

# Portable Panic

## The Evolution of USB Insecurity

As USB devices have evolved into useful storage media, they've also turned into a security nightmare for organizations. The usage of USB devices should be encouraged and embraced today in our tightening economy to aid in the reduction of operating costs. Take control of the removable media threat, control the flow of inbound and outbound data from your endpoints and enable managed use of these productivity tools by enforcing removable device usage policies.

## Overview

After nearly 15 years of development, USB storage devices come in just about every conceivable shape and size, from 1 gigabyte (GB) thumb drives fashioned as sushi rolls to standard external drives with capacities up to 6 terabytes (TB). Once a mere novelty peripheral, these devices are now as common as the mouse and keyboard. Analysts say by 2010 the market will have shipped 2.8 billion USB-enabled devices.

Unfortunately, even as USB devices have evolved into useful storage media, they've also turned into a security nightmare for organizations. The development of USB technology has always been about ease of use, connectivity, low cost and performance – with little if any thought to security. It is not only corporate users who enjoy the benefits of today's USB devices. Cyber-criminals and data thieves are increasingly using removable media to introduce malware and steal information from computers. One only need read the news regularly to see that USB devices are involved time and time again in today's highest profile data breaches, either through the loading of breach-causing malware into the backend corporate network, by facilitating intentional covert removal of copied data, or simply by enabling data loss through the misplacement of an unencrypted device.

## Historical Perspective

Didn't we forget something? When engineers first started working on the Universal Serial Bus (USB) format in 1994, their goal was to develop a single, power-efficient standard that could replace the growing number of peripheral connections that cluttered the back of our PCs. Security was the farthest thing from their minds—back then it was hardly on the minds of most IT pros.

From the establishment of the USB 1.0 standard to the roll-out of iPods and thumb drives and through the development of mega-storage devices, innovation has always been about speed, capacity and convenience. With the most recent release of the USB 3.0 standard, we're now seeing data transfer rates at a blazing 5 Gbit/s, more than 10 times faster than the previous iteration. At the same time, USB flash drives will soon hit 128 GB and external drives have ballooned to 6 TB. This has meant great things for the business world, which hails these devices as incredible productivity boosters.

But as we approach the roll out of the first USB 3.0-enabled devices, all of those gains may well be negated by the fact that even as times have changed in regard to security, the USB standard has not. Security is still as neglected as the day USB was first conceived.

File Type	Typical Size (KB)	Typical Number of Filers per:		
		512MB USB Drive	2GB USB Drive	32GB USB Drive
Text / Email	15	34,560	139,500	1,984,700
Document	100	5,185	20,920	297,750
Spreadsheet	1485	350	1,410	20,050
10 MegaPixel JPG	2250	230	930	13,210

Table 1. Storage Capacity for USB Devices

## Portable Panic - The Evolution of USB Insecurity

- 1994 — Development towards USB standards begins.
- 1995 — The USB Implementers Forum (USB-IF) is formed and quickly followed by the development of the first USB Silicon by Intel.
- 1996 — The initial USB 1.0 standard (Low-Speed) is released, with a specified data rate of 1.5 Mbit/s (187.5 kB/s).
- 1997 — More than 500 USB-related products in development.
- 1998 — The Apple iMac becomes the first publicly released computer that replaces traditional peripheral connections with USB ports exclusively. The USB 1.1 standard (Full-Speed) is released; it is the earliest revision to be widely-adopted, rated at 12 Mbit/s (1.5 MB/s) which is more than 10X faster than serial communications.
- 2000 — Storage meets USB connectivity – the first USB flash drive, manufactured by Singapore-based “Trek” and sold through IBM, is released with a capacity of 8 MB – 5X the storage capacity of a floppy disk at the time. The USB 2.0 standard (Hi-Speed) is released and gains considerable traction with a broad range of PC equipment vendors. The speed of USB devices grows to 480 Mbit/s (60 MB/s) – a 40X increase over the established USB 1.1 standard.
- 2001 — The Apple iPod, featuring FireWire 400 connectivity, is released with 5 GB of storage.
- 2003 — Apple adopts the use of USB technology for syncing and later offers full operational connectivity using either FireWire or USB.
- 2005 — Apple transitions to the USB standard and only uses FireWire connectivity for charging. An estimated 1.5 billion USB-enabled devices have been shipped.
- 2006 — U3 develops a method of auto-launching applications from USB flash drives, allowing the creation of portable work environments. Users can now work with applications such as a web browsers on the U3-enabled device; all traditional information (such as customizations, settings, browser history, etc.) is stored with the application on the USB device, eliminating all traces of application use from the PC. U3 technology also makes creating an auto-executing program or bootable USB device a trivial matter.
- 2008 — The USB 3.0 (SuperSpeed) standard is released, with data transfer rates greater than 10X that of USB 2.0. The performance of USB 3.0 is 5 Gbit/s (625 MB/s) and capacity of USB flash drives will soon hit 128 GB. At the same time, the capacity of commercially available “hard drives” offering USB connectivity has grown to 6 TB.

