

Hijack This Tutorial

Contributed by David Noel-Davies

Hijack This Tutorial (the program may be downloaded from [here](#))

This article is for advanced users.

If you are not familiar with running processes on your computer as well as anything ever installed that could tie into your web browser, it will not be much help to you.

Finally, Hijack This has been taken over by Trend Micro. This new version can be downloaded [here](#).

You should have scanned your machine with anti-spyware, virus and Trojan tools before using Hijack This.

This article is meant for those wishing to learn more about what HijackThis is showing you and how to analyze logs yourself. It is not really meant for novices. It is meant to be more educational for intermediate to advanced PC users.

Below explains what each section means and each of these sections are broken down with examples to help you understand what is safe and what should be removed.

Official Hijack This Tutorial:

Each line in a HijackThis log starts with a section name, for example;

R0, R1, R2, R3 - Internet Explorer Start/Search

pages URLs

F0, F1 - Autoloading programs

N1, N2, N3, N4 - Netscape/Mozilla Start/Search
pages URLs

O1 - Hosts file redirection

O2 - Browser Helper Objects

O3 - Internet Explorer toolbars

O4 - Autoloading programs from Registry

O5 - IE Options icon not visible in Control
Panel

O6 - IE Options access restricted by
Administrator

O7 - Regedit access restricted by Administrator

O8 - Extra items in IE right-click menu

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

O10 - Winsock hijacker

O11 - Extra group in IE 'Advanced Options'
window

O12 - IE plugins

O13 - IE DefaultPrefix hijack

O14 - 'Reset Web Settings' hijack

O15 - Unwanted site in Trusted Zone

O16 - ActiveX Objects (aka Downloaded Program
Files)

O17 - Lop.com domain hijackers

O18 - Extra protocols and protocol hijackers

O19 - User style sheet hijack

O20 - AppInit_DLLs Registry value autorun

O21 - ShellServiceObjectDelayLoad Registry key
autorun

O22 - SharedTaskScheduler Registry key autorun

O23 - Windows NT Services

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

What it looks like:

Quote:

R0 -
HKCU\Software\Microsoft\Internet
Explorer\Main,Start Page =

<http://www.google.com/>

R1 -
HKLM\Software\Microsoft\Internet
Explorer\Main,Default_Page_URL =

<http://www.google.com/>

R2 - (this type is not used by
HijackThis yet)

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.

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

F0, F1, F2, F3 - Autoloading programs from INI files

What it looks like:

Quote:

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.

Pacman's Startup List can help with identifying an item.

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

What it looks like:

Quote:

N1 - Netscape 4:
user_pref("browser.startup.homepage",
"www.google.com"); (C:\Program
Files\Netscape\Users\default\prefs.js)

N2 - Netscape 6:
user_pref("browser.startup.homepage",
"http://www.google.com");
(C:\Documents and
Settings\User\Application
Data\Mozilla\Profiles\default09t1tfl.slt\prefs.js)

N2 - Netscape 6:

```
user_pref("browser.search.defaultengine",  
"engine://C%3A%5CProgram%20Files%5C Netscape%20%5Csearchplugins%5CSBWeb_02.src");  
(C:\Documents and  
Settings\User\Application  
Data\Mozilla\Profiles\default09t1tfl.slt\prefs.js)
```

What to do:

Usually the Netscape and Mozilla homepage and search page are safe. They rarely get hijacked, only Lop.com has been known to do this. Should you see an URL you don't recognize as your homepage or search page, have HijackThis fix it.

O1 - Hostsfile redirections

What it looks like:

Quote:

```
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
```

```
O1 - Hosts file is located at  
C:\Windows\Help\hosts
```

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.

The last item sometimes occurs on Windows 2000/XP with a Coolwebsearch infection. Always

fix this item, or have

CWS shredder repair it automatically.

