

Re: how do i remove a trojan spy virus?

## Re: how do i remove a trojan spy virus?

---

*Source:*

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help\\_and\\_support/2005-07/msg02754.htm](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2005-07/msg02754.htm)

---

- *From:* "pcbutts1" <[pcbutts1@xxxxxxxxxxx](mailto:pcbutts1@xxxxxxxxxxx)>
  - *Date:* Sun, 10 Jul 2005 06:43:42 GMT
- 

In order to remove this infection you will need to use HijackThis to manually remove the infection:

Print out these instructions as you will need to shutdown every window that is open later in the fix.

Download HijackThis <http://www.pcbutts1.com/downloads/HijackThis.zip> and save it to your C:\ folder. Extract the hijackthis.zip file to c:\hijackthis. you will use this program later.

Enter the Windows Control Panel and double-click on Add/Remove Programs.

When the installed programs list appears, double-click on the following entries if they exists and allow them to uninstall.

Security IGuard

Virtual Maid

Search Maid

PSGuard

Then exit the Add/Remove Programs screen and the Control Panel.

## Re: how do i remove a trojan spy virus?

click [HERE http://www.pcbutts1.com/downloads/Smithfraud.reg](http://www.pcbutts1.com/downloads/Smithfraud.reg) and select Save As (in Internet Explorer it's labeled Save Target As) in order to download the Smitfraud.reg file. Save this file to your desktop.

Locate the smitfraud.reg file on your desktop and double-click it. When asked if you want to merge with the registry, click the YES button. Wait for the "merged successfully" prompt then follow the rest of the instructions below.

Configure your computer so you can see all hidden files.

To enable the viewing of Hidden files follow these steps:

Close all programs so that you are at your desktop.

Double-click on the My Computer icon.

Select the Tools menu and click Folder Options.

After the new window appears select the View tab.

Put a checkmark in the checkbox labeled Display the contents of system folders.

Under the Hidden files and folders section select the radio button labeled Show hidden files and folders.

Remove the checkmark from the checkbox labeled Hide file extensions for known file types.

Press the Apply button and then the OK button.

Now your computer is configured to show all hidden files.

Download Killbox <http://www.pcbutts1.com/downloads/killbox.zip> and save it to your desktop. Extract killbox.zip to your desktop. Then double-click on the killbox.exe program.

When the program is open, select the option labeled Delete on reboot.

Do not close killbox, and open open notepad, by clicking on Start, then Run, and typing notepad.exe and pressing the OK button.

When notepad is open, copy and paste the following text into the notepad

Re: how do i remove a trojan spy virus?

## Re: how do i remove a trojan spy virus?

screen. You do this by highlighting each of the below filenames and then pressing Control–C on your keyboard. Then click on the open notepad windows and press Control–V to paste the contents into the notepad.

C:\wp.exe

C:\wp.bmp

C:\bsw.exe

C:\Windows\sites.ini

C:\Windows\popuper.exe

C:\Windows\zloader3.exe

C:\Windows\system32\wp.bmp

C:\Windows\System32\hhk.dll

C:\Windows\System32\wldr.dll

C:\Windows\System32\helper.exe

C:\Windows\System32\intmon.exe

C:\Windows\System32\shnlog.exe

C:\Windows\system32\perfci.ini

C:\Windows\System32\intmonp.exe

C:\Windows\System32\msmsgs.exe

C:\Windows\system32\msole32.exe

C:\Windows\System32\ole32vbs.exe

C:\WINDOWS\system32\oleadm.dll

C:\WINDOWS\system32\oleadm32.dll

Return to Killbox, go to the File menu and select Paste from Clipboard.

Still in Killbox, click the red–and–white Delete File button. Click Yes at the Delete on Reboot prompt. Click No at the Pending Operations prompt. If your computer does not restart automatically, restart it manually.

Re: how do i remove a trojan spy virus?

## Re: how do i remove a trojan spy virus?

While your computer is restarting, tap the F8 key continually until a menu appears. Use your up arrow key to highlight Safe Mode, then press the enter button on your keyboard.

Using Windows Explorer, delete the following files, if found, ( do NOT try to find them by "search" because they will not show up that way)

FOLDERS to delete if found:

C:\Program Files\Search Maid

C:\Program Files\Virtual Maid

C:\Windows\System32\Log Files

C:\Program Files\Security IGuard

C:\Program Files\PSGuard

While still in Safe Mode, do the following:

Make sure all programs and windows are closed. Double-click on C:\hijackthis\hijackthis.exe that you had downloaded and extracted earlier. When the program starts place a check next to each of the following entries, if found, then click FIX CHECKED button.

R1 – HKCU\Software\Microsoft\Internet Explorer\Main,Default\_Search\_URL =  
<http://www.quicknavigate.com/search.php?qq=%1>

R1 – HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =  
<http://www.quicknavigate.com/bar.html>

R1 – HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =  
<http://www.quicknavigate.com/search.php?qq=%1>

R1 – HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =  
<http://www.quicknavigate.com/search.php?qq=%1>

R1 – HKCU\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =  
<http://www.quicknavigate.com/search.php?qq=%1>

R1 – HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =

Re: how do i remove a trojan spy virus?

