Disable Autorun to prevent computer virus infections–USB flash drives threats

Almost any PC user use intensively the USB Flash Drives called popular memory sticks to transfer data between computers or between different devices as photo cameras, portable players and the computer. Many people use such a drive to share photos or music or even games with the friends and an Flash Drive with interesting content will travel from a computer to another borrowed by its owner. The Autorun and Autoplay , a rather useless I dare to say and source of troubles Windows feature, and the portable character of the flash drives create the perfect context for malware spreading. From my experience, a lot of small companies which still run Windows XP or even Vista, has a lot of troubles with Autorun method of malware spreading.

AutoPlay make reference to what programs must be used to play different media files types stored on CD or DVD disks when inserted, asking the user to choose a program to open a certain media file when the CD or DVD is inserted, or will treat the content with the action registered for that file type recognized by the extension. For example if you insert a CD with mp3 files in Windows XP the Autoplay can present to the user a set of options about how to handle that specific media file, but if the user chosen in the past to open that files type with Windows Media Player and the "Always do the selected action" tick box was ticked, Windows will directly open the mp3 files with Media Player without questions asked. That mean the handler for mp3 files was registered in Autoplay system. Each media type can have registered a default action or handler for it.

Autorun is a technology used to automatically launch programs by reading commands from a file called **autorun.inf** stored in the *root directory* of the storage medium. This file is a plain text file thus can be created or edited with Notepad and are predominantly in Installers CD, when somebody insert a Installer CD, the setup will start automatically without user interaction.

Example of autorun.inf file content :

```
[autorun]
open= Installer_example.exe
icon = example.ico
```

Both *Installer_example.exe* and *example.ico* must be placed in the root directory of the USB flash drive or CD-DVD root .

It's obvious for everybody that a malware creator can exploit very easy this Windows feature to launch his malware when an USB stick is inserted in the computer and thus spreading the malware. There is two directions a malware can move :

- from the computer to the USB device
- or from the USB device example a simply pen drive, to the computer.

It must be said that Microsoft makes with newer Windows versions important steps in USB Storage devices security but in only one way : the control of autorun files stored on USB devices are better now.

For example in Windows versions prior to XP, the autorun file commands are executed instantly without user interaction when a new drive or content type is recognized in the system. For Windows

XP SP2 and SP3 and Windows Server 2003 SP1 and SP2 Microsoft released a security update, KB967715 that fix several problems with disable of Autorun like:

- Autorun for a network drive cannot be disabled
- The shortcut menu and double-click functionality of Autorun can not be disabled

Also to correctly disable the Autorun in Windows Vista and Windows Server 2008, the update that must be installed is KB950582.

However, in Windows XP were introduced **Autoplay** feature and for some drive types instead of direct execution of autorun.inf commands, the Autoplay will be invoked.

In **Windows Vista and Windows Server 2008,** there is no automatic execution of autorun.inf, though, beware, Autorun tasks can be executed by double clicking the USB device icon or by open the context menu with right-click and selecting Autorun. Thus, in Windows Vista the Autorun is an **option** presented to the user, without automatic execution capabilities like in earlier Windows versions, this is behaviour appearing when Autorun policy is Not configured or Disabled. With this policy Enabled, the autorun.inf instructions can be either completely disabled or automatically executed. My recommendation is to completely disable Autorun tasks.

In **Windows 7**, the Autorun tasks are restricted to CD-DVD-ROM drive types, without possibility to open Autorun, either via context menu or icon double-click. The Autorun is restricted to only display an icon and a label, the rest of instructions are ignored, so it's no more a security issue.

All these can be a little confusing, let's talk about practically virus protection. The easier is to use little programs, most of them freeware, to deal with Autorun threats, instead of playing with the *Windows registry* which is dangerous if you are not very sure what you do. I mean all the Autorun settings or Autorun policies settings are reflected and can be edited via *Windows registry* with a registry editor like *regedit.exe* .

