Homepage

Resources

HijackThis Tutorial

Support Forum

Tools

HJTHotkey

Get Files

BBCode to HTML

HijackThis Tutorial - How to Analyse a HijackThis log

Hijackthis is a tool that lists most if not all know places on your computer that spy/adware is known to target. These include all software that starts up when you turn on your computer, everything that starts with your browser, items in the hosts file which may cause your browser to redirect to unwanted sites as well as many other things.

What are Spyware, Adware, Trojans, Hijackers, BHO's?

Before you start, you can save time by running the following malware removal programs-

Run Adaware- www.lavasoft.de instructions- AdAware tutorial

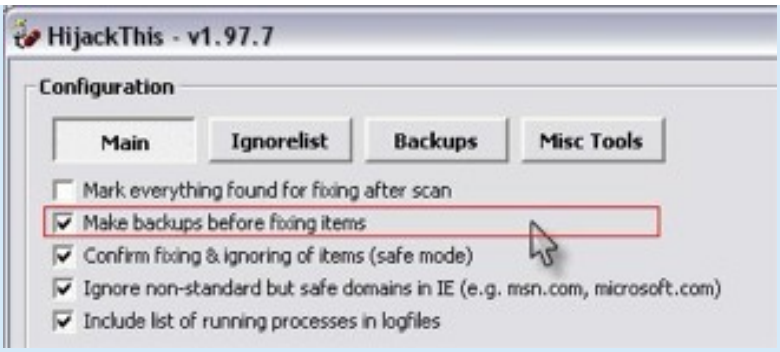
Run Spybot S&D- http://www.safer-networking.org/index.php?page=download instructions- http://www.bleepingcomputer.com/tutorials/tutorial43.html

Run a Free Online Virus scan- Trend Micro Free Online Virus scan

Before fixing anything in HijackThis

1) It is important to create a permanent folder for it e.g. C:\HJT. This is because it will create backups which you may want to restore later if anything goes wrong. There are instructions here on creating a permanent directory for HijackThis- http://russelltexas.com/malware/createhjtfolder.htm

2) Run HijackThis and click "config". Make sure it is set to create backup (it should already be set to do this by default).



Note: Make sure that all browser windows (e.g. Internet Explorer) are closed before clicking **"fix selected"** otherwise HijackThis may not be able to remove some the items.

Each Item in the log has it's own code at the start of every line. Each code represent a different area of your computer/ registry. The following are instructions on how to research each item to tell whether or not it needs fixing.

- **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**

Added in HijackThis 1.98.x:

- **O20 - AppInit_DLLs Registry value autorun**
- **O21 - ShellServiceObjectDelayLoad Registry key autorun**
- **O22 - SharedTaskScheduler Registry key autorun**

Added in HijackThis 1.99.x:

- **O23 - NT Services**

Where/How to look them up-

- **R0, R1, R2, R3** - Internet Explorer Start/Search pages URLs

Example-

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.ntlworld.com
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,HomeOldSP = http://www.google.co.uk
R3 - URLSearchHook: PerfectNavBHO Class - {0428FFC7-1931-45b7-95CB-3CBB919777E1} - C:\PROGRA~1\PERFEC~1\BHO\PERFEC~1.DLL (file missing)

Researching Items-

These web addresses are those that start when your browser does or are set as your default search pages. If you do not recognise the address or it is an address that you do not want as you default homepage or search page then have HijackThis fix it. To see if these items are **CoolWebSearch** related, they can be looked up here-

http://www.webhelper4u.com/CWS/cwsbyalphanumeric.html. or here http://users.skynet.be/bk136527/CWS/CWSdomains.htm

load the website and go to **edit>find (On this Page)** or by pressing Ctrl+F and copy the URL (e.g. **google.com)** into the search box that appears. Click "**Find next**".

