

HijackThis Tutorial

Essential program to help remove spyware

What is HijackThis ?

HijackThis is a program developed by Merijn Bellekom, a Dutch student studying chemistry and computer science. One of Merijn's programs, Hijackthis, is an essential utility to help find and remove spyware, viruses, worms, trojans and other pests.

This is a basic guide to understanding HijackThis logs, what specific sections mean and some tips on reading it yourself. Although its best to have a knowledge person help you examine the Hijackthis logs, knowing more about the logs help individuals understand more about them and their use.

Overview

Each line in a HijackThis log starts with a section name. (For technical information on this, click 'Info' in the main window and scroll down. Highlight a line and click 'More info on this item'.)

R0, R1, R2, R3 - IE Start & Search page

What it looks like:

```
R0 - HKCUSoftwareMicrosoftInternet ExplorerMain,Start
Page=http://www.google.com/
R1 - HKLMSoftwareMicrosoftInternet
ExplorerMain,Default_Page_URL=http://www.google.com/
R3 - Default URLSearchHook is missing
```

What to do:

If you recognize the URL at the end as your homepage or search engine, it's OK. If you don't, check it and have HijackThis fix it. In cases like the random.dll hijacker you may want to leave them til later but in general if you dont recognize it, fix it.

For the R3 items, always fix them unless it mentions a program you recognize.

F0, F1 - Autoloading programs

What it looks like:

```
F0 - system.ini: Shell=Explorer.exe Openme.exe
F1 - win.ini: run=hpfsched
```

What to do:

The F0 items are always bad, so fix them.

The F1 items are usually very old programs that are safe, so you should find some more info on the filename to see if it's good or bad.

N1, N2, N3, N4 - Netscape/Mozilla Start & Search page

What it looks like:

N1 - Netscape 4: user_pref("browser.startup.homepage", "www.google.com");

(C:\Program Files\Netscape\Users\defaultprefs.js)

N2 - Netscape 6: user_pref("browser.startup.homepage", "http://www.google.com");

(C:\Documents and Settings\User\Application Data\Mozilla\Profiles\default\9t1tfl.slt\prefs.js)

N2 - Netscape 6: user_pref("browser.search.defaultengine",

"engine://C%3A%5CProgram%20Files%5C Netscape%206%5Csearchplugins%5CSBW eb_02.src"); (C:\Documents and Settings\User\Application

Data\Mozilla\Profiles\default\9t1tfl.slt\prefs.js)

What to do:

Usually the Netscape and Mozilla homepage and search page are safe. They rarely get hijacked. Should you see an URL you don't recognize as your homepage or search page, have HijackThis fix it.

O1 - Hosts file redirection

What it looks like:

O1 - Hosts: 216.177.73.139 auto.search.msn.com

O1 - Hosts: 216.177.73.139 search.netscape.com

O1 - Hosts: 216.177.73.139 ieautosearch

What to do:

This hijack will redirect the address to the right to the IP address to the left. If the IP does not belong to the address, you will be redirected to a wrong site everytime you enter the address. You can always have HijackThis fix these, unless you knowingly put those lines in your Hosts file.

O2 - Browser Helper Objects

What it looks like:

O2 - BHO: Yahoo! Companion BHO - {13F537F0-AF09-11d6-9029-0002B31F9E59} - C:\PROGRAM FILES\YAHOO!\COMPANION\YCOMP5_0_2_4.DLL
O2 - BHO: AcroIEHlprObj Class - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} - C:\Adobe\Acrobat 5.0\Acrobat\ActiveX\AcroIEHelper.ocx
O2 - BHO: (no name) - {724d43a9-0d85-11d4-9908-00400523e39a} - C:\Program Files\Siber Systems\AI RoboForm\RoboForm.dll

What to do:

If you don't directly recognize a Browser Helper Object's name, use TonyK's BHO List to find it by the class ID (CLSID, the number between curly brackets) and see if it's good or bad. In the BHO List, 'X' means spyware and 'L' means safe.

O3 - IE toolbars

What it looks like:

O3 - Toolbar: &Yahoo! Companion - {EF99BD32-C1FB-11D2-892F-0090271D4F88} - C:\PROGRAM FILES\YAHOO!\COMPANION\YCOMP5_0_2_4.DLL
O3 - Toolbar: Popup Eliminator - {86BCA93E-457B-4054-AFB0-E428DA1563E1} - C:\PROGRAM FILES\POPUP ELIMINATOR\PETOOLBAR401.DLL (file missing)
O3 - Toolbar: &RoboForm - {724d43a0-0d85-11d4-9908-00400523e39a} - C:\Program Files\Siber Systems\AI RoboForm\RoboForm.dll

What to do:

If you don't directly recognize a toolbar's name, use TonyK's Toolbar List to find it by the class ID (CLSID, the number between curly brackets) and see if it's good or bad. In the Toolbar List, 'X' means spyware and 'L' means safe.

