

How to remove Virus from USB Drives

One of the ways by which a virus can infect your PC is through USB/Pen drives. Common viruses such as 'Ravmon', 'New Folder.exe', 'Orkut is banned' etc are spreading through USB drives. Most anti virus programs are unable to detect them and even if they do, in most cases they are unable to delete the file, only quarantine it. Here are the things which you can do if you want to remove such viruses from your USB drives.

1. Whenever you plug a USB drive in your system, a window will appear similar to the one shown below



2. Don't click on Ok , just choose 'Cancel'.
3. Open the Command Prompt by typing '**cmd**' in the run box.
4. In the command prompt type the **drive letter:** and press enter.
5. Now type **dir /w/a** and press enter.
6. This will display a list of the files in the pen drive. Check whether the following files are there or not:
 - Autorun.inf
 - Ravmon.exe
 - New Folder.exe
 - svchost.exe
 - Heap41a
 - or any other exe file which may be suspicious.
7. If any of the above files are there, then probably the USB drive is infected.
8. In command prompt type **attrib -r -a -s -h *.*** and press enter.
9. This will remove the Read Only, Archive, System and hidden file attribute from all the files.
10. Now just delete the files using the command **del filename**.
Example **del Ravmon.exe**.
Delete all the files that are suspicious.

Example:

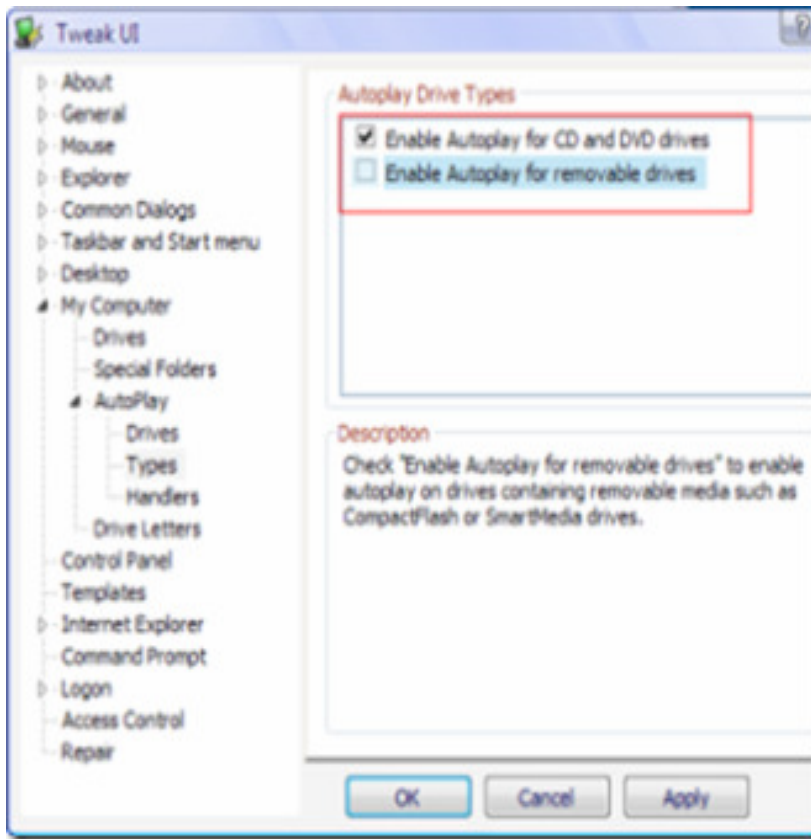
- Microsoft Windows XP [Version 5.1.2600]
- (C) Copyright 1985-2001 Microsoft Corp.

-
- L:\Documents and Settings\kayzg>o:
- O:\>
-
- O:\>dir /w/ac
- Volume in drive O is KAYZGPEKEE2
- Volume Serial Number is D834-F037
- Directory of O:\
- [untitled folder] [System]
- [Documents] winzip90.exe
- sdat5277.exe LaunchU3.exe
- ethereal-setup-0.99.0.exe ethereal 1.doc
- PROJECT NETWORK MANAGEMENT.doc About the Raila Virus 1.doc
- About the Raila Virus.doc KAYUMBO G.doc
- 9 File(s) 63,575,709 bytes
- 3 Dir(s) 547,983,360 bytes free
- O:\>
- O:\>del Autorun.inf
- Could Not Find O:\Autorun.inf
- O:\>

11. To be on a safer side, just scan the USB drive with an anti virus program to check whether it is free of virus or not.
12. Now remove the drive and plug it again. In most of the cases, the real culprit turns out to be the “**Autorun.inf**” file which mostly gets executed when someone clicks Ok in the dialog window which appears above. Thus the infections can spread

Security Tips

1. **Disable the Autoplay feature of USB drives.** If you disable the Autoplay feature of USB drives, then there are lesser chances of the virus spreading.
2. A tool which can perform such a function is [Tweak UI](#). Download it from [here](#) and install it.



3. Now you can disable the Autoplay feature of the removable drives as shown above.

4. Run the program, expand *My Computer*, *AutoPlay*, and then click *Types*. On the right panel under *AutoDrives Types* un-tick *Enable Autoplay for removable drives*.

5. By following the above steps, you can keep your USB drives clean.

Other simple ways

1. Don't loan your flash drive to anyone. If you do you're taking a risk there. Lending your flash card is not a good idea. You don't know what's on your friend's computer or what worm will work its way to your flash drive then to your computer.
2. When you insert it to your USB port run your anti virus scanner on it first. **BEFORE YOU OPEN THE DRIVE!!!!** If it is infected it will tell you.
3. Make sure you update your anti virus program first. Anytime you hook anything to your computer scan for virus before you open it.

How to quickly scan your flash drive

1. When you connect the flash drive, before open your flash drive:
 - Right click [on removable disk,]
 - scan with antivirus then you can use,
 - If you are going to copy any file from your pc, first scan the particular then only copy to your flash drive.