à travers ses outils de sécurité. Certains risquent de ne pas apprécier.

Crédit photo : © rvlsoft – Shutterstock

Voir aussi
Quiz Silicon.fr – Crimes et châtiments sur Internet