O2 - Browser Helper Objects

What it looks like:

Quote:

O2 - BHO: Yahoo! Companion BHO -
{13F537F0-AF09-11d6-9029-0002B31F9E59}
- C:\PROGRAM
FILES\YAHOO!\COMPANION\YCOMP5_0_2_4.DLL

O2 - BHO: (no name) -
{1A214F62-47A7-4CA3-9D00-95A3965A8B4A}
- C:\PROGRAM FILES\POPUP
ELIMINATOR\AUTODISPLAY401.DLL (file
missing)

O2 - BHO: MediaLoads Enhanced -
{85A702BA-EA8F-4B83-AA07-07A5186ACD7E}
- C:\PROGRAM FILES\MEDIALOADS
ENHANCED\ME1.DLL

What to do:

If you don't directly recognize a Browser Helper
Object's name, use

TonyK's BHO & 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
BHO List, 'X' means spyware and 'L' means safe.

O3 - IE toolbars

What it looks like:

Quote:

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: rzillcgthjx -
{5996aaf3-5c08-44a9-ac12-1843fd03df0a}
- C:\WINDOWS\APPLICATION
DATA\CKSTPRLLNQUL.DLL

What to do:

If you don't directly recognize a toolbar's name, use

TonyK's BHO & 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 in the 'Application Data' folder (like the last one in the examples above), it's probably Lop.com, and you definately should have HijackThis fix it.

O4 - Autoloading programs from Registry or Startup group

What it looks like:

Quote:

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

O4 - Global Startup: winlogon.exe

What to do:

Use

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

If the item shows a program sitting in a Startup group (like the last item above), HijackThis cannot fix the item if this program is still in memory. Use the Windows Task Manager (TASKMGR.EXE) to close the process prior to fixing.

O5 - IE Options not visible in Control Panel

What it looks like:

Quote:

O5 - control.ini: inetctl.cpl=no

What to do:

Unless you or your system administrator have knowingly hidden the icon from Control Panel, have HijackThis fix it.

O6 - IE Options access restricted by Administrator

What it looks like:

Quote:

O6 -
HKCU\Software\Policies\Microsoft\Internet
Explore\Restrictions present

What to do:

Unless you have the Spybot S&D option 'Lock homepage from changes' active, or your system administrator put this into place, have HijackThis fix this.

O7 - Regedit access restricted by Administrator

What it looks like:

Quote:

O7 -
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System,
DisableRegedit=1

What to do:

Always have HijackThis fix this, unless your system administrator has put this restriction into place.

O8 - Extra items in IE right-click menu

What it looks like:

Quote:

O8 - Extra context menu item:
&Google Search -
res://C:\WINDOWS\DOWNLOADED PROGRAM
FILES\GOOGLETOOLBAR_EN_1.1.68-DELEON.DLL/cmsearch.html

O8 - Extra context menu item: Yahoo!
Search - file:///C:\Program
Files\Yahoo!\Common/ycsrch.htm

O8 - Extra context menu item: Zoom
&In - C:\WINDOWS\WEB\zoomin.htm

O8 - Extra context menu item: Zoom
O&ut - C:\WINDOWS\WEB\zoomout.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:

Quote:

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:

Quote:

O10 - Hijacked Internet access by New.Net

O10 - Broken Internet access because of LSP provider 'c:\progra~1\common~2\toolbar\cnmib.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, or

Spybot S&D from Kolla.de.

Note that 'unknown' files in the LSP stack will not be fixed by HijackThis, for safety issues.

O11 - Extra group in IE 'Advanced Options' window

What it looks like:

Quote:

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:

Quote:

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

O12 - Plugin for .PDF: C:\Program
Files\Internet
Explorer\PLUGINS\nppdf32.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:

Quote:

O13 - DefaultPrefix:

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

O13 - WWW Prefix:

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

O13 - WWW. Prefix:

<http://ehhttp.cc/?>

What to do:

These are always bad. Have HijackThis fix them.

O14 - 'Reset Web Settings' hijack

What it looks like:

Quote:

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 sites in Trusted Zone

What it looks like:

Quote:

O15 - Trusted Zone:

<http://free.aol.com>

O15 - Trusted Zone:

*.coolwebsearch.com

O15 - Trusted Zone: *.msn.com

What to do:

Most of the time only AOL and Coolwebsearch silently add sites to the Trusted Zone. If you didn't add the listed domain to the Trusted Zone yourself, have HijackThis fix it.

O16 - ActiveX Objects (aka Downloaded Program Files)

What it looks like:

Quote:

O16 - DPF: Yahoo! Chat -

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

O16 - DPF:

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

<http://download.macromedia.com/pub/s...sh/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.

