OTL is a flexible, multipurpose, diagnostic, and malware removal tool. It also has some curative ability.

****

Introduction

Donation Information

OTL is FREE. However, it is the result of significant investments of time and effort by OldTimer. The program contains many thousands of lines of code, and is updated often as malware changes. OldTimer also spends countless hours offering support to forum helpers and their malware victims. If you find his OTL tool helpful, and would like to support his efforts, buy him a cup of coffee. Or, simply click the Paypal button below:

Tutorial Information

This tutorial has been created by and is the property of emeraldnzl. Please contact emeraldnzl prior to quoting from this tutorial, to obtain permission for using it at other sites, and for information on any pending updates. Also note this tutorial was originally authored to offer guidance to helpers offering malware removal assistance at various forums.

Note: This is the master copy of the OTL Tutorial. If hosting this tutorial by permission at another site check the date at the bottom to verify that you have the latest version. These tools are constantly being updated.

Important note!: While OTL is primarily a diagnostic tool, it has advanced removal abilities. If you don't understand the instructions in this guide, please seek assistance from an expert listed in one of the forums below. Use special caution when creating any scripts. Improper use can result in data loss, or an unbootable system.

Translations

This OTL tutorial is offered in mutiple languages (links may leave this site).
English:

- GeeksToGo

French:

- Assiste

Table of contents

10. O2 Browser Helper Objects
11. O3 Internet Explorer Toolbars
12. O4 Automatic Start up Entries
13. O6 Local Machine Policies
14. O7 User Policies
15. O8 Internet Explorer Context Menu
16. O9 Internet Explorer buttons/Tools menu
17. O10 Layered Service Providers
18. O12 Internet Explorer Plugins
19. O13 Internet Explorer Default prefix
20. O15 Internet Explorer Trusted Zones
21. O16 ActiveX objects
22. O17 Transmission Control Protocol
23. O18 Extra Protocols
24. O19 User Style Sheet
25. O20 AppInit_Dills/Winlogon Notify
26. O21 ShellServicObjectDelayLoad
27. O22 SharedTaskScheduler
28. O24 Windows Active Desktop Components
29. O27 Image File Execution Options
30. O28 Shell Execute Hooks
31. O29 Security Providers
32. O30 Lsa
33. O31 SafeBoot
34. O32 Autorun files on drives
35. O33 MountPoints2
36. O34 BootExecute
37. O35 shell spawning values
38. O36 appcert dlls
39. O37 file associations
40. O38 session manager\subsystems

6. Pre-defined Custom Scan Command Example
7. Custom Scans - Standalone Commands
8. Quick Reference of available Directives & Commands
    1. :processes
    2. :OTL
    3. :Services
    4. :Reg
    5. :Files
    6. :Commands
9. Switches
10. Commands/Switches
11. CleanUp

What it will work with

OTL has 32bit and 64bit functionality. It will work with all Windows OS NT and later, that is, Operating Systems from 2000 through to Windows 7.

It does not work with Windows 9x machines.

Diagnosis

Generally OTL is used as an initial diagnosis tool at the start of a problem analysis. It is helpful not only in the identification of malware but also in telling you some useful information about the user's computer. However, especially when another tool (for example ComboFix) has been used as a starter, it can be used as a follow up tool to add to the understanding of a machine's infection and allow for fixes that might otherwise be risky or onerous in their preparation and application. One of OTL's greatest strengths is its ability to perform custom scans for any files or registry data. As malware continues to find new ways to infect systems, OTL is not required to be updated to identify it. Simply implementing a new custom scan for the specific information needed is all that is required. You can see where this is currently being utilized in the G2G Malware and Spyware Cleaning Guide. As the malware runs its course, if it becomes obsolete and is no longer a threat, the custom scans can be removed and new ones implemented if necessary. Many user's develop their own lists of custom scans to deliver the exact information that they wish to see regarding a system.

Fixes

OTL has a wide range of directives that can be used both to manipulate the computer's processes and to fix problems you have identified.

In addition there are a number of switches that can be used both for diagnostic purposes and for malware removal.

Cleanup

OTL has a CleanUp feature that will automatically remove many of the tools that are commonly used in malware removal from the user's machine. This function can be used in conjunction with your prevention speech.

Preparation for use

Nowadays malware will often interfere with the tools we use. Like many other tools OTL.exe can be renamed to say OTL.com if malware has blocked the exe name.

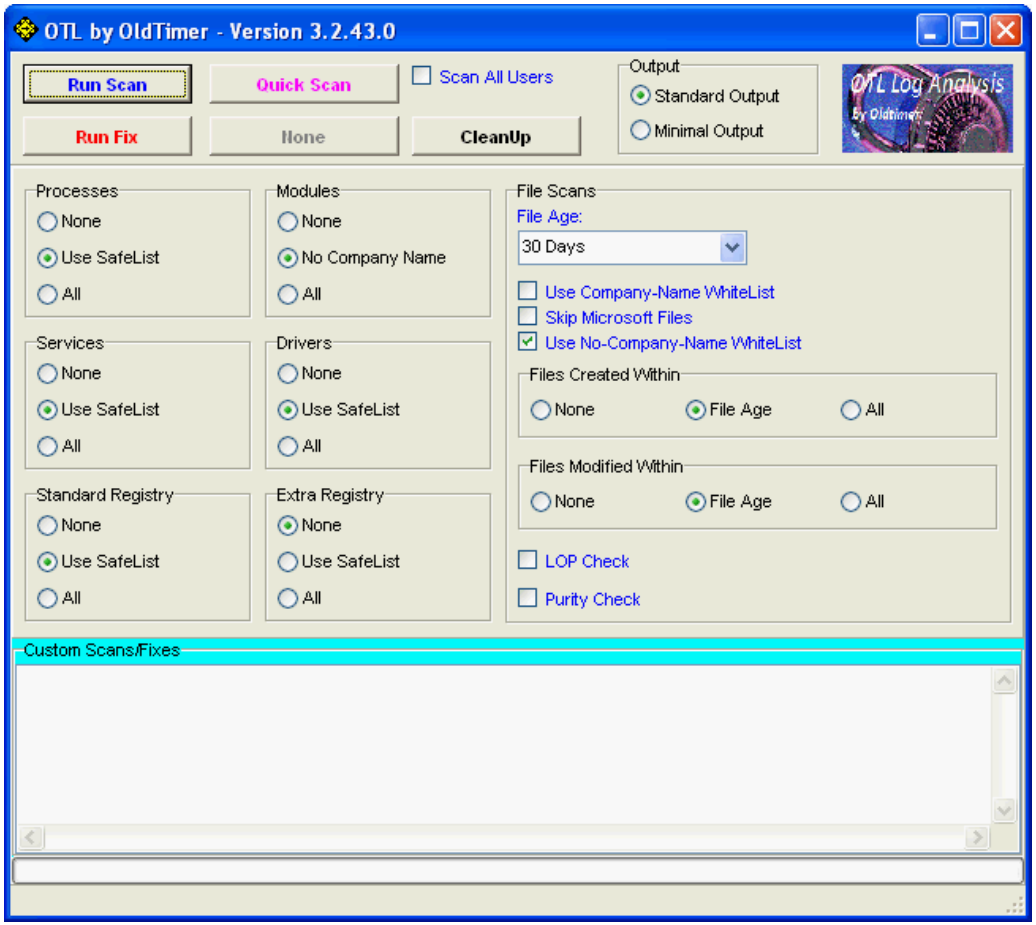
OTL does not create a backup so unless ERUNT or another backup program is in use you are relying on System Restore if a problem develops. With the types of infections prevalent nowadays it is wise to have a fall back position. Installation of the Recovery Console is recommended.

You do not need to tell the user to turn wordwrap off in Notepad. OTL will do that for them. If wordwrap is on, it will be reset to its original setting when you do the cleanup but you need to use OTL's cleanup function.

Running OTL

User is instructed to download OTL to the desktop. From there it is a simple matter to double click the OTL icon to run it. OTL icon looks like this

Once OTL is opened the user is presented with a console looking like this:



Looking at an example canned below you will see how the user can configure OTL to carry out the scans that a forum helper wants:

CODE

- Download OTL to your desktop.
- Double click on the icon to run it. Make sure all other windows are closed to let it run uninterrupted.
- When the window appears, underneath Output at the top change it to Minimal Output.
- Under the Standard Registry box change it to All.
- Check the boxes beside LOP Check and Purity Check.
- Click the Run Scan button. Do not change any settings unless otherwise told to do so. The scan wont take long.
  - When the scan completes, it will open two notepad windows. OTL.Txt and Extras.Txt. These are saved in the same location as OTL.
  - Please copy (Edit->Select All, Edit->Copy) the contents of these files, one at a time, and post it with your next reply.

Once OTL has completed its first scan it will save notepad copies of the scans in the folder that OTL was started from. Unless set to produce an Extras log it will only produce OTL.txt in subsequent scans.

A copy of an OTL fix log is saved in a text file at

- :_OTL\MovedFiles
  in most cases this will be C:_OTL\MovedFiles

Download Links

Direct Download Links

Download links. The latest version of OTL can be downloaded from http://oldtimer.geekstogo.com/OTL.exe or www.itxassociates.com/OT-Tools/OTL.exe

In addition, for users that cannot run executables. You can now download OTL either as a .com, or a .scr file.

Links:
http://oldtimer.geekstogo.com/OTL.com
http://oldtimer.geekstogo.com/OTL.scr

or:
www.itxassociates.com/OT-Tools/OTL.com
www.itxassociates.com/OT-Tools/OTL.scr

Note: When using these links, use Internet Explorer to download. If using Firefox, you should right-click and use "Save link As". Otherwise, on some systems, FF attempts to open the file as a script and just a bunch of gibberish is displayed.

Output

Header

Here is an example of a header:

> OTL logfile created on: 23/02/2011 9:51:56 a.m. - Run 1
> OTL by OldTimer - Version 3.2.21.0 Folder = C:\Users\Anyone\Desktop
> 64bit- An unknown product (Version = 6.1.7600) - Type = NTWorkstation
> Internet Explorer (Version = 8.0.7600.16385)
> Locale: 00001409 | Country: New Zealand | Language: ENZ | Date Format: d/MM/yyyy
>
> 4.00 Gb Total Physical Memory | 3.00 Gb Available Physical Memory | 73.00% Memory free
> 8.00 Gb Paging File | 7.00 Gb Available in Paging File | 86.00% Paging File free
> Paging file location(s): ?:\pagefile.sys [binary data]
>
> %SystemDrive% = C: | %SystemRoot% = C:\Windows | %ProgramFiles% = C:\Program Files (x86)
> Drive C: | 200.00 Gb Total Space | 91.76 Gb Free Space | 45.88% Space Free | Partition Type: NTFS
> Drive D: | 265.75 Gb Total Space | 241.65 Gb Free Space | 90.93% Space Free | Partition Type: NTFS
>
> Computer Name: Anyone-PC | User Name: Anyone | Logged in as Administrator.
> Boot Mode: Normal | Scan Mode: Current user | Include 64bit Scans
> Company Name Whitelist: Off | Skip Microsoft Files: Off | No Company Name Whitelist: On | File Age = 30 Days

A proper perusal of this information can save you time in the long run.

Description by line

First line: tells you what date the log was created on, what time of day and what run it was.

Note: the date will be shown in the format set by the user in Control Panel.

Sometimes a user will mistakenly post an old log. The information in this line will alert you to that.

