利用 IronKey USB 闪存盘

防范 BadUSB

IronKey™ 和 DataTraveler® 加密 USB 闪存盘不易受到 BadUSB 恶意软件的影响。BadUSB 是在 2014 年 8 月举办的黑帽大会上揭露的，为首个旨在攻击设备本身而非设备中数据的 USB 恶意软件。IronKey 是安全领域的领头羊，在所有控制器固件中使用数字签名，使得其产品不受这种新威胁的影响。

正如关于 BadUSB 的黑帽会议所揭露的，此攻击更改用于控制 USB 硬件行为的固件，从而让 USB 设备变成主机，并最终可能感染其他计算机和 USB 设备。修改后的控制器固件无法被当今的防恶意软件解决方案检测到，在许多情况下可能还是无法被检测到。

正如研究人员阐释的，此漏洞的最佳防范举措是为固件更新使用代码签名。如果签名的固件被修改，设备将无法对固件进行身份认证，并且不会运行。这将阻止感染扩展，但会导致设备不可用。正因为如此，除了使用签名的固件，IronKey 还利用基于硬件的安全密钥保护用于更新固件的机制。这将阻止签名的固件被篡改，篡改会导致设备无法使用。

其他主要特性

其他主要安全特性（适用于 IronKey 和 DataTraveler 加密 USB 闪存盘）：

- 安全的军用级 256 位 AES 全磁盘硬件加密
- FIPS（联邦信息处理标准）140-2 Level 3 认证
- 集中管理 支持远程擦除/禁用丢失或被盗的设备
- 多因素身份认证
- 内置密码保护策略
- 坚固、防水的金属外壳，可阻止物理性入侵，抗外观破坏
- 病毒/恶意软件防范

IRONKEY™

Kingston TECHNOLOGY