Javacool's SpywareBlaster has a huge database of malicious ActiveX objects that can be used for looking up CLSIDs. (Right-click the list to use the Find function.)

O17 - Lop.com domain hijacks

What it looks like:

Quote:

O17 -
HKLM\System\CCS\Services\VxD\MSTCP:
Domain = aodsl.net

O17 -
HKLM\System\CCS\Services\Tcpip\Parameters:
Domain = W21944.find-quick.com

O17 - HKLM\Software\..\Telephony:
DomainName = W21944.find-quick.com

O17 -
HKLM\System\CCS\Services\Tcpip\..\{D196AB38-4D1F-45C1-9108-46D367F19F7E}:
Domain = W21944.find-quick.com

O17 -
HKLM\System\CS1\Services\Tcpip\Parameters:
SearchList = gla.ac.uk

O17 -
HKLM\System\CS1\Services\VxD\MSTCP:
NameServer =

69.57.146.14,69.57.147.175

What to do:

If the domain is not from your ISP or company network, have HijackThis fix it. The same goes for the 'SearchList' entries.

For the 'NameServer' (DNS servers) entries, Google for the IP or IPs and it will be easy to see if they are good or bad.

O18 - Extra protocols and protocol hijackers

What it looks like:

Quote:

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 (i.e. the CLSID has been changed) by spyware. In the last

case, have HijackThis fix it.

O19 - User style sheet hijack

What it looks like:

Quote:

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. However, since only Coolwebsearch does this, it's better to use

CWShredder to fix it.

O20 - Applnit_DLLs Registry value autorun

What it looks like:

Quote:

O20 - Applnit_DLLs: msconfd.dll

What to do:

This Registry value located at

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Windows

loads a DLL into memory when the user logs in,
after which it stays in memory

until logoff. Very few legitimate programs use
it (Norton CleanSweep uses

API TRAP.DLL), most often it is used by trojans
or aggressive browser hijackers.

In case of a 'hidden' DLL loading from this
Registry value (only visible when

using 'Edit Binary Data' option in Regedit) the
dll name may be prefixed with

a pipe '|' to make it visible in the log.

O21 - ShellServiceObjectDelayLoad Registry
key autorun

What it looks like:

Quote:

O21 - SSODL - AUHOOK -
{11566B38-955B-4549-930F-7B7482668782}
- C:\WINDOWS\System\auhook.dll

What to do:

This is an undocumented autorun method, normally
used by a few Windows system

components. Items listed at

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\

ShellServiceObjectDelayLoad

are loaded by Explorer when Windows starts.
HijackThis uses a whitelist

of several very common SSODL items, so whenever
an item is displayed in

the log it is unknown and possibly malicious.
Treat with extreme care.

O22 - SharedTaskScheduler Registry key autorun

What it looks like:

Quote:

```
O22 - SharedTaskScheduler: (no name)
-
{3F143C3A-1457-6CCA-03A7-7AA23B61E40F}
- c:\windows\system32\mtwirl32.dll
```

What to do:

This is an undocumented autorun for Windows
NT/2000/XP only, which

is used very rarely. So far only CWS.Smartfinder
uses it. Treat with care.

O23 - Windows NT Services

What it looks like:

Quote:

O23 - Service: Kerio Personal

Firewall (PersFw) - Kerio
Technologies - C:\Program Files\Kerio\Personal
Firewall\persfw.exe

What to do:

Quote:

This is the listing of non-Microsoft services. The list should be the same as the one you see in the Msconfig utility of Windows XP. Several trojan hijackers use a homemade service in addition to other startups to reinstall themselves. The full name is usually important-sounding, like 'Network Security Service', 'Workstation Logon Service' or 'Remote Procedure Call Helper', but the internal name (between brackets) is a string of garbage, like 'O?ŽrtňăĚ²\$Ó'. The second part of the line is the owner of the file at the end, as seen in the file's properties.

Note that fixing an O23 item will only stop the service and disable it. The service needs to be deleted from the Registry manually or with another tool. In HijackThis 1.99.1 or higher, the button 'Delete NT Service' in the Misc Tools section can be used for this.