If it's not on the list and the name seems a random string of characters and the file is somewhere in a folder named 'Application Data', it's definitely bad, and you should have HijackThis fix it.

O4 - Autoloading programs from Registry

What it looks like:

O4 - HKLM..Run: [ScanRegistry] C:\WINDOWS\scanregw.exe /autorun
O4 - HKLM..Run: [SystemTray] SysTray.Exe
O4 - HKLM..Run: [ccApp] "C:\Program Files\Common Files\Symantec Shared\ccApp.exe"
O4 - Startup: Microsoft Office.lnk = C:\Program Files\Microsoft Office\Office\OSA9.EXE

What to do:

Use PacMan's Startup List to find the entry and see if it's good or bad.

O5 - IE Options not visible in Control Panel

What it looks like:

O5 - control.ini: inetcpl.cpl=no

What to do:

Unless you've knowingly hidden the icon from Control Panel, have HijackThis fix it.

O6 - IE Options access restricted by Administrator

What it looks like:

O6 - HKCUSoftwarePoliciesMicrosoftInternet ExplorerRestrictions present

What to do:

Unless you have the Spybot S&D option 'Lock homepage from changes' active, have HijackThis fix this.

O7 - Regedit access restricted by Administrator

What it looks like:

O7 - HKCUSoftwareMicrosoftWindowsCurrentVersionPoliciesSystem, DisableRegedit=1

What to do:

Always have HijackThis fix this.

O8 - Extra items in IE right-click menu

What it looks like:

O8 - Extra context menu item: &Google Search - res://C:WINDOWSDOWNLOADED PROGRAM FILESGOOGLETOOLBAR_EN_1.1.68-DELEON.DLL/cmsearch.html

O8 - Extra context menu item: Yahoo! Search - file:///C:Program FilesYahoo!Common/ysearch.htm

What to do:

If you don't recognize the name of the item in the right-click menu in IE, have HijackThis fix it.

O9 - Extra buttons on main IE toolbar, or extra items in IE 'Tools' menu

What it looks like:

O9 - Extra button: Messenger (HKLM)

O9 - Extra 'Tools' menuitem: Messenger (HKLM)

O9 - Extra button: AIM (HKLM)

What to do:

If you don't recognize the name of the button or menuitem, have HijackThis fix it.

O10 - Winsock hijackers

What it looks like:

O10 - Hijacked Internet access by New.Net

O10 - Broken Internet access because of LSP provider

'c:progra~1\common~2\toolbar\mib.dll' missing

O10 - Unknown file in Winsock LSP: c:\program files\newton knows\vmmain.dll

What to do:

It's best to fix these using LSPFix from Cexx.org, Spybot Search and Destroy, or WinsockXPFix

O11 - Extra group in IE 'Advanced Options' window

What it looks like:

O11 - Options group: [CommonName] CommonName

What to do:

The only hijacker as of now that adds its own options group to the IE Advanced Options window is CommonName. So you can always have HijackThis fix this.

O12 - IE plugins

What it looks like:

O12 - Plugin for .spop: C:\Program Files\Internet Explorer\Plugins\NPDocBox.dll

O12 - Plugin for .PDF: C:\Program Files\Internet Explorer\PLUGINS\ppdf32.dll

What to do:

Most of the time these are safe. Only OnFlow adds a plugin here that you don't want (.ofb).

O13 - IE DefaultPrefix hijack

What it looks like:

O13 - DefaultPrefix: <http://www.pixpox.com/cgi-bin/click.pl?url=>

O13 - WWW Prefix: <http://prolivation.com/cgi-bin/r.cgi?>

What to do:

These are always bad. Have HijackThis fix them.

O14 - 'Reset Web Settings' hijack

What it looks like:

O14 - IERESET.INF: START_PAGE_URL=<http://www.searchalot.com>

What to do:

If the URL is not the provider of your computer or your ISP, have HijackThis fix it.

O15 - Unwanted site in Trusted Zone

What it looks like:

O15 - Trusted Zone: <http://free.aol.com>

What to do:

So far, only AOL has the tendency to add itself to your Trusted Zone, allowing it to run any ActiveX it wants. Always have HijackThis fix this.