However, let's tell you about one extreme Autorun hack, about how to disable it for *any drive type* ,CD-DVD-ROM or USB devices, by creating and adding to the registry, a registry file(text file with .reg extension) with the next content :

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\IniFileMapping\Autorun.inf]
@="@SYS:DoesNotExist"
```

Basically, these IniFileMapping method tells Windows that autorun.inf files on any drive has *no information or commands* to read from and all these type of files will be ignored. Read more about this hack at Nick Brown blog.

One of the most effective tool for preventing computer virus infection via an USB drive is **Ninja Pendisk!**. It's a freeware tool able to immunize your USB flash drive, preventing its virus infection if it's plugged into an infected computer, in this way stopping the malware spread. Also will protect your PC revealing all the malicious and hidden files from an USB thumb drive.

Another similar tool is **Autorun Protector**, which protect your PC against USB thumb drives threats or your thumb drive against viruses possibly coming from an infected computer. The software create

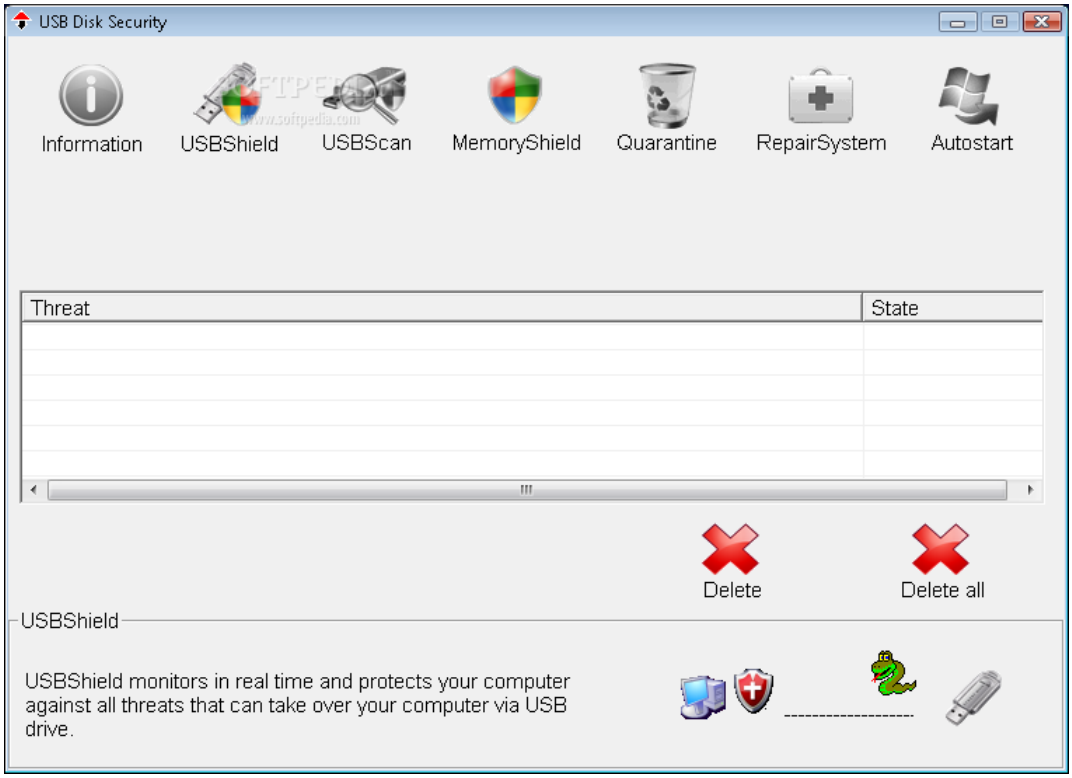
a protected autorun.inf file that can not be overwritten by a malware.

Net Studio USB FireWall will reveal the autorun.inf file content if any exists and will warn you when a program try to start from the USB drive.

Panda USB and AutoRun Vaccine, is one of the *best* and popular free utility created by Panda Security that immunize the USB flash drive creating an un-deletable and secure autorun.inf file on it. The PC can also be immunized by disabling the Autorun feature thus preventing any executable to be run automatically from an USB flash drive, CD-ROM or DVD-ROM.

Naevius USB Antivirus is a real-time protection utility that protects your PC from all kinds of malware residing on USB drives.

USB Disk Security provides 100% protection against any threats coming from the USB drive(pen drive, thumb drive, memory sticks and so on). USB Disk Security is 100% compatible with all security software and has a very small installer of approximately 1MB.



USB WriteProtector enables or disables the write protection for USB drives.

GGreat USB AntiBody(it's now discontinued !!!) is a nice free utility able to prevent or eliminate known or unknown USB viruses.

DriveSentry Desktop Free(there is also commercial versions) features :

-Antivirus, Anti-malware, Anti-spyware
-Protects desktop PC's and removable storage devices such as USB memory keys.
-FREE license for non-commercial use, easily upgradable to Security Suite

In order to assure the best virus infection prevention for your PC, the Autorun feature settings must be well-known and the best security measures applied. It's recommended that Autorun feature to be disabled on any PC to eliminate a possibly malware infection.

Share this:

- Share