

November 24, 2008

IronKey Press Release

The media has recently reported incidents involving the spread of the W32.SillyFDC worm, a low-risk piece of malware that sometimes infects PCs and networks via USB flash drives. The IronKey secure USB flash drive—which was developed in part with support from the U.S. Department of Homeland Security (DHS)—was designed from the outset with an array of defenses against malware and crimeware. First and foremost, the same hardware-based approach that makes IronKey encryption the world's most secure also makes an IronKey drive a trusted platform for mobile data. In fact, because authentication is performed in hardware using unique digital certificates, an IronKey flash drive is more secure than a typical personal computer. This emphasis on trust even extends to the manufacturing process: all IronKey drives are manufactured and provisioned in secure U.S. facilities.

To further ensure that our enterprise and government customers are protected against the latest threats, IronKey has announced a new Anti-Malware Initiative, which is detailed in the press release below. For more information go to <https://learn.ironkey.com/docs/whitepapers/ironkey-nonsecure-usb-perils-wp.pdf>

IRONKEY ANNOUNCES COMPREHENSIVE ANTI-MALWARE INITIATIVE FOR USB REMOVABLE MEDIA AND FLASH DRIVES

Anti-Virus and Remote Protection Updates Keep IronKey Devices Protected Against Latest Threats

LOS ALTOS, Calif., Nov. 24, 2008 - IronKey, maker of the world's most secure flash drive, today announced a comprehensive initiative to protect portable and mobile media from viruses, worms, trojans, botnets, crimeware and other malware threats. Enterprises and government agencies have been under attack from targeted malicious software (malware) that is attempting to penetrate protected networks by bringing malware and crimeware into these networks. It installs malicious code into USB removable media when used on personal computers at home and while traveling, and then spreads into corporate and government networks when the device is used on those networks. With over 120 million USB flash drives purchased every year, this problem is significant and is growing exponentially as cyber criminals expand their activities.

IronKey devices are intelligent, secure storage devices with strong, two-factor authentication and on-board security co-processors. As security processor costs become more affordable, it is possible to embed increasingly sophisticated layers of protection inside portable devices to protect enterprise and government networks from media-borne malware and crimeware. This enables IronKey

secure storage devices to provide the highest levels of anti-virus and anti-malware support in hardware. Hardware support for anti-malware provides an unbeatable layer of protection for mobile devices to prevent malware from spreading onto enterprise networks. The IronKey Anti-Malware Initiative Includes the Following:

Always-on hardware encryption. IronKey USB flash drives encrypt all stored data with military grade AES CBC mode encryption without installing software or drivers. Malware cannot circumvent or disable the encryption of sensitive stored data, making this a safe repository for storing confidential information, intellectual property and protected personal information.

Malware-protected software and firmware updates. IronKey devices can be updated remotely via a secure update service. All firmware and software is validated by industry leading 2048-bit RSA digital signatures, preventing the installation of malicious software or firmware onto IronKey devices.

Secure manufacturing processes. Unlike many computer hardware products that are manufactured in offshore, uncontrolled factory environments, all IronKey devices are designed and manufactured in the USA, which dramatically reduces that risk of hostile factories implanting malware onto silicon or memory chips during the manufacturing process.

Secure provisioning and quality assurance processes. IronKey devices will not function without secure and digitally signed and verified firmware and software. These software and firmware images are developed, security scanned, anti-malware scanned, and digitally signed at IronKey premises in the USA. All IronKey devices are inoperable until they are loaded with verified and scanned software and firmware from IronKey headquarters. This provides a security validation that is unmatched in the industry, ensuring that IronKey devices have not been tampered with in the manufacturing or supply chain process.

Real-time anti-malware scanning. IronKey is integrating best-of-breed anti-malware scanning technology to prevent malware from untrusted computers from infecting IronKey secure storage devices, and then spreading into corporate and government networks. IronKey has numerous patent-pending technology innovations that leverage the power of the on-board crypto processor to enable anti-malware protection in the hardware on the IronKey device to protect data and networks without requiring the installation and operation of software or drivers on host computers.

Top-tier US based ASIC security processor design team. IronKey's continued innovation in the areas of intelligent security processors on very small form-factor portable storage devices, particularly USB flash drives or memory sticks, allows IronKey to deliver the world's most secure flash drive with intelligent on board anti-malware and anti-crimeware technology. IronKey has a

top-tier ASIC security processor design team that develops the world's most secure, intelligent security processors for secure storage and authentication. The integration of intelligent security processors into standard USB flash drive formats provides affordable, easy to use, and effective protection against data loss, data leakage, and malware for enterprise and government customers.

IronKey Enterprise remotely managed devices provide revolutionary security capabilities at an affordable price. IronKey devices are available to enterprises and government agencies starting at \$79 for 1GB of secure, protected storage. When plugged into a computer with network access, IronKey devices receive automatic updates to applications, malware protection, authentication tokens and security policies. IronKey also protects against malware being transferred to the device, and malware cannot disable the device's hardware-based security features.

IronKey understands the requirements of highly-secure networks. IronKey's initial research was partially funded by the Department of Homeland Security's (DHS) Science and Technology Directorate. The IronKey secure USB devices can withstand both simple and sophisticated attacks and all IronKey products have been FIPS 140-2 Level 2 validated.

IronKey Enterprise solutions can be centrally managed so their use is governed and managed by an organization's access-control and security policy that allows only trusted and privileged users to access the device. Once authorized, the IronKey device will fully integrate with the host malware and virus inspection software from best-of-breed vendors including McAfee, Symantec, Checkpoint, Kaspersky, NOD32, Trend, Microsoft and other various anti-malware solutions.

About IronKey

IronKey products and services bring the power of authentication, encryption, identity management and privacy to consumers and businesses around the world. We blend world-class security expertise with product design that emphasizes usability, simplicity, and accessibility. All IronKey products are FIPS 140-2 Level 2 validated. The IronKey Team consists of experts in consumer devices, information security, privacy and secure banking technologies, with prior executive roles at Apple, Arcot Systems, Earthlink, Entrust, First Data Corp, GeoTrust, PayPal, RedCannon, RSA Security, Teros, Tumbleweed, Valicert, and VISA.

Founded in 2005, IronKey is privately held and based in Los Altos, CA. For more information, visit: www.ironkey.com.