Superfish : Lenovo reconnaît avoir préinstallé un logiciel espion

Lenovo a admis cette semaine avoir préinstallé un **logiciel espion** dans certains de ses PC portables. Ce programme compromet les échanges sécurisés SSL et les certificats associés. Le premier fabricant mondial de PC a, dans un premier temps, minimisé l'affaire, avant de réviser sa communication. Le risque est très élevé selon les experts en sécurité informatique, qui ont révélé la faille.

Superfish installe son propre certificat racine

Depuis plusieurs mois, des utilisateurs de **notebooks Lenovo** sous Windows (hors ThinkPad) se plaignent de la présence d'un programme publicitaire ou *adware* d'un partenaire du groupe chinois : la société **Superfish** de Palo Alto, Californie. L'adware surveille le trafic web de l'utilisateur et injecte des recommandations produits dans les résultats de recherche. Et ce y compris lorsque la connexion web utilise le protocole de sécurisation **SSL** (Secure Sockets Layer). Pour ce faire, Superfish installe son propre certificat racine dans le **gestionnaire de certificats de Windows**, puis agit comme un proxy, et signe à nouveau tous les certificats présentés par des sites **HTTPS** en utilisant le sien. Ainsi, les navigateurs web font confiance à tous les certificats détournés par Superfish.

Or, en plus des désagréments qu'il cause aux utilisateurs, ce système est vulnérable. Au moins sur certaines configurations. Robert Graham, CTO de Errata Security, est ainsi parvenu à extraire le certificat du adware Superfish et a craqué la clé privée associée (« komodia »). Superfish rend les PC Lenovo sur lesquels il est installé vulnérables aux **attaques de l'homme du milieu** (« man-in-the-middle »). Et expose les systèmes au vol d'identifiants et à celui d'autres données personnelles.

PC vendus entre septembre 2014 et février 2015

Après que l'ampleur du problème a été révélée, la division américaine de l'industriel chinois a finalement réagi jeudi 19 février. *« Nous sommes désolés, nous avons déraillé, nous le reconnaissons. Nous veillerons à ce que cela ne se reproduise plus jamais »*, a déclaré sur Twitter Lenovo US, qui propose un guide de désinstallation de Superfish.

Pour tenter de conserver la confiance du marché, Lenovo a également publié un communiqué et une alerte de sécurité. Des notebooks des **séries E, Flex, G, M, S, U, Y, Yoga et Z** vendus entre septembre 2014 et février 2015 sont concernés. Lenovo assure avoir mis un terme à la préinstallation de Superfisfh il y a quelques jours et avoir coupé, en janvier, les connexions serveurs qui permettent son exécution. Le groupe étudie désormais les moyens d'automatiser la procédure de désinstallation, avec Superfish et d'autres partenaires tels que Microsoft et McAfee. En attendant, il revient aux utilisateurs de vérifier si leur PC portable Lenovo est concerné et, si c'est le cas, de désinstaller le programme Superfish et le certificat racine. [MàJ: Lenovo a publié un autre CP au soir du 20/02/2015].

Lire aussi :
Les certificats SSL contrefaits étudiés à la loupe
Résultats Lenovo : intégration réussie d'IBM et de Motorola

crédit photo © Maksim Kabakou – Shutterstock