Lenovo attaqué en représailles de Superfish ?

Il était environ 22 heures ce mercredi à Paris quand les premiers symptômes sont apparus sur le site commercial de **Lenovo** : au lieu de présenter les dernières nouveautés au catalogue du groupe high-tech chinois, la page d'accueil montrait un diaporama d'adolescents visiblement révoltés face à leur webcam, avec en guide de fond sonore la chanson « Breaking Free », issue du film *High School Musical* et que l'on peut traduire par « Se Libérer ».

Un quart d'heure plus tard, la situation était revenue à la normale, excepté quelque problèmes de rendu HTML et la chanson qui tournait toujours en fond. Il a fallu une dizaine de minutes supplémentaires pour que le cache soit totalement purgé, d'après *The Verge*. Le site a toutefois été inaccessible à plusieurs reprises au cours de la nuit, officiellement pour cause de maintenance, constate ITespresso.

D'après Lenovo, **l'attaque portait sur le système DNS**, qui fait notamment le lien entre les adresses IP des serveurs et les noms de domaines. CloudFlare (fournisseur de services de diffusion de contenus) a confirmé ces observations : les pirates sont parvenus à transférer le nom de domaine *lenovo.com* pour qu'il pointe vers un serveur contrôlé par leurs soins. Ils n'ont vraisemblablement pas infiltré le réseau interne de leur victime, ce qui exclurait tout vol de données.

Le collectif Lizard Squad a revendiqué les méfaits sur son compte Twitter, en publiant notamment une citation tirée de High School Musical : « *On se libère ! On s'envole, il n'y a pas d'étoile qu'on ne puisse atteindre au firmament !* »

Un autre indice confirmant l'implication probable de Lizard Squad dans cette affaire se trouvait au sein du code source de la page d'accueil piratée. Y étaient mentionnés les noms de Ryan King et Rory Andrew Godfrey, publiquement identifiés comme membres de Lizard Squad (voir la contribution de Krebs On Security à ce sujet).

Revendication contre Superfish

Lizard Squad a également posté une capture d'écran d'un e-mail entre employés de Lenovo. Il y est question d'un ordinateur Yoga II 11,6 pouces qui ne redémarre plus après avoir retiré Superfish, ce logiciel publicitaire qui a causé un tollé la semaine passée, poussant Lenovo a faire son mea culpa.

Surveillant le trafic Web pour faire remonter des recommandations produits, Superfish est gênant de par sa nature même… mais il expose surtout les machines sur lesquelles il est installé à des attaques de type « Man-in-the-Middle »… et donc au vol de données personnelles. Un constat qui a visiblement déplu à Lizard Squad.

Ce collectif de hackers s'était déjà distingué en participant à des attaques par déni de service distribué (DDoS) qui ont mis hors service les écosystèmes en ligne liés aux consoles de jeux Sony PlayStation et Microsoft Xbox. Il a plus récemment (fin janvier) laissé suggérer de son implication

dans la panne mondiale rencontrée par Facebook. Le réseau social a finalement démenti toute attaque, imputant les dysfonctionnements à « un changement de configuration qui [avait] mal tourné ».

A lire aussi :

Superfish : Lenovo reconnaît avoir préinstallé un logiciel espion

Sécurité : 12 autres logiciels sur la trace de Superfish

crédit photo @ GlebStock – Shutterstock