O16 - ActiveX Objects (aka Downloaded Program Files)

What it looks like:

O16 - DPF: Yahoo! Chat -

<http://us.chat1.yimg.com/us.yimg.com/i/chat/applet/c381/chat.cab>

O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object)

- <http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab>

What to do:

If you don't recognize the name of the object, or the URL it was downloaded from, have HijackThis fix it. If the name or URL contains words like 'dialer', 'casino', 'free_plugin' etc, definitely fix it.

O17 - Lop.com domain hijacks

What it looks like:

O17 - HKLMSystemCCSServicesVxDMSTCP: Domain = aoldsl.net

O17 - HKLMSystemCCSServicesTcpipParameters: Domain = W21944.find-quick.com

O17 - HKLMSoftware..Telephony: DomainName = W21944.find-quick.com

O17 - HKLMSystemCCSServicesTcpip..{D196AB38-4D1F-45C1-9108-46D367F19F7E}: Domain = W21944.find-quick.com

What to do:

If the domain is not from your ISP or company network, have HijackThis fix it.

O18 - Extra protocols and protocol hijackers

What it looks like:

O18 - Protocol: relatedlinks - {5AB65DD4-01FB-44D5-9537-3767AB80F790} - C:\PROGRA~1\COMMON~1\MSIETS\msielink.dll

O18 - Protocol: mctp - {d7b95390-b1c5-11d0-b111-0080c712fe82}

O18 - Protocol hijack: http - {66993893-61B8-47DC-B10D-21E0C86DD9C8}

What to do:

Only a few hijackers show up here. The known baddies are 'cn' (CommonName), 'ayb' (Lop.com) and 'relatedlinks' (Huntbar), you should have HijackThis fix those.

Other things that show up are either not confirmed safe yet, or are hijacked by spyware. In the last case, have HijackThis fix it.

O19 - User style sheet hijack

What it looks like:

O19 - User style sheet: c:WINDOWS\Java\my.css

What to do:

In the case of a browser slowdown and frequent popups, have HijackThis fix this item if it shows up in the log.

If something in your log still puzzles you after this short tutorial, there is nothing stopping you from posting at the SpywareInfo forums. However, one of the reasons I wanted to post this tutorial here is because Spywareinfo.com seems to be the target of many denial of service attacks making it difficult to reach sometimes.

This tutorial was originally created by Merijn, the creator of Hijackthis

Removal Instructions for Other Programs

Spyware Removal and Other Resources

How to Remove SurferBar

Bonzi Buddy Removal

Click2FindNow and I-Lookup Removal

Comet Cursor Removal

Date Manager Removal

About:Blank Homepage Hijacker Removal Instructions and Help

res://random.dll Homepage Hijacker Removal Instructions and Help

Dubolom.com Homepage Hijacker Removal Instructions and Help

[DSO Exploit Removal Instructions and Help](#)

[FastSearch.cc Homepage Hijacker Removal Instructions and Help](#)

[Gator Software Removal](#)

[Hugesearch.net Homepage Hijacker Removal Instructions and Help](#)

[Search-Space.com and Start-Space.com Homepage Hijacker Removal Instructions and Help](#)

[How to Remove Global-Finder.com Homepage Hijacker](#)

[Globaltoolbar Removal](#)

[GoHip Software Removal](#)

[HotBar Toolbar Removal](#)

[Huntbar and Search Toolbar Info and Removal](#)

[Look2Me Removal Instructions and Help](#)

[Lookfor.cc \(res://mshp.dll/index.html\) Homepage Hijacker Removal Instructions and Help](#)

[MaximumSearch.net Homepage Hijacker Removal Instructions and Help](#)

[Ncase Removal Instructions and Help](#)

[People OnPage Toolbar Info and Removal](#)

[Precision Time Removal](#)

[Prolivation.com Removal](#)

[SaveNow and NewDotNet Removal](#)

[SearchMyRequest.com Homepage Hijacker Removal Instructions and Help](#)

[Smartsearch.ws Homepage Hijacker Removal Instructions and Help](#)

[SysUpd.exe \(TSCash\) Removal Instructions and Help](#)

[Ezula TopText \(yellow underlined links\) Removal Instructions and Help](#)

[How to Remove SpeedBlaster and MemoryMeter](#)

[Twaintec.dll Removal Instructions and Help](#)

[WeatherBug Removal](#)

[WinTools Removal Instructions and Help](#)

[Xupiter Removal](#)

[Xzoomy.com Removal](#)

[ZY Web Search \(db105.com\) Removal](#)