

Re: Homepage defaults to MSN at random

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6.browser/2005-07/msg0179>

- *From:* "Jan II" <abuse@xxxxxxxxxxxxxx>
 - *Date:* Tue, 19 Jul 2005 13:37:54 -0400
-

Hi Sportscover IT Department :-)

If the only programs you used to scan the machines with were AdAware Pro and Sophos, then you cannot assume that the machines have been fully cleaned. Neither of those program has all the necessary files to detect and remove all of the types of Trojans, hijackers and other malware there is. And, if you did not run the scans in Safe Mode with Hidden files enabled, then you did not thoroughly scan the systems.

Therefore, if the other suggestions did not resolve the problem, then you likely have some scumware on the systems causing the problem. In addition to updating and running your AV, download, install and run the programs below in Safe Mode with Hidden Files enabled. Some types of malware can replicate itself repeatedly if not removed properly, so even if you have run some of the programs listed here, it is important that you run them again according to the information below so that Windows is not operating to hide any files 'in use' Follow all instructions carefully:

First, Clear the TIF's and empty the recycle bin:
<http://www.mvps.org/winhelp2002/delcache.htm>

Also&empty your Recycle bin.

Then do the following:

WARNING>>>> Backup all documents and files before removing any spyware!!

Most importantly, download install and run CWS shredder here
<http://www.majorgeeks.com/download3019.html>
or here

Re: Homepage defaults to MSN at random

<http://www.trendmicro.com/cwshredder/>

Then download, install and immediately update these three programs before running:

AdAware SE - Update immediately after installing

<http://www.download.com/3000-2144-10045910.html?part=69274&subj=dlpage&taq=button>

SpyBot S & D - Update immediately after installing

<http://www.majorgeeks.com/download2471.html>

Microsoft Windows Antispyware Program (Beta)

<http://www.microsoft.com/athome/security/spyware/software/default.aspx>

Then visit these sites (if possible) to test for parasites and help with basic cleaning:

On-Line Check

<http://aumha.org/a/noads.htm>

and

Quick-Fix Protocol.

<http://aumha.org/a/quickfix.php>

Next, do an Online scan here (if possible) -

http://www.pandasoftware.com/activescan/com/activescan_principal.htm

Make sure that you choose "fix" or "clean".

Download Pocket Killbox from

<http://www.thespykiller.co.uk/files/killbox.exe>

and put it on the desktop where you can find it easily, if needed, but, don't run it yet.

Download, install, and run HiJackThis - it is one of the most important tools to help clean your system of scumware. Follow the instructions carefully:

How to download and install HiJackThis: (it does not need to be updated)

<http://www.bleepingcomputer.com/forums/topict309.html>

Please DO NOT post your log to this newsgroup. It is important that you go

to one of the HiJackThis Support Forums below:

CastleCops HiJackThis Forum

http://castlecops.com/f67-Hijackthis_Spyware_Viruses_Worms_Trojans_Oh_My.html

or Bleeping Computer HiJackThis Forum

<http://www.bleepingcomputer.com/forums/forum22.html>

to allow the program experts there to evaluate your log and advise you of any

necessary steps to clean your system.

(Note: Look for and read the "Important- Read This First" messages in the sections for HiJackThis logs so that you follow proper procedure. You

Re: Homepage defaults to MSN at random

will have to Register before posting on these Forums. Please follow all posting instructions carefully to avoid having your log deleted or ignored.)

Also, please post a link to the forum where you post your HJT log back to this thread so that we can follow your progress there.

CAUTION!!!!!! Before you try to remove spyware using any of the programs below, download a copy of LSPFIX from any of the following sites:

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

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

(if your OS is Win2k or XP) The process of removing certain malware may kill your internet connection. If this should occur, this program, LSPFIX, will enable you to regain your connection.

You should also get a copy of WINSOCKXPFIX to have at hand if needed, available at the links below, but, don't run it yet:

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

and

WinsockXP Fix- WinXP

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

with instructions, at

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

also... From LavaSoft- all versions of Windows-

<http://digital-solutions.co.uk/lavasoft/whndnfix.zip>

(NOTE: It is reported that in XP SP2, the command netsh winsock reset will fix this problem without the need for these programs.)

or Winsock Fix Utility

<http://www.dfwonline.net/files/WinsockFix.zip>

How to Restart in Safe Mode

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

How to Show Hidden Files

<http://snipurl.com/6rl8>

Hope this helps.

Jan :)

MS MVP - IE/OE

Smiles are meant to be shared,
that's why they're so contagious.

Re: Homepage defaults to MSN at random

Replies are posted only to the newsgroup for the benefit of other readers.
How to make a good newsgroup post:
<http://www.dts-1.org/goodpost.htm>

Hi Jan

The affected users are both Win2000 SP4 and XP SP2 using IE6 SP1. Trojan, virus and spyware checks with Adaware 6 Pro and Sophos are both clean (users cannot install anything anyway and all executables and active-X are blocked by strict proxy rules). I am thinking there is an issue with the machines occasionally not picking up their group policies properly and therefore defaulting to the IE defaults rather than the group policy settings. Sometimes, sites in the Trusted zone also are not logged in automatically. The IE start page is locked via group policy, end users cannot change it, and even when MSN comes up, the start page is still set to the correct intranet page anyway it just doesn't open it. I don't want to unlock the greyed out home page option, and I could easily do that though Group Policy anyway, the problem is that IE 'sometimes' ignores its home page settings for no reason.

Cheers
Ben

"Jan 11" wrote:

Hi Sportscover IT Department :-)

You do not give us the version of Windows or IE that is used on these machines (i.e. IE6 SP1, SP2). Have you scanned them

Re: Homepage defaults to MSN at random

for hjackware,
malware, Trojans? If so, what programs did you use?
Were the scans done in
Safe Mode? What was the result?

also...check the following and see if it helps:

If you have SpyBot S&D installed, go to the "Immunize" section.
Is "Lock IE Start Page Settings" ticked?

Homepage Problem errors & information
<http://www.generation.net/~hleboeuf/iehome.htm>
If so, uncheck it.

Unlocks the grayed-out Home Page section on the General Tab
<http://www.mvps.org/winhelp2002/UnlockHomePage.reg>

Unlock My Homepage - Free
<http://www.3ee.com/unlock.asp>

Hope this helps.

Jan :)
MS MVP - IE/OE
Smiles are meant to be shared,
that's why they're so contagious.

Replies are posted only to the newsgroup for the
benefit or other readers.

How to make a good newsgroup post:
<http://www.dts-l.org/goodpost.htm>

>I am having a problem where a couple of users have their IE open at MSN
> rather than at the intranet site specified in Group Policy. Their IE
> homepage

Re: Homepage defaults to MSN at random

> settings are greyed out and set to the intranet site, but clicking the
> home
> button or opening IE bring up MSN instead. This does not happen to
> everyone,
> and does not happen consistently. All Group Policies up to the domain
> default
> policy specify the intranet site as the home page.
>
> Any help appreciated.
> Thanks
> Ben