Instructions for Removing Conficker

Introduction

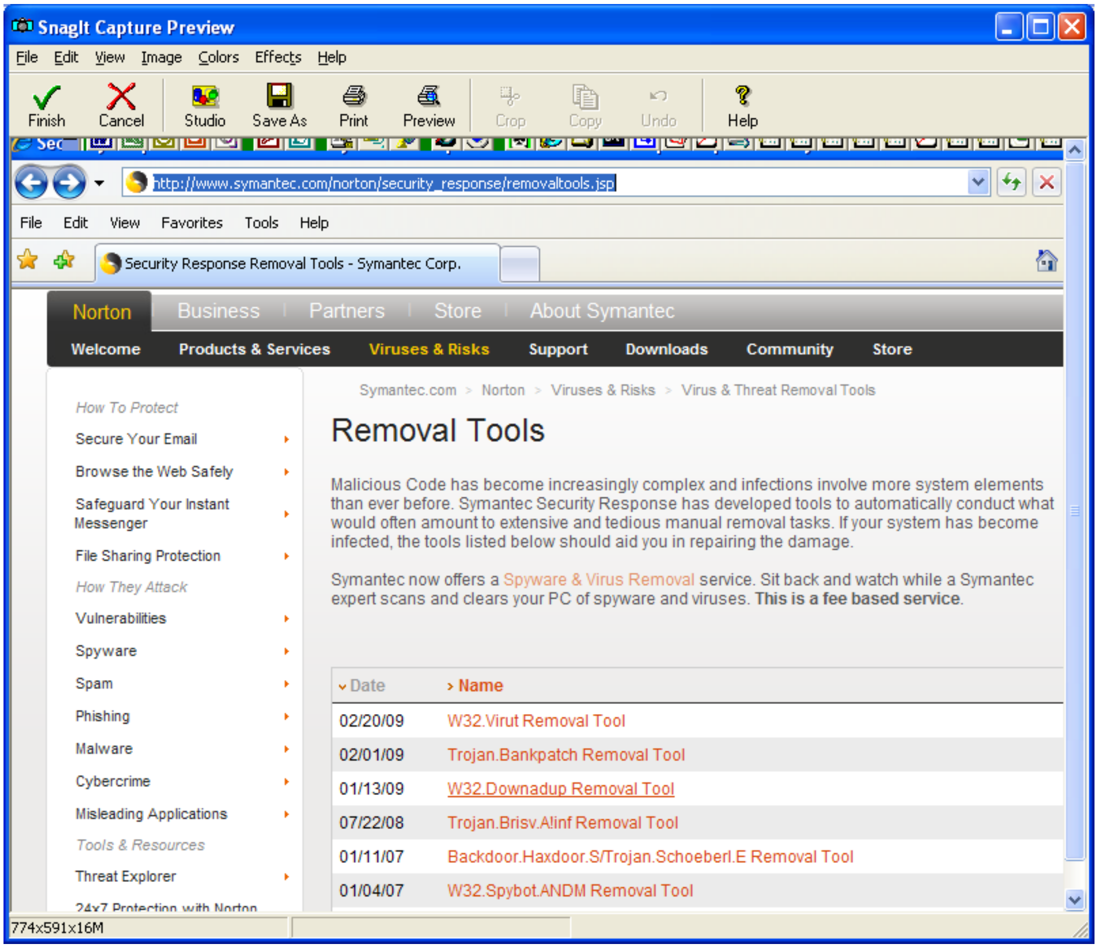
In order to remove this worm, you have to upgrade to Service Pack 3 of Windows XP, and you have to do all Steps.

DO NOT connect to a network or the Internet if you are unprotected

Step 1 – See if you have it.

Go to http://www.symantec.com/norton/security_response/removaltools.jsp

You'll see a long list of removal tools:



Symantec.com > Norton > Viruses & Risks > Virus & Threat Removal Tools

Removal Tools

Malicious Code has become increasingly complex and infections involve more system elements than ever before. Symantec Security Response has developed tools to automatically conduct what would often amount to extensive and tedious manual removal tasks. If your system has become infected, the tools listed below should aid you in repairing the damage.