Second line: shows you the version number and where OTL has been saved to. The version number is particularly important. An old version may not have the most up to date functionality and may lead you to the wrong conclusion when assessing a log. Equally the location may be relevant, particularly if it is saved somewhere other than the desktop.

Third line: shows you the version of Windows that is on the machine, also the type of file system. Very helpful when determining whether other tools you might use are compatible with the user's computer.

Fourth line: gives you the version of Internet Explorer. IE8 can cause problems on some machines.

Fifth line: tells you the country, language and date format the OS is using. Can be useful in preparing replies. The TLA (three letter acronym) ENA in the example represents English New Zealand.

Sixth line: tells you the amount of RAM the machine can access together with the available physical memory and free memory. Often this can help explain a machines symptoms.

Note: The number shown may not reflect the hardware position the user believes is there. RAM reported may appear lower than what is actually on the machine. This can happen when the machine can't actually access all the RAM it has. Possibilities include faulty RAM or Motherboard slot problem or something preventing the BIOS recognising it (e.g. BIOS may need to be upgraded). Also, for 32 bit systems with more than 4GB of ram installed, the maximum amount reported will only be 4GB. This is a limitation on 32-bit applications.

Seventh & eighth lines: Paging file size and paging file space available then Paging file location(s) and how much data is in pagefile.sys. These two lines may alert you to problems with memory allocation.

Note: One thing you might see is the figure reported in the log as larger than what it is on disk. This is because the amount shown in the log is the maximum amount that Windows will/can increase it to if needed.

Ninth line : tells you where the systems drive is operating from, where system root is located and where the program files are working from.

The next few lines: tell you what drives are on the machine, their size, how much free space there is. Whether the disk is partitioned and what type it is. This can be important. You might find a situation where very little free space remains on a hard drive (under 15% free is less than optimum). This can impact on the ability of tools to run. If free space is very low, say under 5%, then there is a chance that the computer will become unbootable when you run a tool. OTL will only report drive information for drives that are present and loaded with media.

The next line tells you the name of the computer, the current user and what level they are logged in as. This can alert you to whether the user has the appropriate permission rights.

Following that there is another group of lines that tell you the boot mode of the computer, whether only the current user settings or all the settings for all users have been included, whether 64-bit scans were included (on 64-bit OSs only), whether or not the Company Name Whitelist was used, whether or not all MS Files have been filtered out of the output and the file age (how many days back have been picked up in the scan) shown in the log.

OTL adds notations to certain log entries:

[2008/01/20 21:52:15 | 01,216,000 | ---- | M - the last character inside the brackets will either be M or C standing for Created or Modified.

All of the scans except the Files Created scan and the Files Created No Company Name scans will show the last modified date of the files. The two Created scans will show the file or folder's created date. A lot of malware will adjust the modified date to try and hide or blend in with other files or folders so seeing the created date helps in determining potential malware. If the file or folders shows a modified date in 2003 but was created in 2010 then it is an indication that it should be looked at a bit more closely. Look at the created scans very closely because they tend to quickly point out malware.

[2010/03/15 18:25:02 | 1609,916,416 | -HS- | M] () -- C:\hiberfil.sys - the four designators after the file size can be RHSD and stand for:

R - Readonly
H - Hidden

S - System
D - Directory

SRV - (NMSAccessU) -- C:\Program Files (x86)\CDBurnerXP\NMSAccessU.exe () - denotes that there is not a company name. The company name will appear inside the trailing parenthesis. Most malware will not have a company name (but some put one in there in an attempt to hide) but not all files without a company name are bad as this example shows.

[2009/03/10 15:54:00 | 00,000,000 | ---D | M - this shows a Directory (D) that was Modified (M) on 2009/03/10.
In this case the example is a Directory and the date shown is the Modified date.

Directories will always have a file size of zero as this example shows. If it was a file then there would not be a D in that portion and the size of the file would normally be greater than zero although you may find files with a zero size as well, but in that case there still would not be a D value there. In this case the example is a Directory and the date shown is the modified date.

Standard Scan Areas

PRC - Processes
MOD - Modules
SRV - Services
DRV - Drivers
Standard Registry
IE - Internet Explorer Settings
FF - FireFox Settings
CHR - Chrome Settings
O1 Hosts File
O2 Browser Helper Objects
O3 Internet Explorer Toolbars
O4 Automatic Start up Entries
O6 Local Machine Policies
O7 User Policies
O8 Internet Explorer Context Menu
O9 Internet Explorer buttons/Tools menu
O10 Layered Service Providers
O12 Internet Explorer Plugins
O13 Internet Explorer Default prefix
O15 Internet Explorer Trusted Zones
O16 ActiveX objects
O17 Transmission Control Protocol
O18 Extra Protocols
O19 User Style Sheet
O20 AppInit_Dills/Winlogon Notify
O21 ShellServicObjectDelayLoad
O22 SharedTaskScheduler
O24 Windows Active Desktop Components
O27 Image File Execution Options
O28 Shell Execute Hooks
O29 Security Providers
O30 Lsa
O31 SafeBoot
O32 Autorun files on drives
O33 MountPoints2
O34 BootExecute
O35 - .com and .exe shell spawning values

O36 appcert dlls
O37 file associations (for .com and .exe shell spawning values)
O38 session manager\subsystems

Files/Folder scans

Extra Registry - separate log automatically run on first OTL scan. Carries out the following scans and places the output in the Extras.txt log. This will only be automatically run the first time an OTL.exe scan is performed. After that, if you want to see this output you will need to instruct the user to select either the Use SafeList or All option in the Extra Registry group before performing the next scan:

File Associations
Shell Spawning
Security Center
Authorized Applications (if running on a non-Vista OS)
Vista Firewall Rules (if running on a Vista or above OS)
Uninstall List
Event Viewer (last 10 error messages in each Event Viewer log)

There are two ways that you can ask the topic starter for the Standard Scans to be presented, Standard Output or Minimal Output (selected on the toolbar). Further you can use the SafeList (default option) or All option for all of the Standard Scans (selected within the particular scan group).

Note: With the Standard output the file date\times are included at the beginning of the line while with the Minimal output only the file name/path and company name are included. For the Processes, Modules, Services, Drivers, and File scans the output will be sorted by file date, but with any custom scans the output will be sorted by location and file name. On 64-bit OSs, the 64-bit items will be listed first in the output with the 32-bit items afterward within the grouping.

The Safe List is a list of 600+ (currently) Microsoft files that are deemed safe which will be filtered out of all scans if the scan includes a Safe List option and that option is chosen for the scan. Choosing the All option for any of these scans will turn the filter off and the output will include all items for that scan.

Note 2: You can customize the scanning options however you want to meet your specific needs. For example, you might want to set the Processes and Modules scans to None and the File Age setting to 180 days. If you do change any of the settings from the default settings then make sure that the ***Run Scan****button is used. When the Quick Scan button is pressed a set of pre-defined settings will be applied, overriding any currently set settings. The Quick Scan settings cannot be overridden. Any custom items in the Custom Scans/Fixes area will not be affected by either the Run Scan or Quick Scan selection. These items will always be run if present.*

There are also some additional pre-defined custom commands that can be used in Custom Scans:

Note: Except for the HijackThisBackups command, any of the output from these scans can be copy/pasted directly into the :OTL section of a fix for removal.

hijackthisbackups - lists all the HJT backups
netsvcs - lists entries under HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost - netsvcs
msconfig - lists entries under HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig
safebootminimal - lists entries under HKEY_LOCAL_MACHINE\system\currentcontrolset\control\safeboot\Minimal
safebootnetwork - lists entries under HKEY_LOCAL_MACHINE\system\currentcontrolset\control\safeboot\Network
activex - lists entries under HKEY_LOCAL_MACHINE\software\microsoft\active setup\installed components
drivers32 - lists entries under HKEY_LOCAL_MACHINE\software\Microsoft\Windows NT\CurrentVersion\Drivers32

Note: by default, each of the above pre-defined scans will use the SafeList to filter out known good files. To override this action and include all files in any of these scans include a ***/ALL*** *switch at the end of the command (Example: netsvcs /all).*

SaveMBR - saves a physical drive's MBR to a file named PhysicalMBR.bin in the root of the system drive. It works on 32- and 64-bit OS's.This is how it works.

SaveMBR:n

where n is the physical drive to use. For most systems this will be SaveMBR:0 for the first (and usually only) physical drive. If there are multiple physical drives then change n to the appropriate boot drive. This has nothing to do with the logical drives (C:, D:, E:, etc).

A copy of the mbr will be saved at:

<SystemDrive>:\PhysicalMBR.bin

in most cases this will be C:\PhysicalMBR.bin

You can then have the file submitted to a malware scanning site for checking.

Example Output

Processes

Shows processes running on the machine.

========== Processes (SafeList) ==========

Standard:
PRC - [2009/11/11 00:03:54 | 00,529,408 | ---- | M] (OldTimer Tools) -- C:\OldTimer Tools\OTL.exe

Minimal:
PRC - C:\OldTimer Tools\OTL.exe (OldTimer Tools)

Modules

Shows kernal modules running on the machine.

========== Modules (SafeList) ==========

Standard:
MOD - [2009/04/28 10:05:56 | 00,715,264 | ---- | M] (Agnitum Ltd.) -- c:\Program Files\Agnitum\Outpost Firewall\wl_hook.dll

Minimal:
MOD - c:\Program Files\Agnitum\Outpost Firewall\wl_hook.dll (Agnitum Ltd.)

Services

Shows services running on the machine.

========== Win32 Services (SafeList) ==========

Standard:
SRV:64bit: - [2008/01/20 21:52:15 | 01,216,000 | ---- | M] (Microsoft Corporation) -- C:\Program Files\Windows Media Player\wmpnetwk.exe -- (WMPNetworkSvc)
SRV - [2009/09/06 12:38:06 | 00,071,096 | ---- | M] () -- C:\Program Files (x86)\CDBurnerXP\NMSAccessU.exe -- (NMSAccessU)

Minimal:
SRV:64bit: - (WMPNetworkSvc) -- C:\Program Files\Windows Media Player\wmpnetwk.exe (Microsoft Corporation)
SRV - (NMSAccessU) -- C:\Program Files (x86)\CDBurnerXP\NMSAccessU.exe ()

Drivers

Shows drivers running on the machine.

========== Driver Services (SafeList) ==========

Standard:
DRV:64bit: - [2009/02/10 16:14:00 | 00,399,384 | ---- | M] (Agnitum Ltd.) -- C:\Windows\SysNative\drivers\afwcore.sys -- (afwcore)
DRV - [2009/09/28 20:57:28 | 00,007,168 | ---- | M] () -- C:\Windows\SysWOW64\drivers\StarOpen.sys -- (StarOpen)

Minimal:
DRV:64bit: - (afwcore) -- C:\Windows\SysNative\drivers\afwcore.sys (Agnitum Ltd.)
DRV - (StarOpen) -- C:\Windows\SysWOW64\drivers\StarOpen.sys ()

Standard Registry

========== Standard Registry (SafeList) ==========

Internet Explorer

========== Internet Explorer ==========

This section shows a selection of browser internet settings from a number of versions of IE.

