

Malware Protection for USB Drives

By Hema Krishnamurthy – ISSA member, Phoenix, USA Chapter

Connect

Malware infection through USB drives, which could result in viruses/worms spreading through and bringing down entire enterprise networks, is a growing concern among private enterprises and government entities.

Abstract

USB drives¹ are commonly used at the workplace because they offer a convenient means of data transfer and storage. However, this convenience is accompanied by security threats that may result in the spread of malware and the loss of valuable data from the drives. Encryption and authentication mechanisms can be used to ensure that confidential data cannot be retrieved in the event the media is compromised. However, malware infection through USB drives, which could result in viruses/worms spreading through and bringing down entire enterprise networks, is a growing concern among private enterprises and government entities.

Computers and networks in households, enterprises, and government agencies are being plagued by viruses, worms, and Trojans that have spread via malware-infected USB drives. Although some security concerns with USB drives (like data loss in the event of media compromise) can be addressed through encryption/authentication mechanisms, malware infections through these drives have opened up a new can of “worms.” Employees and consumers, unaware of the infection, store and in turn transfer the infected data files and the included malware to other computers, releasing the malicious content to the network. USB storage devices may also serve as channels of viral infection if they contain malicious autorun.inf-type files that cause the operating system to automatically execute programs when the device is inserted. This operating system “feature” increases the potential of malware infection in IT systems.

USB drives were banned by the U.S. Department of Defense late last year when a virus called “Agent.btz” infected major segments of the military network after copying itself to USB thumb drives.² While other government agencies and corporations have policies to ban or restrict the use of USB drives, this leads to a loss in productivity, convenience, and business agility. After all, the utility of a “safe” USB drive is about pro-

ductivity and transferring/storing information quickly and conveniently. Hence, in addition to encryption and authentication of data on the drives, measures must be put in place to prevent malware infections. The ban on USB drives that began late last year in the Defense Department is purported to be lifted, but under the condition that the procured drives come equipped with adequate measures to prevent malware infections.

Malware and USB drives

In 2008, according to data gathered by McAfee Avert Labs,³ there had been an explosive growth of malware. New, unique malware has grown by over 10 million variants over the course of the year. AutoRun, a feature of Windows Explorer that enables devices to launch applications using the commands listed in the *autorun.inf* files, serves as a common means of malware infection. The number of AutoRun malware binaries on USB and flash devices has seen a steady increase since 2007. For instance, a vendor at a security conference ended up distributing AutoRun malware-laden USB sticks to attendees and had to recall them later.⁴ With this infection method, the malicious application modifies or creates an autorun.inf file on local drives and removable media that are connected to the computer. When the infected USB flash drive is inserted into another computer, the copy of the malicious application is automatically executed merely by the user physically plugging the device to the computer. The number of computers infected by AutoRun viruses has been on the rise since December 2007, with Asia being in the lead followed by North America.⁵

To meet the need for protected USB drives, many vendors are now offering secure USB drives that encrypt and authenticate the information on the drives.⁶ However, encryption and au-

1 USB devices are known by a variety of common names: flash drive, jump drive, key drive, keychain drive, memory key, pen drive, thumb drive, sticks (www.u3.com).

2 <http://www.wired.com/dangerroom/2008/11/army-bans-usb-d>.

3 http://www.mcafee.com/us/local_content/reports/6623rpt_avert_threat_0709.pdf.

4 <http://blogs.zdnet.com/security/?p=1173>.

5 http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=MAL_OTORUN1&Vsect=P.

6 Hema Krishnamurthy, “USB Storage Media – Secure Convenience?” *ISSA Journal* (December 2007) – <https://www.issa.org/Library/Journals/2007/December/Krishnamurthy-USB%20Storage%20Media-Secure%20convenience.pdf>.

thentication alone are not sufficient to protect information on USB drives. Antivirus solutions should be used in conjunction with these drives to offer a more complete security solution.

USB Security

Encryption and authentication

Data on the USB drive should be encrypted using FIPS-grade encryption algorithms like AES. Encryption prevents an attacker from intercepting and modifying data on the drives. Data integrity algorithms like SHA-2, when used in conjunction with encryption, provide the user with the assurance that the data has not been modified from the original intended value.

Disabling AutoRun/AutoPlay features

When an USB drive is plugged into an infected computer, the virus spreads to the USB drive, which then acts as a carrier of infection vectors for the systems and network into which it is subsequently plugged. As mentioned, the malware could spread automatically when the drive is plugged in if the computer's operating system has an AutoRun-type feature enabled. To mitigate this risk, an organizations security policy can dictate disabling the auto-play function of all removable devices (CDs, DVDs, etc.), and especially USB devices. With AutoRun disabled, the malware will not execute automatically, and hence, any resident malware can be removed through the use of antivirus tools. Alternatively, the drives can protect autorun.inf-type files on the drive from unauthorized changes by having the file stored in a read-only partition on the drive.

In order to mitigate malware risks posed by the AutoRun feature, Microsoft has introduced changes with Windows 7 for non-optical media: Auto-play will no longer work for USB drives. Allegedly, this change will be ported back to Windows XP and Vista.

