

[REVS] Removing about:blank Homepage Hijacker

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0070.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/24/04

To: list@securiteam.com

Date: 24 Jun 2004 15:37:39 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Removing about:blank Homepage Hijacker

SUMMARY

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

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 back to the desired address.

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.

It is advisable to reboot the machine after each step before checking if the removal was successful.

Spyware / trojan removal tools:

<<http://www.spybot.info/>> Spybot – Search & Destroy can detect and remove

Securiteam: [REVS] Removing about:blank Homepage Hijacker

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's start page has changed without your knowing, you most probably have spyware.

<<http://www.spywareinfo.com/~merijn/cwschronicles.html>> CWShredder – A general homepage hijackers detector and remover. Initially based on the article <<http://www.spywareinfo.com/articles/hijacked/>> Hijacked!, but expanded with almost a dozen other checks against hijacker tricks. It is continually updated to detect and remove new hijacks.

<http://www.grisoft.com/us/us_index.php> 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.

The following procedure was written by Ttime2Early on the <<http://www.computercops.biz/postp217898.html>> Computer cops forum.

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:

* <<http://www.resplendence.com/download/reglite.exe>> Reglite.exe

* Microsoft Recovery Console
(an option available on your Windows CD or root drive)
run X:\i386\winnt32.exe /cmdcons
where X is either CD drive letter or Windows installation root dir.

* <<http://www.spywareinfo.com/~merijn/files/HijackThis.exe>>
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 let's call it "hidden.dll"

2) Rename the hidden file:
Close Windows and reboot using "Windows Recovery Console"

Securiteam: [REVS] Removing about:blank Homepage Hijacker

Go to "c:\Windows\system32\" and do two things.
Change file from read only by typing `attrib -r hidden.dll`
Then rename it (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".

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

That's it! You should be running again

By the way, if you go offline with Internet Explorer and type OK to these nasty adware windows you will see the guys who benefit from this hijacker.

Time2Early found:

www.palsol.com

www.likesurfing.com

www.vn.msie.cc (the real web page)

They seem to be selling adware/spyware protection...

ADDITIONAL INFORMATION

Securiteam: [REVS] Removing about:blank Homepage Hijacker

The thorough step-by-step and example was taken from
<<http://www.computercops.biz/postp217898.html>> Time2Early post in
<www.computercops.biz> www.computercops.biz

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.