

## Re: about:blank

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2005-03/0401.html>

---

**From:** Jim Byrd ([jrbyrd\\_at\\_spamlessadelphia.net](mailto:jrbyrd_at_spamlessadelphia.net))

**Date:** 03/16/05

Date: Tue, 15 Mar 2005 15:44:52 -0800

Hi Buster – about:blank (which has many variants) is one of the nastiest of the CoolWebSearch parasites to remove. Lets try the simplest approach first, then if that doesn't do it, we can go on from there. You may ultimately need to sign in at one of the available HiJackThis forums for assistance, but give this a go first:

Start here. Please post back with your results or if you need additional assistance.

First, some precautionary stuff:

#####IMPORTANT#####

Before you try to remove spyware using any of the programs below, download both a copy of LSPFIX here:

<http://www.cexx.org/lspfix.htm>

AND a copy of Winsockfix for W95, W98, and ME

<http://www.tacktech.com/pub/winsockfix/WinsockFix.zip>

Directions here: <http://www.tacktech.com/display.cfm?ttid=257>

or here for Win2k/XP <http://files.webattack.com/localdl834/WinsockxpFix.exe>

Info here: <http://www.spychecker.com/program/winsockxpfix.html>

Directions here: <http://www.iup.edu/house/resnet/wifix.shtm>

The process of removing certain malware may kill your internet connection. If this should occur, these programs, LSPFIX and WINSOCKFIX, will enable you to regain your connection.

NOTE: It is reported that in XP SP2, the Run command netsh winsock reset will fix this problem without the need for these programs. (You can also try this if you're on XP SP1. There has also been one, as yet unconfirmed, report that this also works there.) Also, one MS technician suggested the following sequence:

```
netsh int reset all
ipconfig /flushdns
```

See also: <http://windowsxp.mvps.org/winsock.htm> for additional XPSP2 info/approaches using the netsh command.

#####IMPORTANT#####

#####IMPORTANT#####

Show hidden files and run all of the following removal tools from Safe mode or a "Clean Boot" when possible. Reboot and test if the malware is fixed after using each tool.

HOW TO Enable Hidden Files

<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339>

Clean Boot – General Win2k/XP procedure, but see below for links for other OS's (This for Win2k w/msconfig – you can obtain msconfig for Win2k here: [http://www.3feetunder.com/files/win2K\\_msconfig\\_setup.exe](http://www.3feetunder.com/files/win2K_msconfig_setup.exe) ):

1. StartRun enter msconfig.
2. On the General tab, click Selective Startup, and then clear the 'Process System.ini File', 'Process Win.ini File', and 'Load Startup Items' check boxes. Leave the 'boot.ini' boxes however they are currently set.
3. In the Services tab, check the "Hide All Microsoft Services" checkbox, and then click the "Disable All" button. If you use a third party firewall then re-check (enable) it. For example, if you use Zone Alarm, re-check the True Vector Internet Monitor service (and you may also want to re-check (enable) the zlclient on the Startup tab.) Equivalent services exist for other third party firewalls. An alternative to this for XP users is to enable at this time the XP native firewall (Internet Connection Firewall – ICF). Be sure to turn it back off when you re-enable your non-MS services and Startup tab programs and restore your normal msconfig configuration after cleaning your machine.
4. Click OK and then reboot.

For additional information about how to clean boot your operating system, click the following article numbers to view the articles in the Microsoft Knowledge Base:

310353 How to Perform a Clean Boot in Windows XP

<http://support.microsoft.com/kb/310353>

281770 How to Perform Clean-Boot Troubleshooting for Windows 2000

<http://support.microsoft.com/kb/281770/EN-US/>

267288 How to Perform a Clean Boot in Windows Millennium Edition

<http://support.microsoft.com/kb/267288/EN-US/>

192926 How to Perform Clean-Boot Troubleshooting for Windows 98

<http://support.microsoft.com/kb/192926/EN-US/>

243039 How to Perform a Clean Boot in Windows 95

<http://support.microsoft.com/kb/243039/EN-US/>

#####IMPORTANT#####

Sometimes the tools below will find files which they are unable to delete because they are in use. A program called Copylock, here, <http://noeld.com/programs.asp?cat=misc#CopyLock> can aid in the process of "replacing, moving, renaming or deleting one or many files which are currently in use (e.g. system files like comctl32.dll, or virus/trojan files.)" Another is Killbox, here:

<http://www.downloads.subratam.org/KillBox.zip>

A third which is a bit different but often useful is Delete Invalid File, here: <http://www.purgeie.com/delinv.htm> which handles invalid/UNC file/folder name deleting, rather than the in use problem

Download and run Stinger.exe, here:

<http://download.nai.com/products/mcafee-avert/stinger.exe> or from the link on this page: <http://vil.nai.com/vil/stinger/> ME/XP users be sure to read: <http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.htm>

Download sysclean.com , from Trend Micro, here:

<http://www.trendmicro.com/download/dcs.asp> along with the latest pattern file, here: <http://www.trendmicro.com/download/pattern.asp> Be sure to read the "How-to" info here:

<http://www.trendmicro.com/ftp/products/tsc/readme.txt> (You might also want to get Art's updater, SYS-UP.Zip, here for future updating of these:

<http://home.epix.net/~artnpeg/>). (If you download and use the updater from the beginning, it will automatically handle downloading the other files.)

Place them in a dedicated folder after appropriate unzipping. Show hidden and system files (HowTo here:

<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2002092715262339>)

Disable Restore if you're on XP or ME (directions here:

<http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.htm>), then boot to Safe mode (HowTo here:

<http://service1.symantec.com/SUPPORT/tsgeninfo.nsf/docid/2001052409420406>)

Read tscreadme.txt carefully, then do a complete scan of your system in Safe mode and clean or delete anything it finds. Reboot to normal mode and re-run the scan again.

This scan may take a long time, as Sysclean is VERY extensive and thorough. For example, one user reported that Sysclean found 69 hits that an immediately prior Norton AV v. 11.0.2.4 run had missed.

Download and run the free or trial version of A2 Personal, here:

<http://www.emsisoft.com/en/> Run from a Clean Boot or Safe Mode with Show Hidden Files enabled as above.

Now try the "let's hope we're lucky" approach:

Courtesy of Ron Kinner, MVP:

"There is a German program called Spoonweg.exe which might help.

<http://lunatic-skydance.de/mr/soft/SpoonWeg.exe>

microsoft.public.security.virus: Re: about:blank

It will start to download. Save it somewhere you can find it again then Open it and say YES then Click on Trojaner-Suchen. If it finds the version of about:blank that it is meant to kill it will go and do it then reboot the PC. Otherwise it will say Trojaner Spooner wird nicht gefunden.

Another German program is SpHjFix.exe.

<http://www.trojaner-info.de/cgi-bin/download.cgi?file=sphjfix>

This one speaks English so just Press on Start Disinfection If it doesn't find its target it will say Not Infected across the top of the little window. Otherwise follow the instructions.

Both of these probably run better in Safe Mode (F8 – without Networking)

Finally if both of the above fail then try one of the methods in:

<http://www.pchell.com/support/aboutblank.shtml> "

I can also recommend the procedures at [www.pchell.com](http://www.pchell.com) .

If none of this helps, then post back and we'll take things to the next level. (Even if it does fix it, please post back – there are some followup steps that you need to take.)

--

Please respond in the same thread.

Regards, Jim Byrd, MS-MVP

In news:C44F8112-A2D5-45CD-B505-446DF8685C00@microsoft.com,

Buster <Buster@discussions.microsoft.com> typed:

> Hey, iv recently gained a virus on my computer called "About:Blank",  
> iv had it once befor and failed to remove it so i rebuilt my  
> computer. Iv now got it again and carn't get rid of it. does anyone  
> Know how to get rid of it without rebuilding my machien or buyin anti  
> spyware??