Another way to find if the website is bad is to look it up in a hosts file. The domain can be looked up in the text version of the hosts file found here-

http://www.mvps.org/winhelp2002/hosts.htm

(Click the link on that page which says ***"To view the HOSTS file in plain text form."*** and then use the same method as above to search the file)

If the domain name is found then you will need to have hijackthis fix it and also download and run CWShredder from here- http://www.intermute.com/spysubtract/cwshredder_download.html

(HJTHotkey can also search for a domain by selecting it in the log an pressing Alt + C)

R3 Items should always be fixed unless you recognise the name. You could also use google to look them up.

Special cases-

Most cases of CWS that may not appear in the CWS database can be found here- cwschronicles look down the list and compare the items to your log. Normally if CWShredder can't fix the items then there is a link to manual instructions. A lot of the newer variants appear on the home page here- http://www.spywareinfo.com/~merijn/ first. If you still have no luck and don't recognise the item then you could look it up in a search engine such as google.

(note: old "special cases" removed as they are outdated)

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

Example-

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

Researching Items-

Programs that run at startup. Mainly old programs. see **O4 - Autoloading programs from Registry** for research

Special cases-

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

Example-

N1 - Netscape 4: user_pref("browser.startup.homepage", "http://www.xupiter.com/toolbar2"); (C:\PROGRA~1\Netscape\Users\default\prefs.js)

Researching Items-

These web addresses are those that start when your browser (Netscape/Mozilla) does or are set as your default search pages.

These rarely get hijacked. If you don't recognise the URL then look it up (**see R1,2,3 items above**)

- **O1 - Hosts file redirection**

What is a hosts file?

Example-

O1 - Hosts: 38.115.131.131 sk2.slsk.org
O1 - Hosts: 38.115.131.131 www.slsk.org
O1 - Hosts: 38.115.131.131 mail.slsk.org
O1 - Hosts: 38.115.131.131 server.slsk.org

Researching Items-

When you type in the address on the right, you will be redirected to the IP address on the left so you may end up on a page you don't want to be on or the webpage won't show at all.

If you didn't put these in your hosts file or if the IP on the left doesn't point to the URL on the right then have hijackthis fix them

Special cases-

- **O2 - Browser Helper Objects**

What is a BHO?

Example-

O2 - BHO: (no name) - {00000762-3965-4A1A-98CE-3D4BF457D4C8} - C:\Program Files\Lycos\Sidesearch\sidesearch1311.dll
O2 - BHO: (no name) - {00000EF1-0786-4633-87C6-1AA7A44296DA} - C:\WINDOWS\System32\ddm3dia.dll
O2 - BHO: (no name) - {000E7270-CC7A-0786-8E7A-DA09B51938A6} - C:\WINDOWS\System32\n3tpa1.dll

Researching Items-

To see if these items are malware related, they can be looked up at the following website-

http://computercops.biz/CLSID.html

Copy the CLSID (e.g. **{00000762-3965-4A1A-98CE-3D4BF457D4C8}**) or file name e.g. **ddm3dia.dll** into the search box on the above site and click "Search". If the BHO name is found then you will notice a letter in the status column of the line. This letter will be one of the following-

X for certified spyware/foistware, or other malware,
L for legitimate items,
O for 'open to debate'
? for BHOs of unknown status.

Fix the Items with an **X** next to them. If they are not found then google can be used.

Alternatively, HJTHotkey or can search for a CLSID or file name by selecting it in the log an pressing Alt + B and/or Ctrl +B

Special cases-

Look2Me-

msg116.dll, msg117.dll, msg118.dll, msg119.dll, msg120.dll, msg121.dll, msg122.dll, upd116.exe, upd117.exe, upd118.exe, msg121.cpy.dll, msg{********-****-****-****-************}****.dll, where * represents a character.

more information: http://www.pestpatrol.com/PestInfo/v/vx2_abetterinternet.asp
removal- http://www.pchell.com/support/look2me.shtml , http://www.kephyr.com/spywarescanner/library/look2me/index.phtml , kill2me

