Bénéficiez d'une bonne protection contre BadUSB

pour vos clés USB IronKey.

Les clés USB sécurisées IronKey™ et DataTraveler® ne sont pas sensibles au logiciel malveillant BadUSB, révélé à l'occasion de la conférence The Black Hat qui a eu lieu en août 2016. BadUSB est le premier logiciel malveillant ciblant les clés USB conçu pour attaquer la clé en elle-même, plutôt que les données se trouvant sur celle-ci. Le leadership d'IronKey dans le domaine de la sécurité, notamment son utilisation de signatures numériques dans tous les micrologiciels du contrôleur, protège ses produits contre cette nouvelle menace.

Comme l'a révélé la conférence Black Hat, l'attaque du logiciel malveillant BadUSB modifie le micrologiciel contrôlant le comportement de la clé USB, ce qui lui permet d'héberger cette menace et de potentiellement contaminer, par la suite, d'autres ordinateurs et clés USB. Les solutions anti-logiciel malveillant actuelles sont dans l'incapacité de détecter les micrologiciels modifiés du contrôleur. Et, dans un grand nombre de cas, la menace peut rester indétectable.

Comme l'ont expliqué les chercheurs, la meilleure protection contre cette menace est d'utiliser un système de signature du code pour les mises à jour du micrologiciel. Si le micrologiciel doté d'une signature est modifié, la clé n'est pas en mesure d'authentifier le micrologiciel et ne fonctionne pas. Cela empêche la propagation de la menace, mais rend la clé inutilisable. C'est pour cette raison qu'en plus d'utiliser des micrologiciels avec signature, IronKey protège le mécanisme de mise à jour des micrologiciels à l'aide de clés de sécurité matérielles. Ceci empêche la violation des micrologiciels dotés d'une signature, qui rendrait, à son tour, la clé inutilisable.

FONCTIONNALITÉS PRINCIPALES SUPPLÉMENTAIRES

Fonctionnalités principales supplémentaires liées à la sécurité Disponible pour les clés USB sécurisées IronKey et DataTraveler :

- Chiffrement matériel du disque entier AES 256 bits sécurisé et de qualité militaire
- Validation FIPS (Federal Information Processing Standards) 140-2 de niveau 3
- Gestion centralisée prenant en charge l'effacement / la désactivation à distance des clés perdues ou volées
- Authentification multifactorielle
- Stratégies de protection par mot de passe intégrées
- Boîtier métallique résistant et étanche conçu pour résister aux piratages physiques et une grande inviolabilité
- Protection antivirus / logiciel malveillant

IRONKEY™