IE:64bit: - HKLM\..\SearchScopes,DefaultScope = {0633EE93-D776-472f-A0FF-E1416B8B2E3A}
IE:64bit: - HKLM\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/...ms}&FORM=IE8SRC
IE - HKLM\..\SearchScopes,DefaultScope = {0633EE93-D776-472f-A0FF-E1416B8B2E3A}
IE - HKLM\..\SearchScopes\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}: "URL" = http://www.bing.com/...ms}&FORM=IE8SRC
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SysWOW64\blank.htm
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft....k/?LinkId=69157
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft....k/?LinkId=54896
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Secondary_Page_URL = [binary data]
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Extensions Off Page = about:NoAdd-ons
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page =
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft....k/?LinkId=54896
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Security Risk Page = about:SecurityRisk
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://www.microsoft...p...ER}&ar=home
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Search,CustomizeSearch = http://ie.search.msn...st/srchcust.htm
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Search,CustomSearch = http://uk.red.client...fo/bt_side.html
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Search,Default_Search_URL = http://www.microsoft...amp;ar=iesearch
IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Search,SearchAssistant = http://ie.search.msn...st/srchasst.htm
IE - URLSearchHook: {18944614-1340-4483-bac9-6778840b9970} - C:\Program Files\TalkTalk Mail Toolbar\talktalkmailtb.dll (AOL LLC.)

IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Search_URL = http://www.google.com/ie
IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page =
IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Page_Transitions = 1
IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://www.google.com
IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://www.aol.co.uk/talktalk
IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Search,Default_Search_URL = http://www.google.com/ie
IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Search,SearchAssistant = http://www.google.com/ie
IE - URLSearchHook: {18944614-1340-4483-bac9-6778840b9970} - C:\Program Files\TalkTalk Mail Toolbar\talktalkmailtb.dll (AOL LLC.)
IE - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0
IE - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyOverride" = *.local

IE - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyServer" = 0.0.0.0:80

Looking at some items from the above example we see:

- IE:64bit: - HKLM\..\SearchScopes,DefaultScope = {0633EE93-D776-472f-A0FF-E1416B8B2E3A}
  - IE default main search engine Bing

    An example list of good, questionable and bad (with search providers) shows the following GUID's:
    > {0633EE93-D776-472f-A0FF-E1416B8B2E3A} - Live Search or nowadays Bing
    > {84CBB9A2-6089-4BC9-91DB-B948E1907E8B} - Google
    > {DEA6C301-90B8-4B12-9C32-2A9935D739EE} - Yahoo
    > {6A1806CD-94D4-4689-BA73-E35EA1EA9990} - Ask (questionable... may be foistware)
    > {56256A51-B582-467e-B8D4-7786EDA79AE0} - MyWebSearch - Adware MyWebSearch

- IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft....k/?LinkId=54896
  - IE default main search engine Bing

- IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft....k/?LinkId=69157
  - IE main default page MSN

- IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft....k/?LinkId=54896
  - IE default main search engine Bing

- IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Extensions Off Page = about:NoAdd-ons
  - One of the lesser known features of Internet Explorer 7 is the "No Add Ons" mode. This page is used when No Add Ons mode is in operation.

- IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Local Page =
  - local page is blank. Another setting looks like this =C:\WINDOWS\System32\blank.htm

- IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Main,Security Risk Page = about:SecurityRisk
  - Informs the user not to browse with the current security settings because they may be harmful to the computer. See here for a list of common about: addresses

- IE - HKLM\SOFTWARE\Microsoft\Internet Explorer\Search,CustomSearch = http://uk.red.client...fo/bt_side.html
  - Yahoo web page
    - related to Yahoo BHO

- IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Start Page = http://www.aol.co.uk/talktalk
  - indicates the default home page

- IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Main,Search Page = http://www.google.com
  - Google is set as a main search page

- IE - HKCU\SOFTWARE\Microsoft\Internet Explorer\Search,Default_Search_URL = http://www.google.com/ie
  - indicates Google.com/ie set as a default search engine

Proxy settings.

- IE - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyEnable" = 0
  - = 0 indicates the proxy server is disabled (set value of 'ProxyEnable' equal to '1' for proxy enabled or '0' for disabled)

- IE - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyOverride" = *.local
  - indicates that Internet Explorer will not use the proxy for all internal network addresses

- IE - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings: "ProxyServer" = 0.0.0.0:80
  - Is not a regular IP but 0.0.0.0 means "every IP that the computer provides". It listens on the loopback (127.0.0.1) as well as the internal network address. Many AV applications create a proxy server to filter outgoing mail through.

Note *See instruction about to how to remove items from IE in the* ***:OTL*** *section under* ***Quick Reference of available Directives & Commands for fixes*** *below.*

Firefox

========== FireFox ==========

This area shows the Firefox browser internet settings.

FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0007-ABCDEFFEDCBA}:6.0.07
FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0012-ABCDEFFEDCBA}:6.0.12
FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0013-ABCDEFFEDCBA}:6.0.13
FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0014-ABCDEFFEDCBA}:6.0.14
FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0015-ABCDEFFEDCBA}:6.0.15
FF - prefs.js..extensions.enabledItems: jqs@sun.com:1.0
FF - prefs.js..extensions.enabledItems: {20a82645-c095-46ed-80e3-08825760534b}:1.1
FF - prefs.js..extensions.enabledItems: {ABDE892B-13A8-4d1b-88E6-365A6E755758}:1.0
FF - prefs.js..extensions.enabledItems: {B13721C7-F507-4982-B2E5-502A71474FED}:2.2.0.102
FF - prefs.js..extensions.enabledItems: {972ce4c6-7e08-4474-a285-3208198ce6fd}:3.0.14
FF - prefs.js..network.proxy.no_proxies_on: "localhost"

FF - HKLM\software\mozilla\Firefox\Extensions\\{20a82645-c095-46ed-80e3-08825760534b}: c:\WINDOWS\Microsoft.NET\Framework\v3.5\Windows Presentation Foundation\DotNetAssistantExtension\ [2009/06/23 22:50:00 | 00,000,000 | ---D | M]
FF - HKLM\software\mozilla\Firefox\Extensions\\jqs@sun.com: C:\Program Files\Java\jre6\lib\deploy\jqs\ff [2009/03/10 15:54:00 | 00,000,000 | ---D | M]
FF - HKLM\software\mozilla\Firefox\Extensions\\{ABDE892B-13A8-4d1b-88E6-365A6E755758}: c:\program files\real\realplayer\browserrecord\firefox\ext [2009/09/06 17:41:17 | 00,000,000 | ---D | M]
FF - HKLM\software\mozilla\Mozilla Firefox 3.0.14\extensions\\Components: C:\Program Files\Mozilla Firefox\components [2009/09/23 09:12:35 | 00,000,000 | ---D | M]
FF - HKLM\software\mozilla\Mozilla Firefox 3.0.14\extensions\\Plugins: C:\Program Files\Mozilla Firefox\plugins [2009/09/23 09:12:35 | 00,000,000 | ---D | M]
FF - HKLM\software\mozilla\Netscape Browser 8.0.3.4\Extensions\\Components: C:\Program Files\Netscape\Netscape Browser\Components [2009/09/23 09:12:35 | 00,000,000 | ---D | M]
FF - HKLM\software\mozilla\Netscape Browser 8.0.3.4\Extensions\\Plugins: C:\Program Files\Netscape\Netscape Browser\Plugins [2009/09/23 09:12:34 | 00,000,000 | ---D | M]
Taking some items from the above example we see:

- FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0007-ABCDEFFEDCBA}:6.0.07
  FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0012-ABCDEFFEDCBA}:6.0.12
  FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0013-ABCDEFFEDCBA}:6.0.13
  FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0014-ABCDEFFEDCBA}:6.0.14
  FF - prefs.js..extensions.enabledItems: {CAFEEFAC-0016-0000-0015-ABCDEFFEDCBA}:6.0.15
  - these are related to Sun's Java Console

- FF - prefs.js..extensions.enabledItems: jqs@sun.com:1.0
  - is an Add-on for Java quick starter

- FF - prefs.js..extensions.enabledItems: {20a82645-c095-46ed-80e3-08825760534b}:1.1
  - Microsofts .NET Framework Assistant for Firefox

- FF - prefs.js..extensions.enabledItems: {ABDE892B-13A8-4d1b-88E6-365A6E755758}:1.0
  - Real Player

- FF - prefs.js..extensions.enabledItems: {B13721C7-F507-4982-B2E5-502A71474FED}:2.2.0.102

- Skype

Chrome

========== Chrome ==========

This area shows the Chrome browser internet settings.

CHR - default_search_provider: Google (Enabled)
CHR - default_search_provider: search_url = {google:baseURL}search?{google:RLZ}{google:acceptedSuggestion}{google:originalQueryForSuggestion}{google:searchFieldtrialParameter}{google:instantFieldTrialGroupParameter}sourceid=chrome&ie={inputEncoding}&q={searchTerms}

CHR - default_search_provider: suggest_url = {google:baseSuggestURL}search?{google:searchFieldtrialParameter}{google:instantFieldTrialGroupParameter}client=chrome&hl={language}&q={searchTerms}
CHR - plugin: Shockwave Flash (Enabled) = C:\Documents and Settings\admin\Local Settings\Application Data\Google\Chrome\Application\14.0.835.202\gcswf32.dll
CHR - plugin: Java Deployment Toolkit 6.0.240.7 (Enabled) = C:\Program Files\Java\jre6\bin\new_plugin\npdeployJava1.dll
CHR - plugin: Java™ Platform SE 6 U24 (Enabled) = C:\Program Files\Java\jre6\bin\new_plugin\npjp2.dll
CHR - plugin: Adobe Acrobat (Disabled) = C:\Program Files\Adobe\Reader 9.0\Reader\Browser\nppdf32.dll
CHR - plugin: Silverlight Plug-In (Enabled) = c:\Program Files\Microsoft Silverlight\4.0.60531.0\npctrl.dll
CHR - plugin: Windows Media Player Plug-in Dynamic Link Library (Enabled) = C:\Program Files\Windows Media Player\npdsplay.dll
CHR - plugin: Remoting Viewer (Enabled) = internal-remoting-viewer
CHR - plugin: Native Client (Enabled) = C:\Documents and Settings\admin\Local Settings\Application Data\Google\Chrome\Application\14.0.835.202\ppGoogleNaClPluginChrome.dll
CHR - plugin: Chrome PDF Viewer (Enabled) = C:\Documents and Settings\admin\Local Settings\Application Data\Google\Chrome\Application\14.0.835.202\pdf.dll
CHR - plugin: Microsoft\u00AE DRM (Enabled) = C:\Program Files\Windows Media Player\npdrmv2.dll
CHR - plugin: Microsoft\u00AE DRM (Enabled) = C:\Program Files\Windows Media Player\npwmsdrm.dll
CHR - plugin: Facebook Plugin (Enabled) = C:\Documents and Settings\admin\Application Data\Facebook\npfbplugin_1_0_3.dll
CHR - plugin: Move Media Player 7 (Enabled) = C:\Documents and Settings\admin\Application Data\Move Networks\plugins\071802000001\npqmp071802000001.dll
CHR - plugin: Google Update (Enabled) = C:\Documents and Settings\admin\Local Settings\Application Data\Google\Update\1.3.21.69\npGoogleUpdate3.dll
CHR - plugin: RIM Handheld Application Loader (Enabled) = C:\Program Files\Common Files\Research In Motion\BBWebSLLauncher\NPWebSLLauncher.dll
CHR - plugin: Google Earth Plugin (Enabled) = C:\Program Files\Google\Google Earth\plugin\npgeplugin.dll
CHR - plugin: Windows Presentation Foundation (Enabled) = c:\WINDOWS\Microsoft.NET\Framework\v3.5\Windows Presentation Foundation\NPWPF.dll
CHR - plugin: Default Plug-in (Enabled) = default_plugin
CHR - Extension: One Piece Theme = C:\Users\Joebloggs\AppData\Local\Google\Chrome\User Data\Default\Extensions\kkhkehkllpkocgnlbkmpkcicednmbfnp\2_0\
CHR - Extension: DivX Plus Web Player HTML5 \u003Cvideo\u003E = C:\Users\Joebloggs\AppData\Local\Google\Chrome\User Data\Default\Extensions\nneajnkjbffgblleaoojgaacokifdkhm\2.1.2.126_0\

Generally speaking the listings are self explanatory however taking some items as examples we see:

- CHR - plugin: RIM Handheld Application Loader (Enabled) = C:\Program Files\Common Files\Research In Motion\BBWebSLLauncher\NPWebSLLauncher.dll
  - related to a BlackBerry handheld devices

- CHR - plugin: Remoting Viewer (Enabled) = internal-remoting-viewer
  - This remoting feature is aimed at enabling Chrome and Chrome OS users to connect to "legacy" apps, which is what Google calls desktop applications, and run them inside the browser.

