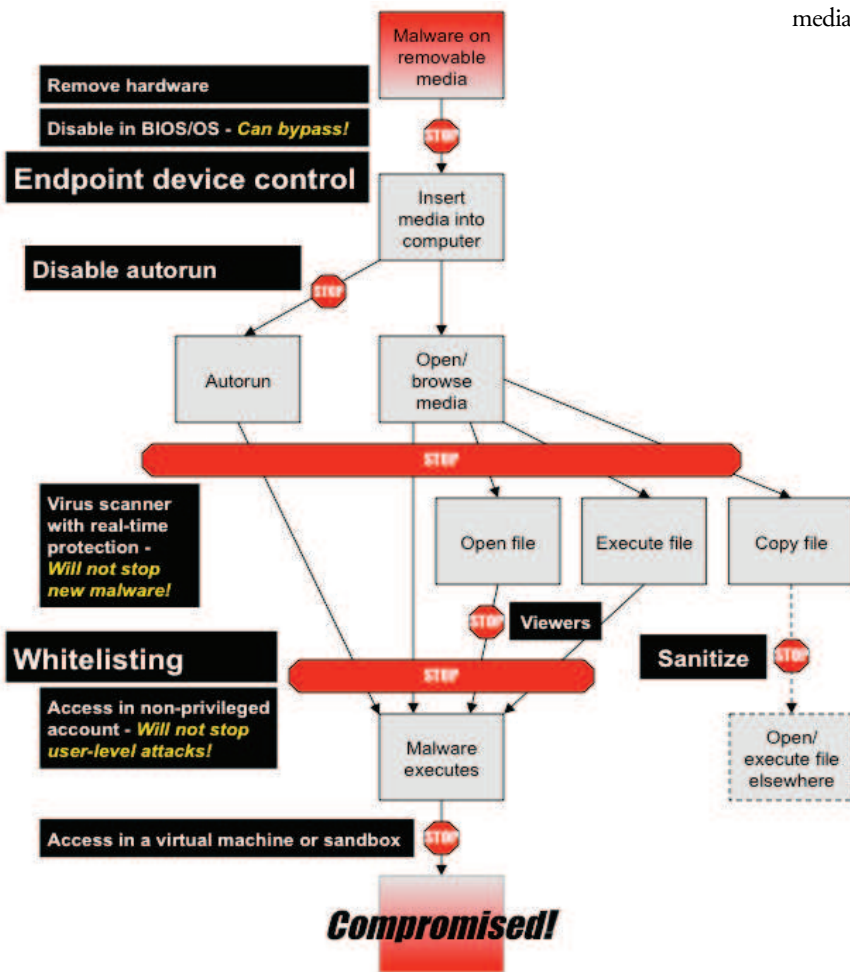


Defense against Malware on Removable Media

Bill, a government official, needs to transfer a few files from his Internet-connected machine to his work computer. He copies the files onto a USB flash drive and then plugs the drive into his work computer...

Removable media such as CDs, DVDs, floppy disks, flash memory cards, or USB drives may be used (either accidentally or intentionally) to transfer malware between computer systems. The diagram shows various tactics that can be used to defend against this threat. Implementing all of these defensive tactics is likely not possible or even desired, but several of these tactics at least should be used together for a defense-in-depth approach. In the diagram, tactics shown with larger fonts offer greater Benefit vs. Cost.



Remove hardware: Remove media hardware devices (CD/DVD and floppy drives, flash memory card slots, USB ports, etc.) from those systems that do not need them. This is the most effective way to prevent the use of removable media, but it requires physically modifying each computer. For large organizations, this may not be feasible—unless it can be done during

the procurement process, or if it is only being done for a small group of computers, such as the laptops used by traveling employees.

- A USB port lock that physically plugs into a USB port and requires a special key to remove can provide some protection against users plugging devices into those ports.
- Alternatively, disable the ports for the media hardware in the BIOS. To prevent anyone from going into setup and re-enabling the ports, set a BIOS password. Note that this is not as secure as physically removing the hardware, as there are ways to bypass or reset the BIOS password.

Disable in OS: Disable operating system support for types of removable media that are not needed.


- For information on disabling support for USB drives in Windows, Linux, Solaris, and Mac OS X, see the “Disabling USB Storage Drives” NSA Fact Sheet (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/fact_sheets.shtml).
- On Windows, IEEE 1394 (FireWire) ports, PCMCIA and SD card slots, etc. can be disabled by disabling the appropriate controllers in the Device Manager: *Control Panel* → *System* → *Hardware* → *Device Manager*. To prevent users from re-enabling these controllers, users should not be given administrator credentials; they should only be allowed to log onto their computers using non-privileged user accounts. Note that USB controllers should NOT be disabled through the Device Manager—disabling pieces of the Universal Serial Bus may cause more than just the external USB connectors to stop working!
- On Linux, disabling support for other removable media devices is done in a similar way as disabling support for USB drives (see the Fact Sheet referenced above): the appropriate kernel objects must be found and deleted. Remember to repeat this each time the kernel is patched or a new kernel is installed.

Endpoint device control: Use an endpoint device control application to automatically enforce that certain types of devices not be connected to computer systems. Your host-based protection provider may even already provide this capability. This is likely the most scalable way to prevent the use of removable media, but it can be time-consuming to manage and monitor.