Symantec now offers a Spyware & Virus Removal service. Sit back and watch while a Symantec expert scans and clears your PC of spyware and viruses. **This is a fee based service.**

Date	Name
02/20/09	W32.Virut Removal Tool
02/01/09	Trojan.Bankpatch Removal Tool
01/13/09	W32.Downadup Removal Tool
07/22/08	Trojan.Brisv.A!inf Removal Tool
01/11/07	Backdoor.Haxdoor.S/Trojan.Schoeberl.E Removal Tool
01/04/07	W32.Spybot.ANDM Removal Tool

Choose the one marked W32.Downadup Removal, and download it.

NOTE: You’ll need an administrator account to run this tool.

Step 2: Remove

IMPORTANT: Disconnect your PC from the internet (or network, if applicable), and run the tool.

Run the

If it finds anything, it will clean it; reboot and try again until the virus is removed.

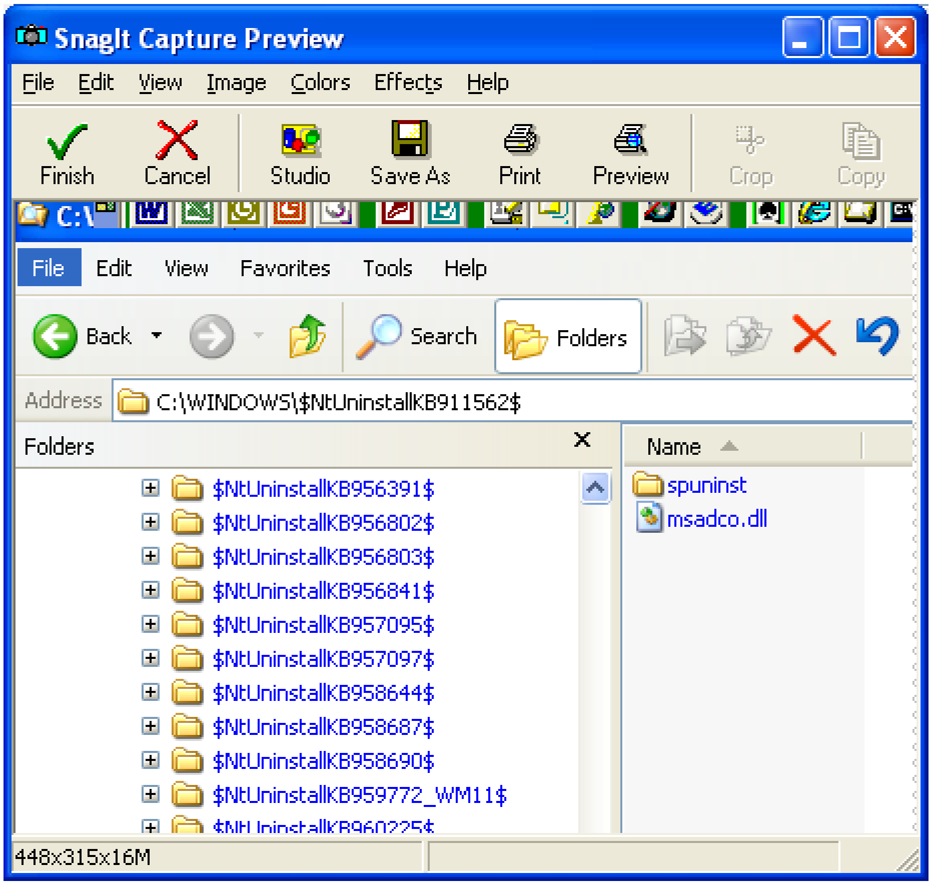
We recommend a full power off (at the wall) for at least 30 seconds on each “reboot”.

Step 3: See if you’re spreading it and stop the spread if you are.

The worm spreads through scheduling a task for its dispersal. Click the Start button, go to the Control Panel, and click on Scheduled Tasks. If you see any marked AT1, AT2, etc., delete them, and then empty the Recycle Bin. Other tasks may or may not be OK; once you’ve reconnected, you can always Google them.