- CHR - plugin: Chrome PDF Viewer (Enabled) = C:\Documents and Settings\admin\Local Settings\Application Data\Google\Chrome\Application\14.0.835.202\pdf.dll
  - Built-in PDF viewer that works inside Chrome's sandbox

Note *See instruction about to how to remove items from Chrome in the* ***:OTL*** *section under* ***Quick Reference of available Directives & Commands for fixes****below.*

O1 through to O38

GeekU students - For OTL reg points discussion GeekU students should go here.

O1 Hosts File

The Hosts File is used in an operating system to map hostnames to IP addresses. The file contains lines of text consisting of an IP address in the first text field followed by one or more hostnames. The importance from a malware viewpoint is that a hijacker may change an entry in the file to redirect an attempt to reach a particular web site to another web site chosen by the hijacker. Alternatively, a hijacker might modify the hosts file to block a connection if it exists e.g. an anti-virus update connection. If you suspect malicious activity here you can either remove individual entries under the :OTL directive or use the command [RESETHOSTS] (see under the :Commands section) to reset the Hosts File back to it's default value.

O2 Browser Helper Objects (BHO)

Browser Helper Objects (BHO) which extend the functionality of the Internet Explorer browser. Malware and Foistware makers can use this area to add their own functionality e.g. spyware. Because BHO's can be both legitimate and/or malicious, care needs to be exercised when analysing these objects. Usually if these items need fixing they will be placed under the :OTL directive.

O3 Internet Explorer Toolbars

Items related to Internet Explorer Toolbars are listed. Foistware will often add objects here.

O4 Automatic Start up Entries

A number of AutoStart entries are listed. Malware is often placed in these automatically starting keys.

O6 Local Machine Policies

Relates to registry keys for the Local Machine Policy settings. You can see how the registry entries OTL picks up (mostly under HKLM\software\microsoft\windows\currentversion\policies...) are configured. Malware can change these.

O7 User Policies

Relates to registry keys for User Policy settings.

(O8) Internet Explorer Context Menu

Lists items added to the Context Menu of Internet Explorer. Malware or Foistware may add items here. Many are legitimate though so, as always, take care in modifying or removing anything here.

O9 Internet Explorer buttons/Tools menu

Relates to additional buttons found on the Internet Explorer Toolbar or in the 'Tools' menu.

O10 Layered Service Providers (LSP)

Relates to LSP or Layered Service Providor DLLs. Malware inserted here can spy on Internet Traffic. OTL will remove the catalog entries included in the fix and then reorder the winsock stack so there won't be a broken LSP chain i.e. you can use OTL to fix these items. Care: a broken chain will prevent a machine connecting to the Internet.

O12 Internet Explorer Plugins

Lists Internet Explorer Plugins. Occasionally malware is added here.

O13 Internet Explorer Default prefix

Allows Internet Explorer to add the appropriate protocol prefix to URL when browsing. Similar behavior to adding http prefix to URLs starting with www. Malware can hijack this.

O15 Internet Explorer Trusted Zones

Lists items in the Internet Explorer Trusted Zone. Malware can add domains or IP addresses here.

O16 ActiveX objects

Lists ActiveX objects which add functionality to Internet Explorer. Many legitimate objects are here but many malicious and foistware objects can be added here also.

O17 Transmission Control Protocol (TCP)

Lists DNS (Domain Name System or Service) servers used by the computer. Occasionally you can find a malicious Domain Name here. Check the IP address before action.

O18 Extra Protocols

Lists extra protocols, handlers and filters. These can be changed by malware.

O19 User Style Sheet

Shows User Style Sheets. Malware can modify this key.

O20 AppInit_Dll's/Winlogon Notify

Lists files being loaded through AppInit_DLLs and the Winlogon Notify Subkeys.

O21 ShellServiceObjectDelayLoad

Lists files being loaded through the ShellServiceObjectDelayLoad registry key.

O22 SharedTaskScheduler

Lists files being loaded through the SharedTaskScheduler registry value.

O24 Windows Active Desktop Components

Lists Windows Active Desktop Components.

O27 Image File Execution Options

Lists items under HKey_Local_Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

Explanation here.

O28 Shell Execute Hooks

HKey_Local_Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks

These are loaded every time you launch a program (using Windows Explorer or by calling the ShellExecute(Ex) function). This startup module like the other startup DLL modules is notified of the program you launch and can perform any additional task before the the program is actually launched.

O29 Security Providers

Lists items under HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders

QUOTE O29 - HKLM SecurityProviders - (xlibgfl254.dll) - .Trashes [2008/11/03 13:08:10 | 00,000,000 | -H-D | M]
O29 - HKLM SecurityProviders - (digiwet.dll) - File not found
These are examples of bad ones. Care needs to be exercised as legitimate items will show here too.

O30 Lsa

Lists items under HKEY_LOCAL_MACHINE\system\currentcontrolset\control\lsa

QUOTE O30 - LSA: Authentication Packages - (C:\WINDOWS\system32\opnnLbaA.dll) - C:\WINDOWS\System32\opnnLbaA.dll File not found

The above is an example of a bad one.

Note: LSA items 32bit versus 64bit:

O30:64bit: - LSA: Authentication Packages - (msv1_0) - C:\Windows\SysNative\msv1_0.dll (Microsoft Corporation)
O30 - LSA: Authentication Packages - (msv1_0) - C:\Windows\SysWow64\msv1_0.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (kerberos) - C:\Windows\SysNative\kerberos.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (msv1_0) - C:\Windows\SysNative\msv1_0.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (schannel) - C:\Windows\SysNative\schannel.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (wdigest) - C:\Windows\SysNative\wdigest.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (tspkg) - C:\Windows\SysNative\tspkg.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (kerberos) - C:\Windows\SysWow64\kerberos.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (msv1_0) - C:\Windows\SysWow64\msv1_0.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (schannel) - C:\Windows\SysWow64\schannel.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (wdigest) - C:\Windows\SysWow64\wdigest.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (tspkg) - C:\Windows\SysWow64\tspkg.dll (Microsoft Corporation)

For items that are located in the HKLM\System branch of the registry, there is only one value but it will be interpreted differently by 32bit applications and 64bit applications. In the examples above you can see that the 64bit interpretations will look to files in the sysnative folder (the 64bit system32 folder) and the 32bit interpretations will look to the syswow64 folder (the 32bit system32 folder). Removing any of these items will affect both 32bit and 64bit operations. Removing one or the other matching lines will remove the item from the single registry location but will only move the file for the line selected. If you want to remove both files for matching items like these then include both in the fix. It is important to understand where items in the log are located in the registry to determine whether a single registry item is read by both 32bit and 64bit applications. What you could find in a situation like this is that the file pointed to by the 32bit interpretation is bad but the 64bit interpretation is fine (most malware only affects 32bit applications because the 64bit OS does not allow changes to its files). Since the registry value is shared by both you do not want to remove it because that could cause system issues.

Now take this example of the LSA items above:

O30:64bit: - LSA: Authentication Packages - (msv1_0) - C:\Windows\SysNative\msv1_0.dll (Microsoft Corporation)
O30 - LSA: Authentication Packages - (msv1_0) - C:\Windows\SysWow64\msv1_0.dll ()
O30:64bit: - LSA: Security Packages - (kerberos) - C:\Windows\SysNative\kerberos.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (msv1_0) - C:\Windows\SysNative\msv1_0.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (schannel) - C:\Windows\SysNative\schannel.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (wdigest) - C:\Windows\SysNative\wdigest.dll (Microsoft Corporation)
O30:64bit: - LSA: Security Packages - (tspkg) - C:\Windows\SysNative\tspkg.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (kerberos) - C:\Windows\SysWow64\kerberos.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (msv1_0) - C:\Windows\SysWow64\msv1_0.dll ()
O30 - LSA: Security Packages - (schannel) - C:\Windows\SysWow64\schannel.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (wdigest) - C:\Windows\SysWow64\wdigest.dll (Microsoft Corporation)
O30 - LSA: Security Packages - (tspkg) - C:\Windows\SysWow64\tspkg.dll (Microsoft Corporation)

In this example you can see that the msv1_0.dll file for the 32bit interpretation has been compromised. It should be a Microsoft file but in this case it has been replaced by an unknown file. In this situation you will want to only remove the file from C:\Windows\SysWow64\msv1_0.dll but NOT the registry entry. You would also need to replace the bad msv1_0.dll with a valid one because it is required for application support.

O31 SafeBoot

Lists items under HKEY_LOCAL_MACHINE\system\currentcontrolset\SafeBoot

O32 Autorun files on drives

Accessing an infected removable device such as a thumb drive or flash drive through "My Computer" (clicking on the drive) will cause that autorun.inf to run.

Depending on the AutoRun/AutoPlay settings, then, when the autoplay screen comes up on insertion; the user can be tricked into running a bad file. By clicking an icon in the "use this program to run"... dialogue, a non legitimate program added to the autorun.inf file on that drive can be run.

Some malware adds autorun.inf files to the root of all logical drives.

O33 MountPoints2

The registry key that keeps track of all USB devices that have been connected to the computer.

Lists items under HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2

O34 BootExecute

Specifies the applications, services, and commands executed during startup.

Lists items under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager

O35 shell spawning values

Lists shell spawning values for .com and .exe registry settings (no other extensions).

O35 items (like any other items in the Registry Scan) can simply be placed in the :OTL section of a fix (where the ones from the Extras log cannot).

With Win Police Pro you will see a file name instead of the "%1" %*. If you see that, include those lines in the fix.

O36 appcert dlls

Lists items under HKEY_LOCAL_MACHINE\system\currentcontrolset\control\session manager\appcertdlls key

O37 file associations (for comfile and exefile shell spawning values)

Lists file associations for shell spawning values for .com and .exe registry settings.

Shell spawning and file associations are intimately intertwined. The O35 items show the shell spawning values (comfile and exefile) and the O37 items show the file associations (.com and .exe).

You can see these values if you run the Extra Registry scan but when you don't get that then these values can be hidden. The O37 line gives you the ability to see these even when the Extras Registry scan is not run.

The file association value is a single default value that will point to the shell spawning value. It is the shell spawning value where additional executables can be set to run for specific file types through the association. For example the user's file association for .exe files should be pointing to exefile but malware can change it to point to a new spawning key which is loading a "badfile". The file should show up in the file scans, but only moving that file and not fixing the association value will create a situation where .exe files cannot run.

When fixing items here OTL will set any HKLM .com or .exe file association settings back to the defaults but delete any user's .com or .exe file association keys and always set the HKLM shell spawning settings back to normal.