### Surveying the Risks

Simply put, the ease of use, the prevalence of the format and the inherent insecurity of USB make it a dream for most crooks and mischief makers. Let's examine three of the top risks, and some of the hacker tools and techniques that factor into these risks.

#### Malware Propagation

Security companies are reporting an increase in malware that propagates via USB devices and other removable media. In fact, it was just such a worm outbreak that led the US Army to ban the use of USB devices in late-2008. Malware, such as the SillyFDC worm that plagued the Army, copy themselves to all drives connected to infected machines. Any USB device connected to an infected machine would then become infected and later when it is connected to yet another machine, that machine too also begins infecting other USB devices plugged into it. This "worm like" malware propagation method copies itself to all available drives, shares, removable media and peer-to-peer software application file folders. The most popular methods currently in use are:

» **Simple file copy method**

Relies on social engineering to entice the user to click on an application icon to launch the application which then copies itself to all available drives.

» **AutoRun.inf modification method**

Modifies or creates an AutoRun.inf file on all available drives, shares and removable

media. When an infected USB drive is later inserted into another computer, the malicious software automatically executes with no user intervention.

#### Data Loss

The widespread use of USB devices within an organization can open it up to data loss on two major fronts: data stolen by copying onto a device, and data stolen by copying from a device.

In the former case, Pod-Slurp was one of the first programs to highlight the insecurity issues of USB devices. Simply plugging a USB device loaded with Slurp into a victim's computer would automatically start the scripts copying each and every document from the host PC's `My Documents` directory on to the USB stick. One could modify the script to target spreadsheets, PowerPoint files or any specific filetype of one's choice. Further, it could easily be modified to send files via email or FTP instead of copying them to the USB device.

As for the second scenario, this can be particularly dangerous if a user has innocently loaded sensitive material onto a USB drive and decides to use it on public, unsecured computers, such as systems at airport business centers, Kinko's locations, hotels and libraries.

In a 2005 demonstration at a closed security conference, the author demonstrated a program he wrote called "USB-Puke" that simply silently created a "dd" image (bit-bit copy) of any USB drive

that was inserted into the author's laptop. The use of "dd" allowed the author to not only capture copies of all existing files on the users USB drive but to also recover unallocated space containing previously deleted files on the users USB key that remained as remnants on the drive's unallocated space. The demonstration was eye-opening to attendees and was seen as a good tool for raising awareness. However, because of abuse considerations the author never released program publicly. Since then, innumerable other tools have cropped up in the wild with similar attributes and even more advanced features.

For example, HTTP RAT automatically opens a back channel over HTTP to the Public Internet that allows a remote person to simply connect to a compromised PC via Firefox. The remote user can then browse through all connected or available network drives to pick and choose which files to steal remotely over the HTTP connection. And USB Switch Blade extracts all password hashes using `pwdump` from the target machine for later use in password cracking. Simply walk up to the victim's machine, plug in the USB device for only 60 seconds or less, and walk away with all password hashes. Other variations include the ability to also grab browser history for later mining of user financial site credentials, MSN messenger user credentials and more.

### Anonymous Hacking

An extremely useful feature of USB drives is their ability to act as a "PC on a stick" through the use of certain platform and virtualization utilities such as BartPE/PeToUSB, UBCD4, UNetBootin and MojoPac. It also makes it possible for malicious users to replicate their entire Windows hacking lab with a USB device and run it on virtually any PC with an available USB port. When the malicious user is done, she simply removes the USB device and leaves without a trace.

Similarly, terrorist organizations have adopted the use of encrypted communications software on a USB stick. A terrorist can anonymously walk into any cybercafé, plug in a USB device containing software such as Mujahedeen Secrets 2, send email, files or have chat communications using military-grade encryption, and then simply unplug the device – leaving no trace of its use on the cybercafé PC.

## Not Just USB: Other Removable Media Risks

While this paper focuses on USB devices, it needs to be understood that they are just the tip of the iceberg. The majority of the risks contained within this article is not simply limited to the USB standard, but extend to all forms of removable media in use today including CD, DVD and Blu-ray drives as well as FireWire and eSATA connected devices.

### CD, DVD and Blu-ray removable media

Many of today's popular CD-based network penetration testing tools that are used by individuals with good intent can unfortunately also be used by an unauthorized malicious person with bad intent. Examples include placing undetectable malware deep within the network, installing Trojans or key loggers, and creating network backdoors to allow unauthorized persons a direct path through network defenses to the compromised PC. Simply put, you are putting yourself at great risk when you do not control specifically **who** can run **what** applications from your removable media drives. It is hard to imagine any good could come from allowing uncontrolled use of a CD/DVD drive when an unauthorized party runs a disc with something like one of the Astalavista Toolkits on it.

It is not only a matter of a CD, DVD or Blu-ray drive being used as a launching point for a network penetration. The sheer volume of information that can be removed from a network onto removable media through unauthorized copying is increasing. Many are unaware of how much information can quickly be copied to removable media and the unauthorized person simply walks out the door with it; table 2 provides some insight along these lines.

### FireWire Connectivity: an Even Greater Threat?

FireWire threats deserve a mention in this article, as the potential threat may in some ways actually be greater than that posed by USB devices. An example would be the ability to write directly to memory via FireWire, as shown by New Zealand security researcher Adam Boileau of security-assessment.com at Ruxcon in 2006.

