

Les doutes émis sur la sécurité de l'USB sont infondés

par Fred Dart, CEO, FTDI Chip

Récemment, la publication de travaux effectués par Karsten Nohl et Jakob Lell de SRLabs, a fait couler beaucoup d'encre. Ces travaux tentaient de démontrer comment certains périphériques USB étaient susceptibles de permettre l'introduction de malware dans des systèmes informatiques ou des appareils électroniques portables. Certains ont pu en déduire qu'il n'existait aucun moyen valable pour se protéger de ce type de vulnérabilité. Les commentaires provocateurs, pour ne pas dire alarmistes, selon lesquels l'USB serait "intrinsèquement faillible" et selon lesquels les utilisateurs d'ordinateurs ou d'appareils portables devraient perdre toute confiance dès après avoir branché une clé USB, ne sont cependant pas réalistes. Une mise au point s'impose donc.

Les deux chercheurs, basés à Berlin, ont démontré que des clés USB apparemment complètement effacées, ayant été formatées et analysées à l'aide d'un antivirus, pouvaient malgré tout contenir du code malveillant non détecté. Celui-ci pourrait être caché au sein du firmware (micrologiciel) du CI d'interface.

Sur la base de ces résultats, ils ont déduit que cela sonnait la mort des clés USB ainsi que de nombreux accessoires USB, et que certaines entreprises pourraient même en venir à "interdire l'utilisation de toute clé USB". Il a même été suggéré que, en dépit de son écrasante prédominance (avec plus de 6 milliards de ports USB en fonction dans le monde), les résultats de ces recherches signifiaient fondamentalement la fin de l'USB pour le transfert de données. Ceci est tout à fait exagéré, et pour tout dire complètement injustifié. En réalité, l'USB n'est pas plus en risque face aux attaques malveillantes, que les autres vecteurs de transfert de données, qu'il s'agisse des communications sans fil (Bluetooth/Wi-Fi) ou des connexions Internet.

Même si les recherches effectuées chez SRLabs mettent en évidence un danger accru du fait du développement des cyber-attaques dans la société moderne, cela ne signifie pas pour autant que les jours de l'USB soient comptés. Il convient en effet de préciser que la sensibilité du firmware aux manipulations malveillantes, tient en général aux produits à base de microcontrôleurs, dont le firmware peut être modifié en cours d'utilisation pour exécuter des tâches à l'insu de l'utilisateur. Même si cela reste applicable à certains CI d'interface USB du marché, les fabricants de périphériques USB optant pour l'utilisation de circuits interface de meilleure qualité peuvent s'affranchir de cette menace.

Les chercheurs de SRLabs sont même allés jusqu'à affirmer "qu'il n'existe aucune parade contre les attaques USB", mais ceci est très loin d'être exact. Certains grands fabricants de semiconducteurs adressant le marché USB disposent déjà d'une technologie éprouvée pour combattre ce type de problème.

Les CI passerelle USB proposés par FTDI Chip sont de classe "intégrateur", et pas de classe "clé mémoire" (mémoire de masse). Cette classe de dispositifs ne peut être personnalisée afin d'apparaître sous forme de périphérique alternatif. Dans la mesure où ces CI sont câblés (ils s'appuient sur des ASIC dont la fonction est figée), ils ne renferment aucun micrologiciel. Par conséquent il est absolument impossible d'implanter un code malveillant à l'intérieur. Le contrôle des communications est exclusivement assuré par matériel. Certains CI de l'offre FTDI Chip disposent d'une petite mémoire EEPROM, mais uniquement pour y stocker des paramètres ; cette mémoire est beaucoup trop petite pour permettre l'installation d'un malware. En vertu de ce qui précède, les CI passerelle USB de FTDI Chip ne peuvent être reprogrammés pour faire autre chose que ce pour quoi ils ont été initialement conçus, ce qui élimine donc toute possibilité d'effraction. Ces CI de classe "intégrateur", nécessitent un driver/API FTDI spécifique pour accéder à leur contenu.

Il existe donc à l'heure actuelle des CI USB à architecture matérielle, plutôt qu'à base de microcontrôleur, qui sont impossibles à reprogrammer. Le fait même que les recherches mentionnées plus haut omettent de mentionner comment des CI de ce type permettent à l'industrie de surmonter les problèmes évoqués, suggère que tout ceci est davantage motivé par un désir d'auto-promotion, que par la volonté d'agir dans l'intérêt général.

Il n'est pas si rare bien sûr, que des acteurs de la sécurité informatique fassent du battage sur ce genre de sujet... le plus souvent motivés par un secret désir de servir leurs propres intérêts. Il y a toujours eu une tendance à tenir des propos exagérés (et en général mal informés) dans le but de convaincre les gens d'investir dans de nouveaux logiciels ou autres. Le problème est que le recours à des tactiques alarmistes peut souvent aboutir à des réactions disproportionnées.