- In Windows Vista and later, Group Policy can be used to do this enforcement. See <http://msdn.microsoft.com/en-us/library/bb530324.aspx>.
- Data loss prevention solutions may also do endpoint device control. As an added advantage, these solutions can also help protect against data exfiltration.



The Information Assurance Mission at NSA



Disable autorun: On Windows, malware on removable media can use the Autorun functionality to infect the computer when the media is inserted. Because of this, Windows Autorun is disabled by default for all but CD and DVD drives on Windows 7. This setting has also been pushed out via automatic updates to Windows XP, Vista, Server 2003, and Server 2008 as of February 2011; see Microsoft Knowledge Base article 971029.

- Note that some USB drives present themselves as CD drives when inserted; these will still be Autorun.
- Malware could still be transferred from CDs or DVDs. For guidance on disabling Autorun on all removable media, see Microsoft Knowledge Base article 967715 (<http://support.microsoft.com/kb/967715>).
- Note that just disabling Autorun is not guaranteed to stop malware on removable media from automatically infecting computers. For example, disabling Autorun stopped the Conficker worm, but it did not stop the Stuxnet worm.
- Autorun attacks are also possible against Linux. For file managers (such as GNOME Nautilus), disable auto-browse and thumbnailing. Those processes could have vulnerabilities which would allow malware to automatically infect the system. Also consider disabling auto-mount.

Virus scanner with real-time protection: Use a good antivirus product with real time protection (“guard” or “on-access scan”) functionality enabled. This will prevent recognized malware from being executed from the removable media or copied off of it. Be sure that the antivirus product is kept up-to-date. Monitor it to ensure that it is functioning as expected, and regularly review the logs it generates.

- Note that because virus scanners are signature-based, they very often *cannot stop* new malware that has never been seen before!

Whitelisting: Use application whitelisting on the host computer to allow only approved programs to run—any malware that does manage to get onto the host computer will then be prevented from running. This has the advantage of also protecting against new malware that has never been seen before. However, whitelisting requires some overhead to set up and maintain. The policies must be developed and tested before they can be deployed operationally. If not thoroughly tested, some users may not be able to run applications that they need to perform their jobs.

- On Windows, Software Restriction Policies (SRP) can be used to do application whitelisting. For more information, see the “Application Whitelisting Using Software Restriction Policies” NSA guide (Available at www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml). On Windows 7 and Windows Server 2008 R2, AppLocker can be used instead of SRP.
- On Linux, execution restrictions can be enforced by mounting world-writable directories (e.g., /tmp) as separate partitions with the noexec option enabled. Using a mandatory access control technology such as SELinux can prevent an application compromised by malware from doing things it should not be doing. On Mac OS X, the Parental Controls can be used to prevent unapproved applications from launching.

Access in non-privileged account: To prevent malware from installing anything at the operating system level, files on the removable media should only be accessed within a non-privileged user account—that is, not an administrator account. Although this precaution will not prevent malware from compromising the user account, it will make it more difficult for the malware to obtain high-privilege credentials.

Viewers: Use document viewers instead of the full applications to open documents from removable media. This limits functionality, but can protect against malware.

- Microsoft offers free viewers that allow viewing, printing, and copying of Office documents. These viewers do not support macros or Visual Basic for Applications (VBA), so they can protect against some forms of malware in documents. Users expect to just double-click files to open them, so to be effective, the default applications that open Office documents must be changed: go to *Control Panel* → *Folder Options* → *File Types* and change the “Opens with” application for each relevant file extension.
- In Microsoft Office 2010, documents can be opened in “Protected View”, which opens the documents as read-only in an isolated sandbox.
- Several commercial and open source PDF readers provide sandboxing capability and block embedded URLs by default, so PDF documents can be read more safely.
- In Windows Explorer, disable the option to hide file extensions for known file types: *Control Panel* → *Folder Options* → *View* → *Hide extensions for known file types*. If this option is not disabled, a malicious executable file could appear as a harmless document (e.g., malware.doc.exe would appear as malware.doc), and double-clicking on the file would run the malware.

Access in virtual machine or sandbox: Quarantine files from removable media by only transferring and using them within a virtual machine (VM) or sandbox. This can keep any malware contained, including malware inside of documents. If the VM becomes compromised, it can be reverted to a known good state and the host computer remains unaffected.

Sanitize: Before distributing files taken from removable media to other systems, sanitize the files. File cleaning applications can be used, such as FiST (File Sanitization Tool), a tool for sanitizing USB drives. Sanitization can also be done by transformation: converting the files to different formats (and then converting them back, if desired). This will probably result in loss of functionality, but any malware in the files is not likely to survive the conversion process either. Convert the files on a stand-alone conversion computer, within a VM (as described above) in order to prevent compromise of this computer. The VM should have an up-to-date virus scanner running on it, to help defend against malware hijacking the conversion process. Load the files to sanitize and either save them to different formats using *File* → *Save As*, or print them to different file formats (this may require installing special printer drivers). For example:

- Microsoft Word and Excel documents can be printed to application-independent formats such as PDF or XPS.
- Microsoft PowerPoint slides can be saved as image files.
- PDF files can be saved as PostScript or image files.