In March of 2008, he publicly released a tool that allows you to take over any Windows PC by simply connecting a Linux-based PC to the Windows PC FireWire port and running a single command. The command literally overwrites the password protection code within Windows memory, then completely bypasses it. A detailed explanation of how the attack works can be found here: [www.pcadvisor.co.uk](http://www.pcadvisor.co.uk).

File Type	Typical Size (KB)	Typical Number of Filers per:		
		CD Disc	DVD Disc (SS SL)	Blu-ray Disc (DL)
Text / Email	15	46,500	297,000	3,200,000
Document	100	6,980	44,500	480,000
Spreadsheet	1485	470	3,000	32,320
10 MegaPixel JPG	2250	310	1,975	21,300

Table 2. Storage Capacity for CD, DVD and Blu-ray Discs

### Reaping Productivity Gains without the Risks

The traditional definition of a corporate “endpoint” is clearly evolving. For millions of employees, portable mass media represents the next generation of endpoints, shifting from simply PCs and laptops. Because of this evolution, enterprise endpoint security must also grow to address the increasing concerns. Ultimately, this shifting corporate endpoint exposes a new threat vector that IT professionals must confront and secure.

Using epoxy on your USB ports to enforce the ultimate denial of their use is not the answer. Clearly the productivity gains brought by the many USB devices available today outweigh any knee-jerk reaction to explicitly and permanently ban USB devices usage. In fact, the use of USB devices should be encouraged and embraced, especially in today’s economic environment, to help reduce operating costs and perhaps even save some jobs.

To win the war against mobile malware and information theft, organizations must develop clear, in-depth policies regarding the use of removable devices and media within the organization. They must also deploy proactive solutions, such as the Lumension Endpoint Security Suite™, formerly Sanctuary Suite, to support these policies. While the enterprise security war will continue to be long and trying, enterprises can gain a decisive advantage by taking an offensive approach to protecting their organizational endpoints, no matter how much they evolve. After all, the notion of a “PC on a stick” should benefit business processes, not impede them.

### Lumension Endpoint Security Suite™

Lumension Endpoint Security Suite™, formerly Sanctuary Suite, secures endpoints from data theft and loss, unsanctioned devices and applications, and malware threats without relying on reactive signature lists.

By employing a whitelist approach, Lumension enables only authorized applications to run and only authorized devices to connect to a network, laptop or PC – facilitating security and systems management, while providing necessary flexibility to the organization.

### Taking Control of the Removable Media Threat

Lumension Endpoint Security Suite enforces usage policies for removable devices (such as USB flash drives) and other removable media (such as CDs / DVDs) to control the flow of inbound and outbound data from your endpoints.

Applications and removable devices are validated as they are used within the enterprise. Applications or devices that are not authorized are simply not allowed to execute.

Through a central console, application and device control policies are quickly established and enforced through two simple steps: identification and assignment. Lumension Endpoint Security Suite enables organizations to develop granular use poli-

cies – working with the devices and applications rather than simply enabling or disabling them. Policies are managed per user or user group as well as per computer. For devices, policies are enforced by file type, daily volumes, time of day, and many more criteria. Linking application and device policies to user and user-group information stored in Microsoft® Windows® Active Directory™ or Novell® eDirectory™, Lumension enables the immediate association of user groups to devices and applications on the fly – dramatically simplifying the management of endpoint application and device resources.

The Lumension Endpoint Security Suite can also encrypt removable media so that it can be safely used and transported without the fear of exposing confidential data to unauthorized users. Users can access their encrypted data even on computers that do not have client software installed. Centralized and decentralized encryption schemas provide the administrator with the flexibility to centrally encrypt removable media or enable users to encrypt removable media on their own and, more importantly, enforce the use of that encrypted media.

Providing the ultimate flexibility, Lumension enables administrators to allow trusted users to authorize their own applications. This option provides the best of both worlds – flexibility to users and control for administrators through notifications of activity. Auditing and reporting enable administrators to precisely track when devices and applications are used, by whom and how. They can also see attempts to use un-authorized devices or applications and track that as well.

Lumension combines the proven capabilities of its application and device control solutions, providing organizations with the most comprehensive solution for endpoint security management – all from one console. Lumension Endpoint Security Suite removes the risk of data leakage, malware and spyware, improves IT security and network bandwidth, reduces the effort and cost associated with supporting endpoint technologies, and assures regulatory compliance. The solution provides the following:

- » Prevents data leakage via removable media, malware or spyware
- » Protects against malware, viruses and spyware
- » Safeguards against zero-day threats
- » Controls proliferation of unwanted applications and devices
- » Assures and proves compliance with regulations governing privacy and accountability
- » Maximizes benefits of new technologies and minimizes risk

## About Lumension

Lumension™, Inc., a global leader in operational endpoint security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets.

Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year.

Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, India, Hong Kong and Singapore. Lumension: IT Secured. Success Optimized. More information can be found at [www.preventia.co.uk](http://www.preventia.co.uk)