Note: If the spawning key is in the user's branch of the registry, then it will always be removed automatically but you will need to remove the file separately. The file should show up in the file scans and you can take care of it there. If the spawning key shows up with Reg Error: Key error, and it is malware, then you should also include a line in the :REG section to delete it from the HKLM hive just to be safe.

Example of removing a bad value from the HKLM hive

:reg
[-hkey_local_machine\software\classes\"badfile"]

and take care of the file from the file scans or the :Files section.

O38 session manager\subsystems

Lists the values in "session manager\subsystems" key

This value deals with the za infection. It is where za changes an entry for its conserv.dll file. A clean machine will look like this:

O38 - SubSystems\\Windows: (ServerDll=winsrv:UserServerDllInitialization,3)
O38 - SubSystems\\Windows: (ServerDll=winsrv:ConServerDllInitialization,2)
O38 - SubSystems\\Windows: (ServerDll=sxssrv,4)

The example above is taken from a Win 7 machine (XP and Vista will only have the first two lines). If you see ServerDll=conserv in one of the lines you will know that za was or is present. You can fix the value by including the line in the :OTL section of a fix just like any other registry line. OTL will check the OS version and update the registry with the correct values for that OS. This will only fix the registry and you will still need to remove the conserv.dll and any other portions of the infection(s) present.

Pre-defined Custom Scan Command Example

NetSvcs

Lists entries under HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost - netsvcs

Note: Microsoft places a default list of services in this regitry value during setup. Not all of the services are necessarily installed on every machine. 'Service not found'/'File not found' entries are common.

Pay particular attention to the signatures of any files that are listed under this scan.

QUOTE NetSvcs: BtwSrv - C:\WINDOWS\System32\BtwSrv.dll (X-Ways Software Technology)
NetSvcs: 6to4 - C:\WINDOWS\System32\6to4v32.dll ()
NetSvcs: Ias - Service key not found. File not found
NetSvcs: Iprip - Service key not found. File not found
NetSvcs: Irmon - Service key not found. File not found
NetSvcs: NWCWorkstation - Service key not found. File not found
NetSvcs: Nwsapagent - Service key not found. File not found

NetSvcs: Wmi - Service key not found. File not found
NetSvcs: WmdmPmSp - Service key not found. File not found
NetSvcs: helpsvc - C:\WINDOWS\PCHealth\HelpCtr\Binaries\pchsvc.dll (Microsoft Corporation)

In the example above we see:

helpsvc - C:\WINDOWS\PCHealth\HelpCtr\Binaries\pchsvc.dll (Microsoft Corporation) This is legitimate
BtwSrv - C:\WINDOWS\System32\BtwSrv.dll (X-Ways Software Technology) This is not legitimate. Careful - while this one is bad, not all ***non*** Microsoft files are bad. Always check for authenticity.
6to4 - C:\WINDOWS\System32\6to4v32.dll () This is not legitimate

File Scans

There are a number of options that you can choose for the standard file created/modified scans (these do not apply to any custom scans):

- File Age - By default this is set to 30 days (90 days for a Quick Scan) but this can be changed to any number of pre-defined ranges from 1 day to 360 days (available settings are 1,7,14,30,60,90,180,360) when the File Age option is chosen within the Files Created Within or Files Modified Within scans.
- Use Company Name WhiteList - off by default for the standard scans and on by default for a Quick Scan. The company name whitelist is a list of about 150 company names that will filter out files containing these names if this option is selected.
- Skip Microsoft Files - off by default for the standard scans and on by default for a Quick Scan. If on, all files with a company name including Microsoft will be filtered out of the output.
- No-Company-Name Whitelist - on by default for all Files Created/Modified scans. This is a list of files that have no company name but are safe and includes files like ntuser.dat, .hlp files, .nls files, etc. If you want to see those types of files you will need to uncheck the box beside Use No-Company-Name Whitelist.
- Files Created Within/Files Modified Within - The standard file scans. These will be turned off if the None option is chosen; use the File Age setting above if the File Age Option is chosen (the default); and include all files if the All option is chosen.
- LOP Check - off by default for the standard scans and on by default for the Quick Scan. This scan scans the All Users Application Data folder and the user's Application Data folder and lists all files, and all folders present not on the LOP Whitelist (a list of about 160 folders that have been deemed safe) and all files in the Windows Tasks folder.
- Purity Check - off by default for the standard scans and on by default for the Quick Scan. This scan will search for all the known locations in which Purity creates files and folders and list anything found.

You can instruct the user to set any of these options to whatever values you desire to achieve whatever results you are looking for.

In a log

========== Files/Folders - Created within 30 Days ==========

Shows files/folders created within a selected period.

The default period is 30 days but there is a range of options available extending out to 360 days old.

========== Files - Modified within 30 Days ==========

Shows files modified within 30 days. Again there is an option for different periods from 1 to 360 days.

Note: OTL will show the company name of the file. Just because it says, for example, that it is from Microsoft Corporation, does not necessarily mean it's valid. Malware can be written with signatures from all kinds of different valid companies.

Note 2: In some logs a file will show up in the Files Created/Modified scans but also say "File handle not seen by OS". This happens when a file handle to the file cannot be provided by the OS. This is how the file properties like company name and attributes are collected. The file is there but something is preventing opening a handle to it. This can be an indicator of some sort of stealth or rootkit activity. Further investigation is required.

*Note 3: The files created/modified scans also include **ALL** files in the Application Data folders, Program Files folder, and Common Program Files folder. There should normally not be any files directly in these folders. Many infections modify the file date attributes to something much older than what they actually are to hide their presence from scanners that only look at file date/times. This should pick those up.*

========== Files - No Company Name ==========

Lists any .exe, .dll, .ini, etc files of any date that do not have a company name.

========== LOP Check ==========

The Lop check lists all files and folders in the Application Data folders as well as any files in WINDOWS\Tasks .

Any O4 running from the Application Data folder where files and folder names are completely random and make no sense are likely to be LOP.

A LOP filter is included to filter out known good folders during the LOP scan

========== Purity Check ==========

Purity check is a simple scan with no output if nothing is found. the Purity infection has been quite consistent over the years and has a set list of folders it creates in set locations. OTL checks all of the locations for all of the folders and only reports on any found items.

========== Alternate Data Streams ==========

Alternate Data Streams are listed.

Any file or folder found that contains an alternate data stream during any scan (standard or custom) will be placed on this list. ADSs of ZONE.IDENTIFIER, FAVICON, and ENCRYPTABLE are ignored.

To remove an ADS simply copy/paste the line into the :OTL section of a fix.

========== Files - Unicode (All) ==========

An example might look like this:

[1999/09/10 00:00:00 | 00,483,780 | ---- | M] ()(c:\N?mesList.txt) -- c:\N?mesList.txt

Any files or folders found that contain Unicode characters during any scan (standard or custom) will be placed on this list. Just include the line in the :OTL section and OTL will take care of them like any other file.

Extras log

========== Extra Registry ==========

========== File Associations ==========

Shows the file type that each file extensions is associated with along with the application used in the Open command (e.g. .txt files or .reg files)

========== Shell Spawning ==========

Lists shell spawning values for All the file extensions.

Example below shows the result of a scan that shows no infection;

QUOTE [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\<key>\shell\[command]\command]
batfile [open] -- "%1" %* File not found
chm.file [open] -- "C:\WINDOWS\hh.exe" %1 (Microsoft Corporation)

cmdfile [open] -- "%1" %* File not found
comfile [open] -- "%1" %* File not found
exefile [open] -- "%1" %* File not found
htmlfile [edit] -- Reg Error: Key error.
htmlfile [open] -- "C:\Program Files\Internet Explorer\iexplore.exe" -nohome (Microsoft Corporation)

This one shows Win Police Pro

QUOTE [HKEY_LOCAL_MACHINE\SOFTWARE\Classes\<key>\shell\[command]\command]
batfile [open] -- "%1" %* File not found
chm.file [open] -- "C:\WINDOWS\hh.exe" %1 (Microsoft Corporation)
cmdfile [open] -- "%1" %* File not found
comfile [open] -- "%1" %* File not found
exefile [open] -- "C:\WINDOWS\System32\desote.exe" %* ()
htmlfile [edit] -- Reg Error: Key error.
htmlfile [open] -- "C:\Program Files\Internet Explorer\iexplore.exe" -nohome (Microsoft Corporation)

The first item (e.g. exefile) is the key and the second item (e.g. open) is the command. If you see that, you must fix the <key>\[command] key's default value manually in the fix. For the comfile and exefile settings you can use the O35 lines from the Standard Registry scan and simply include them in the :OTL section.

When preparing a fix, ALWAYS include a :reg section to fix the shell spawning values. Include the following as part of the fix:

:reg
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command]
""=""%1" %*"

If you don't do that, the user might be able to boot back into Windows without any problems but they still will not be able to run any .exe files. Note: For .com and .exe files, if you have fixed this through the O35 item then you do not have to include the :reg fix for those two types.

Example of an incorrect fix:

CODE:OTL
PRC - C:\WINDOWS\svchasts.exe ()
SRV - (AntipPro2009_100 [Auto | Running]) -- C:\WINDOWS\svchasts.exe ()
O2 - BHO: (ICQSys (IE PlugIn)) - {76DC0B63-1533-4ba9-8BE8-D59EB676FA02} - C:\WINDOWS\System32\dddesot.dll (ASC - AntiSpyware)
[2009/09/08 09:53:11 | 00,000,036 | ---- | C] () -- C:\WINDOWS\System32\sysnet.dat
[2009/09/08 09:53:09 | 00,000,004 | ---- | C] () -- C:\WINDOWS\System32\bincd32.dat
[2009/09/08 09:53:05 | 00,498,688 | ---- | C] (ASC - AntiSpyware) -- C:\WINDOWS\System32\dddesot.dll
[2009/09/08 09:53:05 | 00,163,840 | ---- | C] () -- C:\WINDOWS\svchasts.exe
[2009/09/08 09:53:05 | 00,000,058 | ---- | C] () -- C:\WINDOWS\ppp4.dat
[2009/09/08 09:53:05 | 00,000,009 | ---- | C] () -- C:\WINDOWS\System32\bennuar.old
[2009/09/08 09:53:05 | 00,000,003 | ---- | C] () -- C:\WINDOWS\ppp3.dat
[2009/09/08 09:53:04 | 00,440,320 | ---- | C] () -- C:\WINDOWS\System32\desote.exe
[2009/09/08 09:53:02 | 00,001,708 | ---- | C] () -- C:\Documents and Settings\some user\Desktop\Windows Police Pro.lnk
[2009/09/08 09:52:54 | 00,000,000 | ---D | C] -- C:\Program Files\Windows Police Pro

:commands
[Reboot]

Example of a correct fix:

CODE:OTL

PRC - C:\WINDOWS\svchasts.exe ()
SRV - (AntipPro2009_100 [Auto | Running]) -- C:\WINDOWS\svchasts.exe ()
O2 - BHO: (ICQSys (IE PlugIn)) - {76DC0B63-1533-4ba9-8BE8-D59EB676FA02} - C:\WINDOWS\System32\dddesot.dll (ASC - AntiSpyware)
[2009/09/08 09:53:11 | 00,000,036 | ---- | C] () -- C:\WINDOWS\System32\sysnet.dat
[2009/09/08 09:53:09 | 00,000,004 | ---- | C] () -- C:\WINDOWS\System32\bincd32.dat
[2009/09/08 09:53:05 | 00,498,688 | ---- | C] (ASC - AntiSpyware) -- C:\WINDOWS\System32\dddesot.dll
[2009/09/08 09:53:05 | 00,163,840 | ---- | C] () -- C:\WINDOWS\svchasts.exe
[2009/09/08 09:53:05 | 00,000,058 | ---- | C] () -- C:\WINDOWS\ppp4.dat
[2009/09/08 09:53:05 | 00,000,009 | ---- | C] () -- C:\WINDOWS\System32\bennuar.old
[2009/09/08 09:53:05 | 00,000,003 | ---- | C] () -- C:\WINDOWS\ppp3.dat
[2009/09/08 09:53:04 | 00,440,320 | ---- | C] () -- C:\WINDOWS\System32\desote.exe
[2009/09/08 09:53:02 | 00,001,708 | ---- | C] () -- C:\Documents and Settings\some user\Desktop\Windows Police Pro.lnk
[2009/09/08 09:52:54 | 00,000,000 | ---D | C] -- C:\Program Files\Windows Police Pro

:reg
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command]
""=""%1" %*"

:commands
[Reboot]

========== Security Center Settings ==========

========== System Restore Settings ==========

Lists policy settings for System Restore.

