

Windows Update serait-il un espion ?

Le site d'un magazine informatique Allemand publie une analyse détaillée du comportement de Windows Update, l'outil de mise à jour de Microsoft. Les techniciens affirment avoir déchiffré ce qu'envoie Windows à Microsoft lors de chaque mise à jour. Toute la configuration du PC y passerait. Mais l'information reste à confirmer : l'article est en partie payant, et les preuves présentées gratuitement sont partielles. Coup de bluff ou révélation ? A vous de juger !

Lorsqu'il se connecte chez l'éditeur, l'outil de mise à jour automatique de Windows est censé ne collecter que quelques informations destinées à identifier la version du système d'exploitation et des composants qu'il met à jour. Mais selon le site TecChannel, Windows Update serait en réalité beaucoup plus bavard : en plus des informations strictement nécessaires à la mise à jour, l'outil ferait remonter à Microsoft une version très détaillée de la configuration du PC, incluant potentiellement la liste de tous les logiciels installés, ceux des autres éditeurs inclus.

Difficile à priori de savoir exactement ce qu'il en est, puisque à chaque connexion au serveur de mise à jour, le trafic est chiffré grâce à un tunnel SSL.

C'est là que TecChannel entre en jeu, en affirmant avoir déchiffré ce trafic à l'aide de TecDump, un sniffer maison modifié pour intercepter les appels à des API de Windows (HttpOpenRequest() et InternetWriteFile()). Cela permet à TecDump d'intercepter ce que Windows Update envoie via Internet avant que ce ne soit chiffré.

Source et Suite chez notre partenaire Futura-Sciences

Par

Publié sur Cafeduweb - Archives le samedi 8 mars 2003

Consultable en ligne : <http://archives.cafeduweb.com/lire/2847-windows-update-serait-il-espion.html>