Re: how do i remove a trojan spy virus?

http://www.quicknavigate.com/search.php?qq=%1

R0 – HKCU\Software\Microsoft\Internet Explorer\Main,Local Page =  
http://www.quicknavigate.com/

R1 – HKCU\Software\Microsoft\Internet Explorer\Main,Default\_Page\_URL =  
about:blank

R1 – HKCU\Software\Microsoft\Internet Explorer\Main,Default\_Search\_URL =  
http://www.startsearches.net/search.php?qq=%1

R1 – HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =  
http://www.startsearches.net/bar.html

R1 – HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =  
http://www.startsearches.net/search.php?qq=%1

R1 – HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =  
http://www.startsearches.net/search.php?qq=%1

R1 – HKCU\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =  
http://www.startsearches.net/search.php?qq=%1

R1 – HKCU\Software\Microsoft\Internet Explorer\SearchURL,(Default) =  
http://www.startsearches.net/search.php?qq=%1

R0 – HKCU\Software\Microsoft\Internet Explorer\Main,Local Page =  
http://www.startsearches.net/

O2 – BHO: VMHomepage Class – {FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF} –  
C:\WINDOWS\System32\hp6DD8.tmp

O4 – HKCU\..\Run: [WindowsFY] c:\wp.exe

O4 – HKCU\..\Run: [WindowsFY] c:\bsw.exe

O4 – HKLM\..\Run: [WindowsFZ] C:\WINDOWS\ZLOADER3.EXE

O4 – HKLM\..\Run: [Security iGuard] C:\Program Files\Security  
iGuard\Security iGuard.exe

O4 – HKLM\..\Run: [PSGuard] C:\Program Files\PSGuard\PSGuard.exe

O9 – Extra button: Microsoft AntiSpyware helper –  
{D5BC2651-6A61-4542-BF7D-84D42228772C} – C:\WINDOWS\System32\wldr.dll

O9 – Extra 'Tools' menuitem: Microsoft AntiSpyware helper –  
{D5BC2651-6A61-4542-BF7D-84D42228772C} – C:\WINDOWS\System32\wldr.dll

O9 – Extra button: Microsoft AntiSpyware helper –  
{D5BC2651-6A61-4542-BF7D-84D42228772C} – C:\WINDOWS\System32\wldr.dll (HKCU)

Re: how do i remove a trojan spy virus?

Re: how do i remove a trojan spy virus?

O9 – Extra 'Tools' menuitem: Microsoft AntiSpyware helper –  
{D5BC2651–6A61–4542–BF7D–84D42228772C} – C:\WINDOWS\System32\wldr.dll (HKCU)

When it is done fixing the entries, exit the HijackThis program and restart your computer so its back into normal mode.

Download Hoster and run it <http://www.pcbutts1.com/downloads/Hoster.exe> .  
Press the Restore Original Hosts button and then press the press OK button.  
When it is done, exit the program.

Click [HERE](#) and select Save As to download DelDomains.inf to your desktop  
<http://www.pcbutts1.com/downloads/DelDomains.inf>.

Now RIGHT-CLICK on the DelDomains.inf file on your desktop and select the Install option.

This will remove all entries in the "Trusted Zone" and "Ranges" also.

Download, install, and run CleanUp  
<http://www.pcbutts1.com/downloads/CleanUp40.exe>

Update and run your antivirus software to clean up any left over traces of these infections.

Your computer should now be free of the Smitfraud / Quicknavigate / VirtualMaid infections.

Some files downloaded were created by Mike Burgess MVP and others. Thanks  
Mike

--

Re: how do i remove a trojan spy virus?

Re: how do i remove a trojan spy virus?

The best live web video on the internet <http://www.seedsv.com/webdemo.htm>  
NEW Embedded system W/Linux. We now sell DVR cards.  
See it all at <http://www.seedsv.com/products.htm>  
Sharpvision simply the best <http://www.seedsv.com>

"EE" <eisleyunay@xxxxxxxxxxxx> wrote in message  
[news:1120954662.457782.78910@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:1120954662.457782.78910@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)  
>I inadvertently downloaded spyware about a month ago and since then my  
> computer's system has been slowly deteriorating. I downloaded lavasoft  
> and adaware but they did absolutely nothing to remove the problems.  
> Recently my entire computer's screen is blue and says "A fatal error  
> has occurred...error caused by Trojan-Spy.html.smitfraud.c" I'm afraid  
> to use the internet on that computer. Can someone please tell me how I  
> can fix this?  
>

---

• **References:**

◆ [how do i remove a trojan spy virus?](#)

◇ From: EE

- Prev by Date: [Re: multimonitor problems](#)
- Next by Date: [Re: code 12 on dell inspiron 5000e laptop](#)
- Previous by thread: [Re: how do i remove a trojan spy virus?](#)
- Next by thread: [New Folder on Desktop](#)
- Index(es):
  - ◆ [Date](#)
  - ◆ [Thread](#)