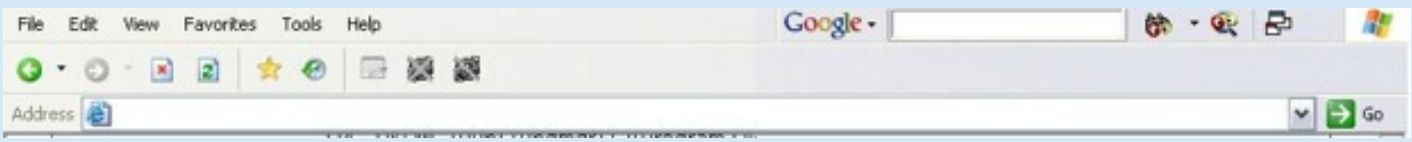
Ad-aware now has a plug-in to remove this one.
see: http://www.lavasoftsupport.com/index.php?showtopic=33729

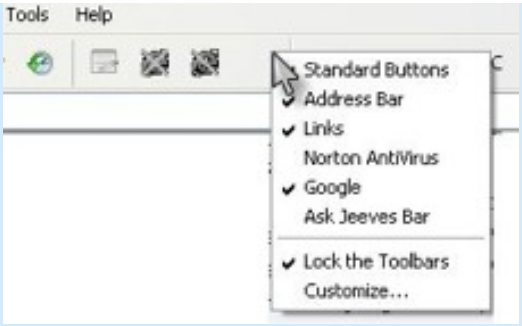
Some malware creates completely random BHO names like with the errorplace.com Hijack. If you are not sure what to fix because you cannot find any information on it then you could either let HijackThis create a backup or use BHODemon to disable it. That way it can easily be re-enabled..

- **O3 - Internet Explorer toolbars**

Example-

O3 - Toolbar: GameBar - {4E7BD74F-2B8D-469E-C0FF-FD69B994BD7D} - C:\PROGRA~1\GAMERI~1\GameBar\gamebar.dll (file missing)
O3 - Toolbar: Norton AntiVirus - {42CDD1BF-3FFB-4238-8AD1-7859DF00B1D6} - C:\Program Files\Norton SystemWorks\Norton AntiVirus\NavShExt.dll





Researching Items-

See **o2 - Browser Helper Objects** items above

Special cases-

- **O4 - Autoloading programs from Registry**

Start-up Applications, Do You Really Need All Of Them?

Example-

O4 - HKLM\..\Run: [ccRegVfy] C:\Program Files\Common Files\Symantec Shared\ccRegVfy.exe
O4 - HKLM\..\Run: [ccApp] C:\Program Files\Common Files\Symantec Shared\ccApp.exe
O4 - HKLM\..\Run: [IST Service] C:\Program Files\ISTsvc\istsvc.exe

Researching Items-

Programs that run at startup

These startup items can be looked up in one of the following databases to determine whether they are good or bad.
If they are indicated as being bad then have HijackThis fix them.

Online Databases-

windowsstartup.com
sysinfo.org
http://computercops.biz/StartupList.html (most up to date)

Offline Databases-
http://www.pacs-portal.co.uk/startup_content.php#THE_PROGRAMS

If you are unable to find the item in the above databases then search for the file name at www.google.com

Special cases-

Peper:

Example of peper- O4 - HKLM\..\Run: [338Y@QN2L8LD3#] C:\WINNT\System32\Djp9g.exe

with a [**random** 14 chars] and a **random** named .exe

Removal tool-

http://downloads.subratam.org/PeperFix.exe

- **O5 - IE Options icon not visible in Control Panel**

Example-

O5 - control.ini: Desk.cpl=no

Researching Items-

If you or your administrator did not put these restrictions then have HijackThis fix them.

Special cases-

- **O6 - IE Options access restricted by Administrator**

Example-

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

Researching Items-

If you (e.g. with Spybot S&D) or your administrator did not put these restrictions then have HijackThis fix them.

Special cases-

- **O7 - Regedit access restricted by Administrator**

What is a Registry Editor?

What is the registry?

Example-

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

Researching Items-

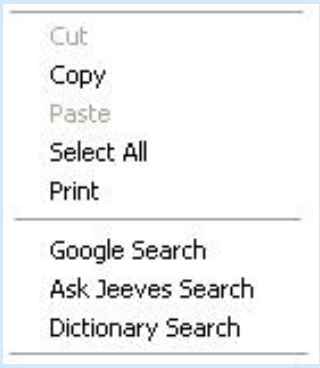
If you or your administrator did not put these restrictions in place then have HijackThis fix them.