Example below shows settings set to disable System Restore.

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore]
"DisableSR" = 1
"DisableConfig" = 1

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore]
"DisableSR" = 1

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sr]
"Start" = 4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SrService]
"Start" = 2

System Restore may be turned off if the user is using an alternative restore utility such as ERUNT or simply to conserve resources. A question needs to asked of the user to ascertain if they are aware of the settings.

Whenever you see a Group Policy key and it is not legitimate, you want to delete the key and not just change the settings. For example, our first inclination here might be to change each of these settings to zero to turn the policies off. That would be good, wouldn't it? Well, yes and no. Yes it would be good because then System Restore would function again, but no because the user would not have any control over it. If DisableSR is set to zero the user cannot turn it off even if they want to. If DisableConfig is set to zero then the configuration screen will be visible but the user won't be able to make any changes to any of the settings. The system will always enforce the default settings. So what we want to do is make these settings "Not Configured" and we do that by deleting the entire key.

The next three settings should always be there and can be set by the user through the System Restore control panel:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore]
"DisableSR" = 1

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sr]
"Start" = 4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SrService]
"Start" = 2

If the user unchecks the box for "Turn system Restore On" then the DisableSR setting will be on and the SR service Start value will be set to 4 (meaning disabled). The SRService service Start value will normally stay at 2 (meaning Auto) but the service will not run when the SR service is disabled. The SR service is the filter driver for the System Restore system. In some cases of malware, the SRService Start value might be set to 4 as well. These settings will all be set when the Group Policy editor is used to disable System Restore but malware could directly change any one or more of these keys/values.

To fix these settings we do not want to simply delete the keys like we do for Group Policy settings. What we want to do with these is set the DisableSR value to zero (meaning the disable is turned off and thus System Restore is enabled); set the SR Start value to zero (meaning that it will start at Boot); and if needed set the SRService Start value to two (meaning that it will auto-start). A reboot is required to make the changes take effect.

Note: An example fix for System Restore and Firewall settings can be found below at the end of the Firewall Settings explanation.

========== Firewall Settings ==========

Lists policy settings for Windows Firewall.

Example below shows settings set to disable Windows Firewall.

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall]

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile]
"EnableFirewall" = 0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile]
"EnableFirewall" = 0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile]
"EnableFirewall" = 0
"DoNotAllowExceptions" = 0
"DisableNotifications" = 0
"DisableUnicastResponsesToMulticastBroadcast" = 0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\GloballyOpenPorts\List]
"139:TCP" = 139:TCP:*:Enabled:@xpsp2res.dll,-22004
"445:TCP" = 445:TCP:*:Enabled:@xpsp2res.dll,-22005
"137:UDP" = 137:UDP:*:Enabled:@xpsp2res.dll,-22001
"138:UDP" = 138:UDP:*:Enabled:@xpsp2res.dll,-22002

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]
"EnableFirewall" = 0
"DoNotAllowExceptions" = 0
"DisableNotifications" = 0
"DisableUnicastResponsesToMulticastBroadcast" = 0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List]
"139:TCP" = 139:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22004
"445:TCP" = 445:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22005
"137:UDP" = 137:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22001
"138:UDP" = 138:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22002

Unless the computer is on a domain it is highly likely that malware set any Group Policy settings. However, for the user settings, some users will, for one reason or another, knowingly turn off the Windows Firewall. Windows Firewall should be turned off if a third party firewall is in use. If a third party firewall is not seen in the services/drivers section and the user settings for the firewall show that it is disabled, then a question to the user is in order to find out if they are aware of the situation.

The Group Policy settings are always under the HKEY_LOCAL_MACHINE\SOFTWARE\Policies\ key. In this case there could be a key for Domain settings, a key for Standard settings, and a key for Public settings (on Vista and Win7):

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall]

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile]
"EnableFirewall" = 0

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile]
"EnableFirewall" = 0

Here, the EnableFirewall values are set to zero meaning that they are turned off, thus disabling the Windows Firewall. Unless the computer is on a company network, it is highly unlikely that these settings should be there. Maybe a user used the Group Policy editor to set them but for the vast majority of users they won't even know what that is. Because they are Group Policy keys, we want to delete the key. Setting these settings to one (thus enabling the Windows Firewall) will force the Firewall to on and not allow the user to make any changes through Security Center. This would be very bad if they were running a third party firewall. Even if the Windows Firewall should be disabled, there are user settings to do that and (unless required by a company IT department) for a home user these Group Policy settings should be removed.

The user controllable settings will show up in the SYSTEM hive:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile]
"EnableFirewall" = 0
"DoNotAllowExceptions" = 0
"DisableNotifications" = 0
"DisableUnicastResponsesToMulticastBroadcast" = 0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\GloballyOpenPorts\List]
"139:TCP" = 139:TCP:*:Enabled:@xpsp2res.dll,-22004
"445:TCP" = 445:TCP:*:Enabled:@xpsp2res.dll,-22005
"137:UDP" = 137:UDP:*:Enabled:@xpsp2res.dll,-22001
"138:UDP" = 138:UDP:*:Enabled:@xpsp2res.dll,-22002

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]
"EnableFirewall" = 0
"DoNotAllowExceptions" = 0
"DisableNotifications" = 0
"DisableUnicastResponsesToMulticastBroadcast" = 0

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List]
"139:TCP" = 139:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22004
"445:TCP" = 445:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22005
"137:UDP" = 137:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22001
"138:UDP" = 138:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22002

Example of a fix for System Restore/Firewall policy settings:

There will normally be two keys: DomainProfile and StandardProfile. If the system is from a home user the DomainProfile settings can be anything and it won't matter because they only apply to computers on a domain. Under the StandardProfile key, the EnableFirewall value is the one we want to check. If it is set to zero as shown above, then the Windows Firewall will not run. This will be set as above if the user goes into the Security Center control panel and sets the Windows Firewall to Off, and this might be legitimate. Check for the presence of a third party firewall and if there are no signs of one, ask the user if they turned the firewall off on purpose. If they did not (or don't know what you are talking about) then set the StandardProfile EnableFirewall value back to one (meaning it is enabled). Once again, a reboot is required for the changes to take effect. So assuming that this is a home user, and the user did not turn off System Restore or the Windows Firewall, we will want to perform the following fix:

```
:reg
[-HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\SystemRestore]
[-HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore]
"DisableSR" = DWORD:0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sr]
"Start" = DWORD:0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SrService]
"Start" = DWORD:2
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]
"EnableFirewall" = DWORD:1

:commands
[reboot]
```

Additional note: On some systems a situation can occur where after performing the above fix System Restore will still not start and the control panel for System Restore might or might not show up in the Properties dialog. This seems to be associated with the SR driver's ImagePath value. It should read "system32\DRIVERS\sr.sys". But after running the fix and rebooting the computer the value changes for some reason to "systemroot\\systemroot\system32\DRIVERS\sr.sys". When an attempt is made to start the SRService service an error generates stating "File not found". Since the SR driver is not running the SRService service cannot start. Setting the value that way does not occur on every system and appears to happen on those it does during the bootup. It is easily fixable however. Just run the following fix:

```
:reg
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Sr]
"ImagePath" = "system32\drivers\sr.sys"

:files
net start srservice /c
```

Everything should be back to normal. As a precaution, if you need to fix the SR driver entry, you might want to run a scan for all services and all drivers. That will show you whether the SRService is running and the SR driver is running (and the paths to their files). If needed, fix the item shown above and start the SRService.

========== Authorzed Applications List ==========

========== HKEY_LOCAL_MACHINE Unistall List ==========

< End of report >

Custom Scans - Standalone Commands

Standalone commands to use in a scan without any other parameters.

BASESERVICES - to show service information for a list of base services that affect a variety of normal system operations.

DRIVES - to obtain some basic drive/partition information. Output will look like this:

========== Custom Scans ==========

========== Drive Information ==========

Physical Drives

Drive: \\\\.\\PHYSICALDRIVE0 - Fixed hard disk media
Interface type: IDE
Media Type: Fixed hard disk media
Model: WDC WD64 00AAKS-65A7B SCSI Disk Device
Partitions: 2
Status: OK
Status Info: 0

Drive: \\\\.\\PHYSICALDRIVE1 - Removable Media
Interface type: USB
Media Type:
Model: Generic USB CF Reader USB Device
Partitions: 0
Status: OK
Status Info: 0

Drive: \\\\.\\PHYSICALDRIVE2 - Removable Media
Interface type: USB
Media Type:
Model: Generic USB MS Reader USB Device
Partitions: 0
Status: OK
Status Info: 0

Drive: \\\\.\\PHYSICALDRIVE3 -
Interface type: USB
Media Type:
Model: Generic USB SD Reader USB Device
Partitions: 0
Status: OK
Status Info: 0

Drive: \\\\.\\PHYSICALDRIVE4 -
Interface type: USB
Media Type:
Model: Generic USB SM Reader USB Device
Partitions: 0
Status: OK
Status Info: 0

Drive: \\\\.\\PHYSICALDRIVE5 -
Interface type: USB

Media Type: Removable Media
Model: Kingston DataTraveler 2.0 USB Device
Partitions: 1
Status: OK
Status Info: 0

Drive: \\\\.\\PHYSICALDRIVE6 -
Interface type: USB
Media Type: Removable Media
Model: SanDisk Cruzer USB Device
Partitions: 1
Status: OK
Status Info: 0

Partitions

DeviceID: Disk #0, Partition #0
PartitionType: Installable File System
Bootable: True
BootPartition: True
PrimaryPartition: True
Size: 583.00GB
Starting Offset: 32256
Hidden sectors: 0

DeviceID: Disk #0, Partition #1
PartitionType: Installable File System
Bootable: False
BootPartition: False
PrimaryPartition: True
Size: 13.00GB
Starting Offset: 626248143360
Hidden sectors: 0

DeviceID: Disk #2, Partition #0
PartitionType: Win95 w/Extended Int 13
Bootable: False
BootPartition: False
PrimaryPartition: True
Size: 1.00GB
Starting Offset: 16384
Hidden sectors: 0

DeviceID: Disk #1, Partition #0
PartitionType: Unknown
Bootable: False
BootPartition: False
PrimaryPartition: True
Size: 7.00GB
Starting Offset: 16384
Hidden sectors: 0

First, all of the physical drives will be listed and then all of the partitions found.

After the drives, all partitions found will be listed. In the DeviceID the Disk listed will point to the physical drive shown first. For Example, Disk #0 Partition #0 is the first partition on the first physical drive. Disk #0 Partition #1 is the second partition on the first physical hard drive. Etc.