Step 4: Check if you’re protected

- Open Windows Explorer
- Go to the C:\Windows folder and open it.
- You should se a list of blue folders, in number order, like the screenshot below:
- Look for $NtUninstallKB958644$. If it’s there – you’re protected



Address C:\WINDOWS\$NtUninstallKB911562$

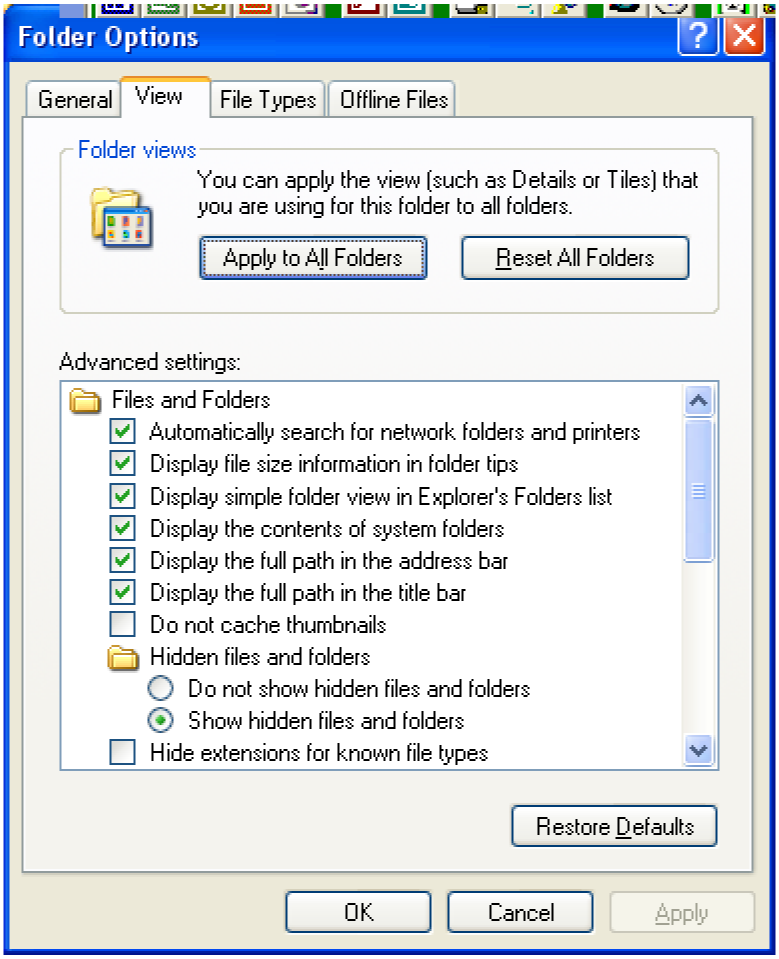
$NtUninstallKB956391$
$NtUninstallKB956802$
$NtUninstallKB956803$
$NtUninstallKB956841$
$NtUninstallKB957095$
$NtUninstallKB957097$
$NtUninstallKB958644$
$NtUninstallKB958687$
$NtUninstallKB958690$
$NtUninstallKB959772_WM11$
$NtUninstallKB960225$

spuninst
msadco.dll

448x315x16M

If you can't see the blue list, do the following:

- One the menu bar, click Tools
- Click the Folder Options menu item
- Select the View tab
- Under "Hidden Files and Folders" (you may have to open this), click "Show hidden files and folders"
- While you're at it, set "Hide extensions to know file types" of if it's on. The confusion this creates can let viruses in
- Click Apply, then Ok. The refresh may take a few seconds; if in doubt, press F5 to refresh manually



You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

Files and Folders
- ☑ Automatically search for network folders and printers
- ☑ Display file size information in folder tips
- ☑ Display simple folder view in Explorer's Folders list
- ☑ Display the contents of system folders
- ☑ Display the full path in the address bar
- ☑ Display the full path in the title bar
- ☐ Do not cache thumbnails
- Hidden files and folders
  - ○ Do not show hidden files and folders
  - ● Show hidden files and folders
- ☐ Hide extensions for known file types

Step 5: Protect yourself

- Go to www.microsoft.com and download the latest security updates.
- Go to your antivirus supplier and download their latest security updates
- Set the downloads to automatic
- Do this at least once a month – MOST INFECTIONS WILL TRY TO TURN THIS OFF