Special cases-

- **O8 - Extra items in IE right-click menu**

Example-

O8 - Extra context menu item: &Google Search - res://C:\Program Files\Google\GoogleToolbar1.dll/cmsearch.html
O8 - Extra context menu item: Backward &Links - res://C:\Program Files\Google\GoogleToolbar1.dll/cmbacklinks.html
O8 - Extra context menu item: Cac&hed Snapshot of Page - res://C:\Program Files\Google\GoogleToolbar1.dll/cmcache.html



Researching Items-

If you do not recognise or want the item as part of Internet Explorer's right click menu then have HijackThis fix it. Look up the file name in google if unsure.

Special cases-

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

Example-

O9 - Extra button: Sidesearch (HKLM)
O9 - Extra button: ICQ Lite (HKLM)
O9 - Extra 'Tools' menuitem: ICQ Lite (HKLM)
O9 - Extra button: Related (HKLM)

Researching Items-

If you do not recognise or want the item as a button on the toolbar in Internet Explorer then have HijackThis fix it.

Look up the file name at http://www.castlecops.com/O9.html or on google if unsure.

Special cases-

- **O10 - Winsock hijacker**

What is Winsock?

Example-

O10 - Hijacked Internet access by WebHancer
O10 - Hijacked Internet access by New.Net

Researching Items-

DON'T fix these with HijackThis.

Check the file name against this list-

http://computercops.biz/LSPs.html

If the file name is listed under "Valid LSP's" then the item is safe. (indicated by a letter V in the state column)

If the file name is listed under "Malware LSP's" use LSPFix from here- http://www.cexx.org/lspfix.htm

or you are unable to find it in the list then I would recommend asking in the forum for further instructions.

Warning: Fixing these in Hijackthis or attempting to fix the wrong items by other methods will break your internet

connection.

Special cases-

New.net

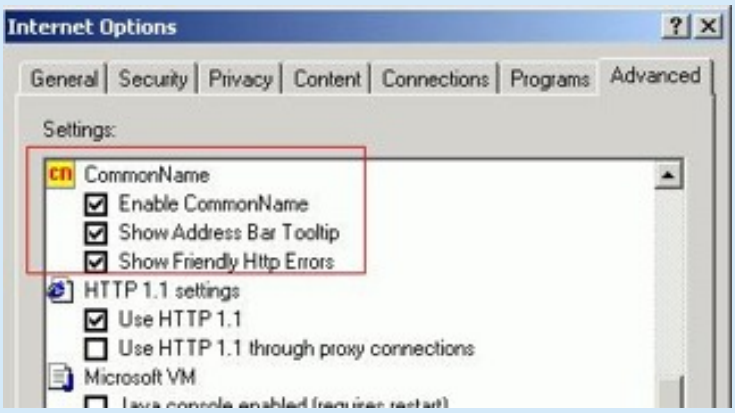
DON'T Fix these with HijackThis or any other software, New.net must be uninstalled from add/remove programs in control panel.

O10 - Hijacked Internet access by New.Net
O10 - Hijacked Internet access by New.Net
O10 - Hijacked Internet access by New.Net

- **O11 - Extra group in IE 'Advanced Options' window**

Example-

O11 - Options group: [CommonName] CommonName



Researching Items-

Always have HijackThis Fix these items

Special cases-

- **O12 - IE plugins**

What is a plugin?

Example-

O12 - Plugin for .mid: C:\Program Files\Internet Explorer\PLUGINS\npqtplugin2.dll
O12 - Plugin for .pdf: C:\Program Files\Internet Explorer\PLUGINS\nppdf32.dll
O12 - Plugin for .spop: C:\Program Files\Internet Explorer\Plugins\NPDocBox.dll

Researching Items-

Mostly safe. Fix items with **.ofb** in. Look up the file name in google if unsure.