The other partition information is just some basic information that might be useful i.e. Bootable, BootPartition, PrimaryPartition, Size, etc.

The partitions will not necessarily be listed in order of the drives (notice that Disk #1 comes after Disk #2 in the partition section) but partitions on the same drive should be next to each other.

HIJACKTHISBACKUPS - lists HijackThis backups

RESTOREPOINTS - list restorepoints

SHOWHIDDEN - shows hidden files on system drive

Quick Reference of available Directives & Commands

The directives/commands are not case sensitive.

:processes

Either individual or all processes can be stopped using this directive.

If you do not include the [EMPTYTEMP] command but still want to kill all processes before running a fix then the command killallprocesses can be placed in this section.

Examples of individual processes you might want to use this directive for might be - TeaTimer, SpywareGuard or another anti-malware program, or any malware related processes.

:OTL

Any lines in a log from any of the standard scans or custom scans for files/folders can be copy/pasted directly into the :OTL section of a fix for removal. Generally :OTL will remove the entry and move the file at the same time. For processes, though, the file will *not* be moved and will need to be dealt with in the :FILES section.

Individual items in the HOSTS file (O1 lines) can only be removed in the :OTL section. If you want to reset the HOSTS file to the default (only the 127.0.0.1 localhost and ::1 localhost lines) then use the command [resethosts] in the :commands section.

IE items that have files (like the URLSearchHooks) will have the registry entry deleted and the file moved. For other IE registry items the rule of thumb is this:

- if the entry contains "ProxyEnable" then the value is set to 0 (zero)

- if the entry contains "AutoConfigURL" then it is deleted

- if you include the DefaultScope line then the value will just be set to nothing and you will need to include a :REG section to set it to something else.

- all other entries are set to blank

For Chrome items the extensions folder is removed. This is not the preferred way to remove extensions since OTL will only delete the extension folder but cannot edit the prefs file. Deleting the extension folder does effectively remove the extension and it cannot run and does not do any harm to Chrome's operation but the extension name remains in the prefs file. ***Use OTL as a last resort only for removing extensions from Chrome.***

The preferred method of removing plugins and extensions in Chrome is through Chrome itself.

For plugins, just have the user type the following into the address box:

```
chrome:plugins
```

This will display a page of all of the installed plugins. There is no option to remove a plugin but a plugin can be disabled from this page. If you want to actually remove the plugin or it doesn't showup in the list of plugins then just delete the file (or possibly folder) shown on the plugin line.

For extensions, have the user type the following into the address box:

```
chrome:extensions
```

This will show all of the installed extensions and each extension can be either disabled or uninstalled from this page. If the extension doesn't show or uninstalling it doesn't remove the files then just delete the folder shown on the extension line.

:Services

OTL will try to stop and disable any running services before deleting them. However, it is important to note that it may have trouble doing this against some of the nastier pieces of malware. In the event that this directive is unable to stop the service then you will need to disable the process in Safe Mode or via another method.

You can also delete any drivers under this directive. Make sure to use the name when deleting any services or drivers and not the description.

:Reg

You can do any sort of registry fix here. A handy feature is that you don't have to deal with hex values. For those complex fixes you aren't sure about you can use the plain text for what you want the key/value to have.

See example below:

Bad entry:-

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"authentication packages"=msv1_0 C:\WINDOWS\system32\byXoMcbC
```

to fix this in a .reg file you would need to do this:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"Authentication Packages"=hex(7):6D,73,76,31,5F,30,00,00
```

If you weren't sure what hex value to use and didn't want to risk messing up that key, you could just do this instead

Fix:-

```
:reg
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]
"Authentication Packages"=hex(7):"msv1_0"
```

OTL will handle the conversion and the registry key will then be fixed.

:Files

All manually entered files and folders are put underneath this directive. Do *not* copy/paste any file/folder lines from the log in this area (those go under the :OTL directive). This is only for any additional files or folders you may need to move (i.e. the files from a process that you want moved or those that come from other logs).

Note: You do not have a separate command for folders when using OTL. Just include the folder under the :Files directive and it will be taken care of.

:Commands

Commands must be placed under the :Commands directive.

[CLEARALLRESTOREPOINTS] - this will remove all current restore points and create a new restore point after the fix is completed.

[CREATERESTOREPOINT] - this will create a new restore point after the fix is completed.

With either of the commands for restore points, OTL will check to see if the appropriate services are running which are required for creating a restore point and attempt to start them if they are not. If the required services are not running and cannot be started you will see a line in the fix log pertaining to the reason why and will need to pursue that at a later time.

Note: You can also use these two commands in a scan. It's important to remember that if used in a scan the brackets are not included i.e. if run in a scan they would look like this:-

clearallrestorepoints or createrestorepoint

Put either CREATERESTOREPOINT or CLEARALLRESTOREPOINTS in the Custom Scans/Fixes box along with any other custom scans you are running (i.e. SAFEBOOTMINIMAL or NETSVCS). The commands are not case sensitive and can be run along with any other scans you might want to run. A line in the log file will show you what the result was (either successful or the reason why it failed).

[EMPTYFLASH] - to remove all Flash cookies.
Note: Not all flash cookies are bad. Some only contain various settings for specific websites but you can't tell what ones do what. If you use the above command all cookies will be removed regardless of what they do.
Note 2: The emptytemp command includes emptyflash and emptyjava so these commands are used when for some reason you wish only to clear flash or java without removing other temp files.

[EMPTYJAVA] - to clear Java cache.
Use this command if you wish to clear Java cache without clearing other temp files.
Note: The emptytemp command includes emptyflash and emptyjava so these commands are used when for some reason you wish only to clear flash or java without removing other temp files.

[EMPTYTEMP] - to empty all of the user, system, and browser temp folders.
Note: if this command is included in a fix then all processes will be killed automatically at the beginning of a fix and a reboot will be required at the end so you do not need to explicitly include the [REBOOT] command in the :COMMANDS section.

[PURITY] - will automatically remove any Purity infection on the system. Purity has a consistent pattern of folders created using Unicode characters and this command will remove all those found without needing to list each folder individually.

[REBOOT] - to force a reboot of the system after a fix completes.
Note: this is not required if KILLALLPROCESSES is used in the :PROCESSES section or [EMPTYTEMP] is used in the :COMMANDS section because a reboot will automatically be forced anyway. It can be included but it will be ignored in these cases.

[RESETHOSTS] - to reset the HOSTS file back to its default value of:
127.0.0.1 localhost
::1 localhost

The current HOSTS file will be moved into a subfolder of the MovedFiles folder, the one which is associated with the fix.

Switches

Switches are additional parameters that can be used with both custom scans or fixes to enhance the output or outcome of the results.

Note: If an invalid switch is included; a line (Invalid Switch:...) will simply be placed in the log and the scan will continue on. If the switch being shown as invalid is in fact correct, then check the version number of OTL the poster is using.

Switches that can be used when performing a custom scan:

/C - to run a DOS command line command
Example:
set /c - to return all environment variables
net stop <servicename> /c - OTL will not start or stop services (only delete them) so you can use this switch with the net command to perform any service management tasks (start, stop, pause, continue)
netstat -r /c - will display the routing tables

Any command that you need to be used at a command line can be used within a custom scan using the /C switch and the output will be included in the log. This can eliminate the need to have the user create and run batch files and then find and post the output files created from them.

/FP - to run a file/folder name pattern search and return all files *and* folders found
Example:
c:\windows|myfile;true;true;true /FP

Parameters:
myfile is the pattern to look for (will return items like c:\windows\myfile.exe, c:\windows\123myfile456.dat, c:\windows\notmyfileeither)
recurse folders (will also include items like c:\windows\system32\helpmyfile.dll, c:\windows\msagent\intl\closetomyfile.ocx)
inc1ude child folders (if true and a folder is found that matches the pattern then the immediate folders underneath it will be shown as well)
include files (if true files with names that match the pattern will be shown; if false then only folders will be shown)

The /FP switch is used internally for some unique scans that are required during the standard scans and most helpers probably won't have a need for it but you can do some really cool things with it so I thought I would just make it available to use. It eliminates the need to run two separate scans (one for folders and one for files) if you need to find all items of both.

/MD5 - to include MD5 values for all files
You will see this being used extensively in the Malware Cleaning Guide to find patched files. There are currently infections that modify OS files in a way that are difficult to detect in any other manner. MD5s are a unique mathematical value that can be calculated for a file to determine whether or not it has been changed. If even one byte in a file is changed the calculated MD5 will also change. Some examples from the Guide are:

%SYSTEMDRIVE%\iaStor.sys /s /md5
%SYSTEMDRIVE%\nvstor.sys /s /md5
%SYSTEMDRIVE%\atapi.sys /s /md5
%SYSTEMDRIVE%\IdeChnDr.sys /s /md5

MD5 values are not stored within files, they are calculated on the fly from the files. The scans above search the entire system drive for the specified file and return all files found with their calculated MD5 values. If the MD5 of the file in the normal operating folder (i.e. system32 or system32\drivers) is different than that in the backup folders (i.e the dllcache folder or the i386 folder) then the file is most likely patched. If the MD5 comes back as nothing, then it is almost a surety that the file has been patched and should be replaced with a valid copy from one of the other locations using a tool like Avenger. Using the MD5 value you can be assured that the file is legitimate.

/MD5START and /MD5STOP - to wrap around files to look for.

Example:
/md5start
eventlog.dll
scecli.dll
netlogon.dll
cngaudit.dll
sceclt.dll
ntelogon.dll
logevent.dll
iaStor.sys
nvstor.sys
atapi.sys
IdeChnDr.sys
viasraid.sys
AGP440.sys
vaxscsi.sys
nvatabus.sys
viamraid.sys
nvata.sys
nvgts.sys
iastorv.sys
ViPrt.sys
/md5stop

This allows you to check files you wish without the need to include any paths because if the scan sees these switches it will always start at the root of the systemdrive and scan the entire drive. It batches all of the files togther and looks for each file as it passes through each folder so only one pass of the hard drive is needed.

If there are a number of files you are looking for to check the MD5s then using /md5start and /md5stop is much more efficient and produces a cleaner log. If you just have one or two items then /md5 will surfice.

Note: Whenever the /md5start /md5stop block is used the searches will also look for any servicepack .cab files. If any of these are found, it will look inside for the file being searched for, and if one is found, it will list it in the output. ***This is not the case if /md5 search alone is used****.*

/LOCKEDFILES - to find locked files that MD5 can't be calculated for.

The scan simply grabs the file and attempts to calculate the MD5 and if it can't, reports the output, skipping any files that it can get an MD5 on.

Note: You need to supply a path/file specification just like any other file scan and the /S switch if you want to go through the sub-folders as well. So if you wanted to see what .dll files are locked just in the system32 folder you would use:

%systemroot%\system32.dll /lockedfiles*

If for some reason all files need to be checked (Windows will normally have a number of locked files by default and unless there is a particular reason it isn't necessary to see all of those) then simply add the /all switch:

%systemroot%\system32*.dll /lockedfiles /all

/RS - to perform a registry search for a pattern
Example:
hklm\software\microsoft\windows\currentversion|somepattern /RS

The /rs switch will search for and return all keys, value names, and data found for the pattern included. If a starting point is not included (e.g. somepattern /rs) then the following areas will be searched:

hklm\software\classes
hklm\software\microsoft
hklm\software\policies
hklm\system\currentcontrolset
hkcu\software\classes
hkcu\software\microsoft
hkcu\software\policies

It is always preferred to specify a starting point for the search.

