

## RE: Anti Spyware

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2005-02/0920.htm>

---

**From:** MAP ([MAP\\_at\\_discussions.microsoft.com](mailto:MAP_at_discussions.microsoft.com))

**Date:** 02/01/05

Date: Tue, 1 Feb 2005 04:27:02 -0800

"NFI" wrote:

> *Hi*  
> *Im having trouble with an about:blank hijacker. I have to use this forum as*  
> *i get hijcked every time i go to a site with for security or spyware. I have*  
> *Windows ME and an updated IE to version 6. I'm told i need Microsoft*  
> *Antispyware (Beta) to fix this problem, BUT i have found i cannot install it*  
> *on Windows ME.*  
>  
> *What can i do (short of updated the operating system)?????????*  
>  
> *Any help would be much appreciated as i'm ready to see how my computer goes*  
> *when dropped from a great height.*  
>  
> *Thanks*

About Buster- <http://www.spychecker.com/program/aboutbuster.html>

<http://www.resplendence.com/reglite>

Presented below are several tools and methods used to remove the about:blank homepage hijacker.

Credit:

The thorough step-by-step and example was taken from Time2Early post in [www.computercops.biz](http://www.computercops.biz)

Details

Vulnerable Systems:

\* Microsoft Internet Explorer

Homepage hijackers are an effect caused by some toolbar programs, trojans or malware. The hostile application changes the default homepage of Internet Explorer to something undesired and does not allow the user to set the homepage.

Below are several tools which can be used to find and remove malware which causes the effect. Presented here is also a manual step-by-step method of removing more persistent homepage hijackers.

Please reboot the machine after each step before checking if the removal was successful.

Spyware / trojan removal tools:

Spybot – Search & Destroy can detect and remove spyware of different kinds from your computer. Spyware is a relatively new kind of threat that common anti-virus applications do not yet cover. If you see new toolbars in your Internet Explorer that you didn't intentionally install, if your browser crashes, or if your browser start page has changed without your knowing, you most probably have spyware.

CWS shredder – A general homepage hijackers detector and remover. Initially based on the article Hijacked!, but expanded with almost a dozen other checks against hijacker tricks. It is continually updated to detect and remove new hijacks.

AVG antiVirus – An antivirus tool which also deals with some hijackers.

Manual step-by-step:

If a persistent hijacker is not removed by the tools listed above, manual removal should be used.

To Remove "About:Blank" Hijacker Adware In Windows XP Home edition Service Pack 1 with Internet Explorer 6.0

(probably works in NT and 2000 with some directory name changes only) follow this procedure:

Programs Needed:

- \* Reglite.exe

- \* Microsoft Recovery Console (an application available on your Windows installation disc). To access the recovery console run the following command:

```
D:\i386\winnt32.exe /cmdcons
```

(Where D should be replaced with the CD drive letter)

- \* HiJackThis.exe

Removal Procedure:

There are two application extensions (.dll) files that need to be deleted.

One is hidden (thanks Akadia!), one is detected with "HiJackThis.exe"

1) With "Reglite.exe" find name of hidden file:

Double Click on "AppInit\_DLLs" located in

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ The

"value" window reveals the hidden file name. (mine was "hlpl.dll", yours may be different!)

In this example we'll call it "hidden.dll"

Browse to the file, right click it, select Properties. Under the General

tab, uncheck Hidden and Read-Only. Select the Security tab and Check the 'Full control' check box to allow deleting it.  
Try deleting the file (Shift + Del or right click and Delete) If it was impossible to delete the file, continue to step 2. Otherwise skip to step 3.

2) Rename the hidden file:

Close Windows and reboot using "Windows Recovery Console"  
Bwose to the system32 directory located at: C:\Windows\system32\  
Replace this path with your system32 dir. In order to know your system32 run cmd and type:  
echo %WINDIR%\System32

After finding your system32 directory do the following:

a) Change file from read only by typing attrib -r hidden.dll  
b) Rename the file (For some reason this only works after rename) type:  
rename hidden.dll nasty.dll  
(and remember that "hidden.dll" is for this explanation only use the name you found earlier)  
Type "exit" and reboot to Windows.

3) Edit registry to remove hidden file:

Run "reglite.exe" again.  
Double Click on "AppInit\_DLLs" located in  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\  
Delete the file in "value" window, the "size" window changes also.  
"Apply" changes and exit "reglite.exe"

4) Edit registry to remove the second file:

Run HiJackThis.exe and scan the registry.  
Check the boxes to remove the following entries:  
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar =  
res://C:\WINDOWS\System32\jheckb.dll/sp.html (obfuscated)  
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page =  
res://C:\WINDOWS\System32\jheckb.dll/sp.html (obfuscated)  
R1 - HKCU\Software\Microsoft\Internet Explorer\Search,SearchAssistant =  
res://C:\WINDOWS\System32\jheckb.dll/sp.html (obfuscated)  
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Bar =  
res://C:\WINDOWS\System32\jheckb.dll/sp.html (obfuscated)  
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =  
res://C:\WINDOWS\System32\jheckb.dll/sp.html (obfuscated)  
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =  
res://C:\WINDOWS\System32\jheckb.dll/sp.html (obfuscated)  
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,HomeOldSP =  
about:blank

(as you can see the second .dll in the example was called "jheckb.dll" yours may be different) For this example let's call it "obvious.dll".

\* Note: As there are MANY variations to this hijacker, the registry entries might differ from the ones listed above. If the entries are different, look for entries containing the name of the second dll, in this example jheckb.dll.

microsoft.public.windows.inetexplorer.ie6.browser: RE: Anti Spyware

Finally delete the two .dlls ("hidden.dll" and "obvious.dll")

That's it! You should be running again