Special cases-

- ## O13 - IE DefaultPrefix hijack

What is a default Prefix?

Example-

O13 - DefaultPrefix: http://www.pixpox.com/cgi-bin/click.pl?url=
O13 - WWW Prefix: http://prolivation.com/cgi-bin/r.cgi?

Researching Items-

Always have HijackThis Fix these items

Special cases-

- ## O14 - 'Reset Web Settings' hijack

Example-

O14 - IERESET.INF: START_PAGE_URL=http://www.freeserve.com/

Researching Items-

This file (IERESET.INF) contains the default setting for internet explorer.

If you don't recognise the URL, it's not your ISP or computer vendor , Have HijackThis fix it.

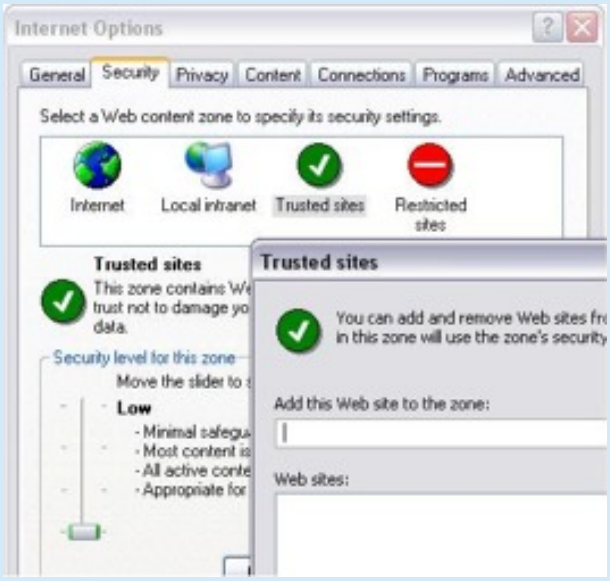
Special cases-

- ## O15 - Unwanted site in Trusted Zone

What are Security Zones?

Example-

O15 - Trusted Zone: http://Download.windowsupdate.com



Researching Items-

The websites added to this zone have very low browser security settings when they are visited. If you never added these to your trusted zone in internet explorer or don't recognise the address then have hijackthis fix them.

Special cases-

- **O16 - ActiveX Objects (aka Downloaded Program Files)**

What are Activex Objects?

Example-

O16 - DPF: {018B7EC3-EECA-11D3-8E71-0000E82C6C0D} (Installer Class) - http://www.xxxtoolbar.com/ist/softwares/v3.0/0006.cab
O16 - DPF: {166B1BCA-3F9C-11CF-8075-444553540000} (Shockwave ActiveX Control) - http://download.macromedia.com/pub/...director/sw.cab
O16 - DPF: {8522F9B3-38C5-4AA4-AE40-7401F1BBC851} - http://216.65.38.226/Download_Plugin.exe
O16 - DPF: {9F1C11AA-197B-4942-BA54-47A8489BB47F} (Update Class) - http://v4.windowsupdate.microsoft.c...7861.7822106481

Researching Items-

Download SpywareBlaster from here- http://www.javacoolsoftware.com/downloads.html

Install it and update it. Under "Protection" click on the "Internet Explorer" tab. There will be a long list there of activeX objects. Right Click on this list and click "Find".

A search window will open. Copy the CLSID e.g. {018B7EC3-EECA-11D3-8E71-0000E82C6C0D}into the the search box. Click "OK" and if the item is found, it will be highlighted. If the item is found then have HijackThis fix it. Also, if you do not recognise the name then have HijackThis fix it.

Special cases-

- **O17 - Lop.com domain hijackers**

Example-

O17 - HKLM\System\CCS\Services\Tcpip\..\{4F90B52F-13D0-4D97-8C56-CBFE7CDC0A07}: NameServer = 198.6.1.218 198.6.100.218

Researching Items-

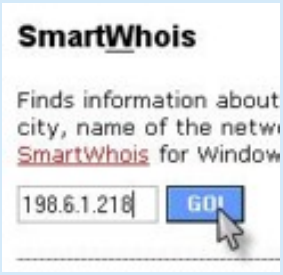
If domain is your ISP then leave it. Or, if this is your (home or company) network address then leave it.

