Obtenha proteção contra BadUSB
com os pendrives IronKey.

IronKey™ e pendrives seguros DataTraveler® não são vulneráveis ao malware BadUSB, conforme revelado na conferência The Black Hat realizada em agosto de 2016. BadUSB é o primeiro malware criado para atacar o dispositivo em si, em vez de atacar os dados no dispositivo. A liderança da IronKey em segurança, incluindo seu uso de assinaturas digitais em todo firmware do controlador, torna seus produtos imunes à esta nova ameaça.

Conforme revelado na sessão Black Hat sobre o BadUSB, o ataque altera o firmware que controla o comportamento do hardware USB, permitindo que o pendrive torne-se um host que pode subsequentemente infectar outros computadores e dispositivos USB. O firmware do controlador modificado não pode ser detectado pelas soluções atuais anti-malware .

Conforme explicado pelos pesquisadores, a melhor proteção contra esta vulnerabilidade é usar assinatura de código para atualizações de firmware. Se o firmware assinado for modificado, o dispositivo não poderá autenticar o firmware e simplesmente não irá operar. Isso evita que a infecção se espalhe, mas resulta em um dispositivo inutilizado. Por essa razão é que, além de usar firmware assinado, a IronKey protege o mecanismo usado para atualizar o firmware com chaves de segurança baseadas em hardware. Isso evita a adulteração do firmware assinado, o que deixaria o dispositivo inutilizado.

OUTRAS CARACTERÍSTICAS IMPORTANTES

Recursos de segurança adicionais Disponíveis para pendrives seguros IronKey e DataTraveler:

- Seguro, grau militar 256 bits AES criptografia total de disco baseada em hardware
- Validação FIPS (Federal Information Processing Standards) 140-2 Nível 3
- Gerenciamento centralizado suportando limpeza/desativação remota de dispositivos perdidos ou roubados
- Autenticação multifator
- Políticas de proteção de senha incorporadas
- Reforçado, estrutura de metal à prova d'água para resistir a ataques físicos inviolável
- Proteção contra vírus/malware

IRONKEY™