Antivirus solutions

The escalating use of USB drives, owing to their portability and ease of use, makes them an easy target for viruses. A virus can also be embedded in what looks like a normal file on a USB device. Hence even if the AutoRun-type feature is disabled, the computer can become infected when the file is opened. This problem can be averted through USB drives with antivirus software installed – on the host or the drive itself – that can perform signature scanning for viruses each and every time there is any change to the files on the drive, thus offering on-access protection.

Although the data on the USB drive can be scanned by the conventional antivirus solution running on the host, portability of the device is reduced as traveling employees will not be able to use the drive on unprotected public computers, without risking the possibility of a malware infection. One way to prevent employees from using the drives on unpro-

tected computers would be the use of host authentication, in which the software on the drive can authenticate the host through the use of trusted host codes or pass codes. Alternatively, writes to the drive may only be permitted if the application running on the drive detects an antivirus solution running on the host. Some USB vendors also offer solutions wherein the application running on the USB installs an antivirus engine along with the supporting virus signature database files on the drive itself. However, this solution requires that the USB vendor maintains the updates and patches to the antivirus software to ensure they are up to date.

USB smart drives

Alternatively, to retain portability, on-drive antivirus solutions can be used. U3 smart drives, developed by SanDisk and M-systems, allow users to carry both applications and files on the drives. Most U3 drives come bundled with built-in password and antivirus protection. U3 files are stored on the drive in a compressed format. When the U3 application is used, the files are decompressed into a directory on the host PC and the application then runs on the PC. With U3, the applications not only can decompress but can also delete themselves, leaving no trace, thus providing an added security measure. At this time on-drive antivirus solutions are supported only on U3 drives. One problem, however, is that U3 relies on the AutoPlay feature of Windows. There is a small, read-only partition on the drive that pretends to be a CD-ROM and automatically runs the U3 launch pad. In security environments where deemed necessary, the AutoRun feature may be disabled and the launch pad executed by the user on demand in order to mitigate risks arising from Autorun malware. Typically, the on-drive antivirus solutions automatically scan the files being written to the drive. If infection is detected in a file, further transfer will be aborted and the user alerted, thus stopping the spread of malware.

Other security measures

Most of the currently available secure USB drives in the market use password controls to unlock the drive. In addition, software controls can be put in place to ensure that secure USB drives cannot be unlocked if they are not plugged into a trusted computer.

The IT departments may incorporate policies that mandate that the software and firmware on the USB drives be updated only through signed packages, thus preventing installation of malicious software. Administrators could also lock down the drives to be in a read-only mode so that data could be copied off of the device, but nothing could be copied onto it. This would allow organizations to safely distribute or exchange information on the drives but prevent any malware from ever being introduced. However, the later method is a very restrictive solution.

Challenges

Organizations could encounter some challenges in deploying USB security solutions. Virus signatures and software patches have to be kept up-to-date on the host systems and smart U3 drives. However, this cannot be done effectively to protect offline computers that are not connected to the Internet. Besides, when new viruses and other malicious attacks strike, traditional signatures are ineffective. Hence, the anti-malware solution that organizations pick should deploy measures like trusted execution and heuristics in addition to traditional pattern matching. Behavioral anti-malware solutions build databases of what constitutes “normal” behavior and the user is alerted by any “abnormal” activities or behaviors.

Some of the other concerns for organizations could be the lowered performance of the USB read/writes owing to the signature scanning occurring on the fly. This is because the files would need to be completely buffered and scanned for virus signatures before the write can go through to the drive. Furthermore, compatibility issues could arise between the USB drive’s antivirus and other antivirus software running on the PC, with potential conflicts in signature databases, etc. This situation could arise if the USB drive comes equipped with an antivirus solution and the host has another antivirus solution running on it.

The files on USB drives could have been infected when manually copied from an infected host or when a malicious application automatically copies itself onto the removable media or when acquired from untrusted sources. The drives can also be infected through inferior quality control and inadequate security measures at the manufacturing facility for U3 drives and on the PC for the regular drives.

Conclusion

Conventional secure USB drives improve security through features such as encryption/authentication of files and strong and secure password management that prevents data loss in the event of media compromise. However, secure USB drives should add another layer of security through use of antivirus solutions that reside on the drive itself.

Antivirus software completes the security feature repertoire of encrypted drives, but a simpler solution would be to avoid infection in the first place. Best practices like using USB drives only on trusted hosts, acquiring files of trusted origin, allowing access to the removable media only if any antivirus solution is running on the host and using trusted and secure manufacturing plants for USB drive manufacturing are some ways in which drive infection can be prevented.

Banning USB drives at the workplace is not a long-term solution for security concerns that accompany these devices. Use of best-of-breed USB antivirus solutions residing on encrypted drives would make these drives a safe repository for storing confidential information, while extending the security perimeter to these portable storage devices, without compromising the convenience and portability of these drives.

About the Author

Hema Krishnamurthy, CCSA, CCSE, CIS-SP, is a software architect with the Information Assurance Group of ITT Corporation in Tempe, Arizona. She has been involved in the information security field for over eight years and has a Masters in Computer Science and MBA. She is also the chair of the ISSA EAC White Papers Committee.



She can be reached at hema.krishnamurthy@issa.org.