Here are the known good (safe) ranges for DNS servers. They are reserved exclusively for networks behind NAT. If the IP address is within these ranges then it is safe.

Private IP Address Ranges

From	To
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

If the domain is in the form of an IP address e.g. **198.6.1.218** then got to http://www.all-nettools.com/toolbox and under "Smart Whois" enter the address



Click Go and it will bring up information about who owns that IP.

Special cases-

- **O18 - Extra protocols and protocol hijackers**

Example-

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

Researching Items-

These can be looked up here-

http://www.castlecops.com/O18.html

Special cases-

- **O19 - User style sheet hijack**

What is a user style sheet?

Example-

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

Researching Items-

Unless you have set up a user style sheet then have HijackThis fix it. You may also need to run CWShredder.

Special cases-

- **O20 (AppInit_DLLs and Winlogon Notify)**

These can be looked up here-

http://www.castlecops.com/O20.html

- **O21 (ShellServiceObjectDelayLoad)**

These can be looked up here-

http://www.castlecops.com/O21.html

- **O22 (Shared Task Scheduler)**

These can be looked up here-

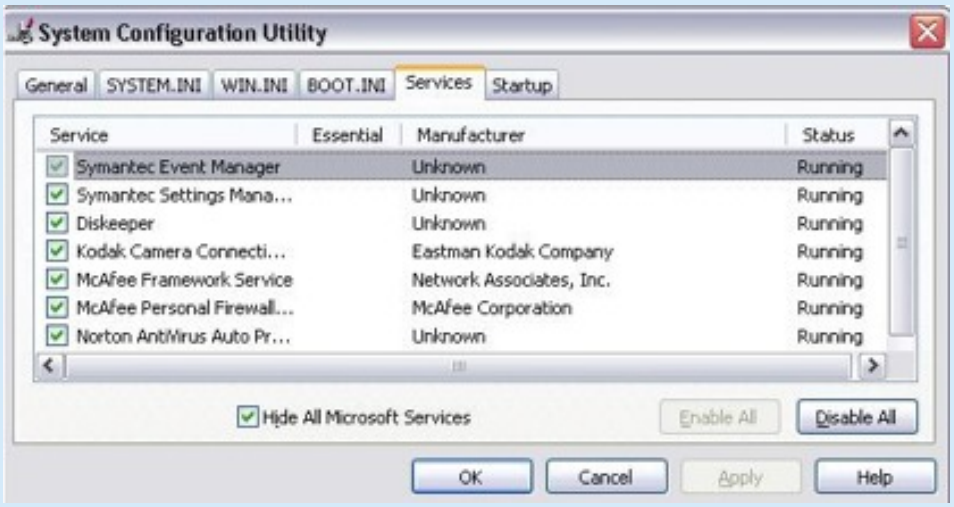
http://www.castlecops.com/O22.html

- **O23 - NT Services**

Example-

O23 - Service: **AOL Connectivity Service - America Online, Inc.** - C:\PROGRA~1\COMMON~1\AOL\ACS**AOLacsd.**

exe
O23 - Service: **Diskeeper - Executive Software International, Inc.** - C:\Program Files\Executive Software\DiskeeperLite**DKService.exe**
O23 - Service: **LexBce Server - Lexmark International, Inc.** - C:\WINDOWS\system32**LEXBCES.EXE**
O23 - Service: **McAfee.com McShield - Unknown** - c:\PROGRA~1\mcafee.com\vso**mcshield.exe**



Researching Items-

This section of the log shows all non-Microsoft services that are set to run automatically (it does not include the ones that are disabled). You will recognise some of these just by looking at the name of the service. Unlike the 04 start-up items, services will run as soon as windows starts (before a user logs on). Be very careful when disabling a service. Make sure the service is definitely bad before fixing it with HijackThis.

These items can be researched here-

http://www.castlecops.com/O23.html
