Nhận được sự bảo vệ khỏi BadUSB từ USB Flash IronKey.

USB bảo mật IronKey™ và DataTraveler® không gặp phải nguy cơ từ mã độc BadUSB được công bố tại hội nghị Black Hat tổ chức vào tháng 8 năm 2016. BadUSB là mã độc USB đầu tiên được thiết kế để tấn công bản thân thiết bị thay vì tấn công dữ liệu trên thiết bị. Việc IronKey đi đầu trong lĩnh vực bảo mật, bao gồm việc sử dụng chữ ký số trong mọi firmware điều khiển, khiến các sản phẩm của mình trở nên miễn nhiễm trước nguy cơ mới này.

Như đã công bố tại hội nghị Black Hat về BadUSB, phương thức tấn công này thay đổi firmware điều khiển hành vi của phần cứng USB, biến thiết bị USB thành thiết bị chủ mà sau đó có thể lây nhiễm sang các máy tính và thiết bị USB khác. Firmware điều khiển bị sửa đổi không được các giải pháp chống mã độc hiện nay phát hiện ra, và trong nhiều trường hợp vẫn tiếp tục không bị phát hiện.

Như các nhà nghiên cứu đã giải thích, cách bảo vệ tốt nhất trước nguy cơ này là sử dụng chữ ký số cho các bản cập nhật firmware. Nếu firmware đã ký bị sửa đổi, thiết bị không thể xác thực được firmware và do đó sẽ không hoạt động. Điều này ngăn chặn sự lây lan của mã độc nhưng kết quả là một thiết bị không sử dụng được. Đó là lý do tại sao ngoài việc sử dụng firmware đã được ký, IronKey còn bảo vệ cơ chế được sử dụng để cập nhật firmware với các khóa bảo mật dựa trên phần cứng. Điều này ngăn chặn việc can thiệp vào firmware đã ký làm cho thiết bị không thể sử dụng được.

NHỮNG TÍNH NĂNG BỔ SUNG CHÍNH

Những tính năng bảo mật bổ sung chính Sẵn có cho USB bảo mật IronKey và DataTraveler:

- Mã hóa phần cứng AES 256 bit cấp quân sự, an toàn trên toàn bộ ổ đĩa
- Xác thực FIPS (Tiêu chuẩn xử lý thông tin liên bang) 140-2 Cấp 3
- Quản lý tập trung hỗ trợ xóa/vô hiệu từ xa các thiết bị thất lạc hoặc mất cắp
- Xác thực nhiều yếu tố
- Các chính sách bảo vệ mật khẩu tích hợp sẵn
- Vỏ kim loại chống va đập, chống nước để ngăn chặn xâm nhập vật lý
- Bảo vệ chống virus/phần mềm độc hại

IRONKEY™

 In tại Hoa Kỳ MKF-743VN

Kingston TECHNOLOGY