

# C:\recycled\Boot.com msqpdxpjbdwopb.xxx

My anti-virus software detected the following file(s) as a virus: -

- 1) C:\recycled\boot.com
- 2) C:\windows\system32\drivers\msqpdxpjbdwopb.sys  
(You might or might not see this file or something similar to this file with different extensions).

What this virus does... On my computer, when I open Internet Explorer the anti-virus software will detect one or more files, *msqpdxpjbdwopb.xxx*, as a threat although the browser stills works. Sometimes when I open a drive, it will prompt me the same threat, or might not allow you to open any drive. I really do not know what other harm this virus will do. Anti-virus software could not 100% remove this virus, you will need to clear it off manually. The important files to look out for are **boot.com**, **autorun.inf** (Located in all your drives if infected. Be careful with this file as some USB thumb drive uses this file and is a legitimate file) and the **recycled** folder. These files/folders mentioned have read only and hidden attributes, therefore some antivirus programs fail to detect this virus.

I have listed the steps here to remove **boot.com** on a Windows Vista computer; steps for other Windows versions are quite similar.

**IMPORTANT:** - Until the problem is fixed DO NOT double click any drive in My Computer, right click > 'Explore' to view it instead. Clear this virus with these instructions at your own risk.

If the following instructions do not make sense, get a PC geek/nerd dude to help you...

1. Start Windows in safe mode.
2. *autorun.inf* file and *recycled* folder are hidden so you need to enable view hidden files. Start > Computer > press Alt key > Tools > Folder Options > View tab > select "Show hidden files and folders" > OK. UNCHECK the following boxes:  
  
 Hide extensions for known file types  
 Hide protected operating system files
3. Find and delete all *autorun.inf* file and *recycled* folder on all hard disks. Use Windows Search to simplify process.

4. Clear all files in 'c:\Documents and Settings\[USER PROFILE]\Local Settings\Temp' folder AND 'c:\windows\temp' folder. (Some files may not delete, that's ok, they're in use by the system and not virus files.)
5. Start > Run > regedit > OK. Click on *Computer* in the left pane once. On the menu click Edit -> Find. Type **boot.com** and click Find Next. Every time it finds a new boot.com, delete it. Keep hitting F3 until all instances of boot.com is deleted in the entire registry. It should find a dozen or so copies.
6. Still in the Registry Editor, click on *Computer* in the left pane once. On the menu click Edit -> Find. Type **recycled** and click Find Next. Every time it finds press the delete key and then enter. Close registry editor when done.
7. Now, we have to clean the virus files on all external drives or flash drives you have used with this computer. First\*\*, disable Autoplay function. In Vista -> Start Control Panel > under 'Hardware and Sound' click on 'Play CDs or other media automatically' > uncheck 'Use AutoPlay for all media and devices' > Save. Secondly, plug in any external drives or flash drives you have used with this computer and open the drive(s) [ **remember not to double click any drive but right-click > 'Explore' to view it instead** ] to view contents. Before you do anything further, back up each autorun.inf before deleting them off external drives, because they might be important – [ autorun.inf is used for some menu loaders on flash drives so they will stop working. Instead edit the 'open=' to point to the menu exe instead of recycled\boot.com ]. Delete **autorun.inf** file and **recycled folder**.

\*\* In Windows XP & lower put in all your suspected flash drives while pressing the shift key, wait for 15 seconds then release shift and open the flash drive in My Computer using method as above.

8. Restart the computer and the problem should be gone.