Tous les périphériques USB sont des pirates en puissance

Dans la longue liste des interventions de la Black Hat qui se déroulent en ce moment à Las Vegas, on retiendra la **session de Karsten Nohl et Jakob Lell**, chercheurs en sécurité pour SR Labs. Elle porte sur la sécurité des périphériques USB et sur la démonstration d'un malware baptisé **BadUSB**.

Les deux chercheurs partent du postulat qu'aucun périphérique USB n'est à l'abri d'un malware. Le cas le plus courant est bien évidemment **la clé USB**. Les spécialistes en charge des tests de pénétration utilisent souvent cette méthode lors d'audit de sécurité dans les entreprises. En général, la plupart des gens pensent que le scan d'un antivirus ou un formatage de la clé suffit pour se débarrasser d'un virus ou d'un logiciel malveillant. Les chercheurs ont démontré que le risque était plus profond en s'attaquant au noyau des périphériques USB.

Les deux consultants ont montré plusieurs prototypes de malwares qui mettent en évidence les faiblesses des terminaux USB. Parmi eux, on trouve BadUSB qui a la particularité d'être **implanté directement dans le firmware**. Il peut donc rester caché pendant longtemps, même après la suppression des fichiers par les utilisateurs. Les chercheurs expliquent à nos confrères de Wired qu'il est très difficile de corriger ce problème : « *avec cette méthode, c'est la façon dont l'USB est conçu qui est touchée. Dès lors, vous devez considérer un périphérique USB comme infecté s'il a touché un ordinateur que vous ne connaissez pas* ».

De la rétro-ingénierie sur le firmware

Pour leurs travaux, les deux chercheurs ont utilisé **le reverse engineering des firmwares**. Ces derniers gèrent notamment les fonctions de communications intégrées dans les contrôleurs des périphériques USB. L'idée est donc de reprogrammer ce firmware pour y placer des éléments malveillants, sans éveiller les soupçons des utilisateurs. Si la clé USB est l'exemple le plus frappant, Karsten Nohl et Jakob Lell précisent que leur malware fonctionne avec **des claviers, des souris, des smartphones** qui se connectent au port USB d'un PC. A travers BadUSB, ils ont pu réaliser certaines attaques comme activer un clavier et taper des commandes. Ils ont également détourné du trafic Internet, modifié les paramètres DNS, etc. La liste n'est pas exhaustive, mais elle montre les risques potentiels. Pour eux, le seul remède est de considérer les périphériques USB comme **des seringues à usage unique**.

Un professeur de l'Université de Pennsylvanie, Matt Blaze, interrogé par le site Wired, constate que « *la démonstration montre que la menace entre l'USB et le PC va dans les deux sens et qu'un périphérique USB compromis est un problème pratique très important* ». Il va même plus loin en supposant que ce type d'attaque est déjà employé par la **NSA**. Il pointe une méthode baptisée **Cottonmouth** découvert dans les documents d'Edward Snowden, qui cachait des malwares dans les périphériques USB. « *Il n'y a pas de détails concernant cette méthode, mais je ne serais pas étonné si les travaux de Karsten Nohl et Jakob Lell faisaient partie du catalogue de la NSA* », conclut l'universitaire.

A lire aussi :

Les distributeurs de billets piratés à l’aide d’une simple clé USB

USB 3.1 : débit doublé et spécifications finalisées