Une attaque via BadUSB publiée pour forcer les constructeurs à réagir

A l'occasion de la conférence BlackHat à Las Vegas, des chercheurs en sécurité avaient étonné en présentant un malware nommé BadUSB et qui avait la particularité de rendre tous les périphériques USB en pirate. Ce malware 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 intervenants ont souligné que leur POC 'preuve de faisabilité) pouvait viser **des claviers, des souris, des smartphones** qui se connectent au port USB d'un PC. Très difficile à corriger, ils estimaient que le seul remède est de considérer les périphériques USB comme **des seringues à usage unique**.

A l'époque leur découverte est restée secrète, avec l'espoir que les constructeurs travaillent sur cette vulnérabilité. Or, deux autres chercheurs viennent de sauter le pas en présentant sur une page GitHub le code d'une attaque expérimentale s'appuyant sur le malware BadUSB. **Adam Caudill et Brandon Wilson** assument cette transparence en expliquant à nos confrères de Wired que « *notre démarche a largement été guidée par le fait que SRLabs (société où travaille les deux chercheurs qui ont découvert BadUSB) ne voulait pas publier son matériel* ». Et d'ajouter : « *Si vous arrivez à démontrer qu'il y a une faille alors vous devez mettre à disposition des éléments pour que les gens puissent s'en protéger.* » L'objectif de cette publication est aussi de **forcer les constructeurs à réagir** et à renforcer la sécurité de l'USB. Aujourd'hui, aucun correctif n'a été apporté à ce problème, souligne les deux chercheurs.

Une transparence maîtrisée

Sur son site, **Adam Caudill** donne quelques détails sur le POC réalisé à partir du malware BadUSB. Une première action permet de créer une seconde partition cachée pour voir les données qui ont été masquées dans la première partition. Par ailleurs, une autre manipulation modifie le mécanisme de protection du mot de passe. Il précise dans son explication que certains éléments n'ont pas été publiés comme le mécanisme d'auto-réplication du code. Il se défend d'avoir publié du code malicieux, car *« il n'y a pas de modification de données ou d'infection d'un ordinateur* ».

Avant la publication des deux chercheurs, le monde de la sécurité n'a pas eu connaissance d'attaques utilisant BadUSB circulant dans la nature. Ce début de transparence va peut-être modifier les choses avec **la possibilité développement de kit d'attaques** s'appuyant sur les périphériques USB. A moins que les constructeurs et les organisations en charge de l'USB prennent rapidement des mesures pour corriger les failles dans les firmwares.

A lire aussi :

Quiz Silicon.fr – L'USB en 10 questions
Le connecteur USB réversible entre en production, les adaptateurs aussi