

IronKey USB 플래시 드라이브로부터 BadUSB 보호를 받아보십시오.

IronKey™ 및 DataTraveler® Secure USB 장치는 2016년 8월에 개최한 블랙햇 회의(The Black Hat conference)에서 발견된 BadUSB이라는 악성 프로그램에 대항할 수 있습니다. BadUSB는 장치에 있는 데이터를 공격하는 대신 장치 자체를 공격하도록 설계된 최초의 USB 악성 프로그램입니다. 모든 컨트롤러 펌웨어 내 디지털 서명 사용 등 보안 분야에서 IronKey의 리더십은 새로운 위협으로부터 제품이 면역이 되게 해줍니다.

블랙햇 세션에서 BadUSB에 대해 알려진 내용에 의하면, 공격이 USB 하드웨어 동작을 제어하는 펌웨어 방식을 변화시켜 다른 컴퓨터 및 USB 장치를 감염시킬 수 있는 호스트가 되도록 USB 장치를 변경시킵니다. 이렇게 변경된 컨트롤러 펌웨어는 오늘날 악성 프로그램 차단 방법으로는 감지되지 않으며, 대부분 발견되지 않은 채 남아있을 수 있습니다.

연구원들의 설명에 의하면, 이러한 취약성에 대항하기 위한 최고의 보호 방법은 펌웨어 업데이트용 코드 서명을 사용하는 것입니다. 서명한 펌웨어가 변경되면, 장치는 펌웨어를 인증할 수 없게 되며 작동하지 않게 됩니다. 이를 통해 확산 감염을 방지할 수 있으나, 이는 장치 사용을 불가능하게 만듭니다. 따라서, 서명한 펌웨어를 사용함과 동시에, IronKey는 하드웨어 기반 보안 키와 함께 펌웨어 업데이트에 사용하는 매커니즘을 보호해줍니다. 이는 서명된 펌웨어를 손상시켜, 결과적으로 장치를 사용 불가능하게 만드는 것을 방지해줍니다.

추가 핵심 기능

추가 핵심 보안 기능 IronKey 및 DataTraveler Secure USB 드라이브에서 사용 가능:

- 보안, 군사 등급 256비트 AES 전체 디스크 하드웨어 암호화
- 연방 정보 처리 표준(FIPS) 140-2 Level 3 검증
- 중앙집중식 관리 분실 또는 도난 장치의 원격 삭제/사용 불가 지원
- 다요소 인증
- 내장 암호 보호 정책
- 견고하고 방수가 되는 금속 케이스로 물리적 침입에 대한 내구성 강화 변조 방지
- 바이러스/악성 프로그램 보호