/RP - to search for all types reparse points

Example: c:\windows*.* /RP or c:\windows*. /RP

or

Example: c:\windows*. /RP /s

Using this switch will show all reparse points (like those used by the current max++ infection) and the results can be simply placed in the :OTL section of a fix to be removed. With /s it will recurse through all sub folders.

/HL - to search for only hard links

Example: c:\windows*.* /HL or c:\windows*. /HL

/JN - to search for only junctions

Example: c:\windows*.* /JN or c:\windows*. /JN

/MP - to search for only mount points

Example: c:\windows*.* /MP or c:\windows*. /MP

At time of writing a very useful scan that you could add to your custom scans would be:

%systemroot%*. /mp /s

This would find all of the current max++ mount points on a system with your initial scan (or a subsequent scan) and you could remove them with your initial fix.

/SL - to search for only symbolic links

Example: c:\windows*.* /SL or c:\windows*. /SL

/SP - to perform a string pattern search within files
Example:
c:\windows*.*|somepattern /SP

Back in the days of WinPFind, this command was used quite often to find malware signatures in files. It is not used often today but is still available.

/S - to recurse sub-folders in a file search or sub-keys in a registry search
Example:
c:\windows*.dat /S

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ACPI /S

This switch is also often used in conjuction with the /MD5 or /U switch to recurse sub-folders in those searches as well.

/U - to only include Unicode files in a search
Example:
c:\windows*.* /U

Files and folders with Unicode values in their names often look like legitimate items in Explorer. During the standard scans, OTL will automatically place any files or folders found with Unicode values in the Unicode section of a log and these can be fixed as easily as any other file or folder by simply placing the lines in the :OTL section of a fix. With many scanners, the names of these files or folders are not properly interpreted and will show up with a ? where the Unicode characters are which makes it impossible to determine what to remove. OTL takes care of that for you. Using the /U switch in a custom scan will return only those files and folders found that contain Unicode characters in their names.

An example of a return is:
< c:*.* /U >

========== Files - Unicode (All) ==========
[1999/09/10 00:00:00 | 00,483,780 | ---- | M] ()(c:\N?mesList.txt) -- c:\NamesList.txt

/X - to exclude files from a search
Example:
c:\windows*.exe /X

This will exclude all .exe files and return everything else.

/64 - to specifically search in 64bit folders or registry keys on 64bit OSs
Example:
c:\windows\system32*.dat /64
hklm\software\microsoft\windows\currentversion\run /64

Because OTL is a 32-bit application, if the /64 switch is not used when scanning on a 64-bit OS, the OS will automatically redirect the scan to the 32-bit areas of the file system or registry where applicable. This switch will override that default behavior and force the scan to the 64-bit areas when needed.

/<some number> - to only include files or folders a certain amount of days old
Example:
c:\windows\system32*.* /3

The above custom scan will only return files created within the last 3 days.

/CREATED - to change the modified file date to the created date. Normally in a custom scan the file information includes the modified file date. Using this switch will change that to include the created date.
Example (no switch):

< c:\temp2*.exe >
[2002/04/23 16:42:00 | 000,379,392 | -H-- | M] () -- c:\temp2\ps.exe
[2008/03/17 21:39:00 | 000,173,688 | ---- | M] () -- c:\temp2\tscc.exe

Example (with /created switch):

< c:\temp2*.exe /created >
[2010/03/03 22:26:30 | 000,173,688 | ---- | C] () -- c:\temp2\tscc.exe
[2011/01/15 06:28:46 | 000,379,392 | -H-- | C] () -- c:\temp2\ps.exe

/DRIVER - to list the same driver information in a driver scan but for a single driver. You need to supply the driver name.
Example:
cdrom /driver

========== Custom Scans ==========
DRV - [2008/04/14 01:10:48 | 000,062,976 | ---- | M] (Microsoft Corporation) [Kernel | System | Unknown] -- C:\WINDOWS\system32\drivers\cdrom.sys -- (Cdrom)

/NCN - to only list files that do not have a company name.
Example:

< c:\windows*.exe /ncn >
[2005/02/10 20:14:18 | 000,098,816 | ---- | M] () -- c:\windows\sed.exe

/SERVICE - Used to list the same service information in a service scan but for a single service. You need to supply the service name. If on a 64-bit OS and a 64-bit and 32-bit service exist it will list both.
Example:
cryptsvc /service

========== Custom Scans ==========
SRV:64bit: - [2012/04/23 12:25:30 | 000,174,592 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Windows\SysNative\cryptsvc.dll -- (CryptSvc)
SRV - [2012/04/23 12:00:53 | 000,133,120 | ---- | M] (Microsoft Corporation) [Auto | Running] -- C:\Windows\SysWOW64\cryptsvc.dll -- (CryptSvc)

/VERSION - to include the file version information.
Example:

< c:\windows*.exe /version >
[2008/04/14 06:42:20 | 001,033,728 | ---- | M] (Microsoft Corporation - Version = 6.00.2900.5512 (xpsp.080413-2105)) -- c:\windows\explorer.exe
[2008/04/14 06:42:22 | 000,010,752 | ---- | M] (Microsoft Corporation - Version = 5.2.3790.2453 (srv03_sp1_qfe.050525-1536)) -- c:\windows\hh.exe
[1998/10/29 16:45:06 | 000,306,688 | ---- | M] (InstallShield Software Corporation - Version = 5, 51, 138, 0) -- c:\windows\IsUninst.exe
[2008/04/14 06:42:30 | 000,069,120 | ---- | M] (Microsoft Corporation - Version = 5.1.2600.5512 (xpsp.080413-2105)) -- c:\windows\notepad.exe
[2008/04/14 06:42:34 | 000,146,432 | ---- | M] (Microsoft Corporation - Version = 5.1.2600.5512 (xpsp.080413-2111)) -- c:\windows\regedit.exe
[2005/02/10 20:14:18 | 000,098,816 | ---- | M] (- Version =) -- c:\windows\sed.exe
[2008/04/14 06:42:36 | 000,032,866 | ---- | M] (Smart Link - Version = 3.80.01MC15) -- c:\windows\slrundll.exe
[2004/08/03 20:07:00 | 000,015,360 | ---- | M] (Microsoft Corporation - Version = 5.1.2600.0 (xpclient.010817-1148)) -- c:\windows\TASKMAN.EXE
[2004/08/03 20:07:00 | 000,049,680 | ---- | M] (Twain Working Group - Version = 1,7,0,0) -- c:\windows\twunk_16.exe
[2004/08/03 20:07:00 | 000,025,600 | ---- | M] (Twain Working Group - Version = 1,7,1,0) -- c:\windows\twunk_32.exe
[2005/06/29 22:34:40 | 000,024,576 | ---- | M] (JSWare - Version = 1.05.0629) -- c:\windows\uninjssv.exe
[2004/08/03 20:07:00 | 000,256,192 | ---- | M] (Microsoft Corporation - Version = 3.10.425) -- c:\windows\winhelp.exe
[2008/04/14 06:42:40 | 000,283,648 | ---- | M] (Microsoft Corporation - Version = 5.1.2600.5512 (xpsp.080413-0852)) -- c:\windows\winhlp32.exe

/VERIFYSIG - to verify if a file is digitally signed and has not been modified. The caveat here is that you need to know if the file is supposed to be digitally signed. If a file is supposed to be digitally signed but has been altered in any way then it will show as not being properly signed. See below.
Example (most Windows files are not digitally signed but the Windows defender files are):

< C:\Program Files\Windows Defender*.* /verifysig >
[2006/11/02 11:01:34 | 000,018,536 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpAsDesc.dll
[2008/01/20 22:47:32 | 000,491,576 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpClient.dll
[2008/01/20 22:47:32 | 000,494,136 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpCmdRun.exe
[2006/11/02 11:01:36 | 000,065,640 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpEvMsg.dll
[2008/01/20 22:47:32 | 000,114,232 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpOAV.dll
[2008/01/20 22:47:32 | 001,099,832 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpRtMon.dll
[2008/01/20 22:47:32 | 000,063,032 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpRtPlug.dll

[2008/01/20 22:47:32 | 000,185,912 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpSigDwn.dll
[2009/04/11 03:11:27 | 000,805,336 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpSoftEx.dll
[2008/01/20 22:47:32 | 000,383,544 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MpSvc.dll
[2008/01/20 22:47:32 | 001,584,184 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MSASCui.exe
[2008/01/20 22:47:32 | 000,295,480 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MsMpCom.dll
[2006/11/02 11:01:35 | 000,011,368 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MsMpLics.dll
[2006/11/02 11:01:34 | 000,654,440 | ---- | M] (Microsoft Corporation is properly Signed) -- C:\Program Files\Windows Defender\MsMpRes.dll

If a file is supposed to be digitally signed but has been altered or does not contain a digital certificate then it will show as not being properly signed. The deployjava1.dll file is digitally signed:

< c:\windows\system32\deployjava1.dll /verifysig >
[2012/05/13 15:56:14 | 000,472,864 | ---- | M] (Sun Microsystems, Inc. is properly Signed) -- c:\windows\system32\deployJava1.dll

and one not properly signed:

< c:\temp1\deployjava1.dll /verifysig >
[2012/08/25 20:07:33 | 000,472,864 | ---- | M] (Sun Microsystems, Inc. is NOT properly Signed) -- c:\temp1\deployJava1.dll

Note: This will look the same as a file that is not digitally signed:

< c:\windows\explorer.exe /verifysig >
[2009/04/11 03:10:17 | 003,079,168 | ---- | M] (Microsoft Corporation is NOT properly Signed) -- c:\windows\explorer.exe

To see if a file is supposed to be digitally signed you can right-click on it a go to the Properties page. If it includes a digital certificate there will be a tab for Digital Signatures with details of the certificate.

Commands/Switches

Commands/Switches that can be used in the :FILES section when performing a fix:

[override] and [stopoverride] - to override the internal list of non-movable files and folders
Example:
:FILES
[override]
c:\windows\system32\userinit.exe
[stopoverride]

OTL includes a list of about 100 files and folders that cannot be moved by default. This is to prevent inadvertantly moving core OS files and folders which could potentially render a system unbootable or unusable. This feature can be overridden using these commands but be very careful when including them. A [stopoverride] command should always be included as soon as possible whenever the [override] command is used to prevent moving a required system file by mistake.

/<some number> - just like in the custom scans, this switch will include all files that match the pattern and also limit the moves to files or folders that have been created within the specified number of days.
Example:
:FILES
c:\windows\system32*.dll /2

This will move all .dll files in the system32 folder that have been created within 2 days. Can be very useful but can also be dangerous. Be careful with using this switch here.

/64 - to access the 64-bit specific folder locations instead of the default 32-bit locations on 64-bit OSs and if the file is found move it from there.
Example:
:FILES
c:\windows\system32\badfile.exe /64

This will cause OTL to look in the 64-bit system32 folder instead of in the 32-bit system32 folder.

@ - to delete alternate data streams.
Example:
:FILES
@c:\windows\system32:somedatastream

Normally you would not need to use this in OTL if a scan has been performed using OTL because any files with ADSs will be listed in the Alternate Data Streams section of the log and you can simply copy/paste the lines into the :OTL section of the fix. If a scan was performed with another tool that does not allow fixes or cannot remove ADSs then you can fix those files with this command in the :FILES section.

/alldrives - to remove a specified file from all drives
Example:
:FILES
somefile.txt /alldrives

This will move all of the copies of a file from the root location of all drives.

If the file is in the same folder on all drives then include that folder as well like this:
:FILES
somefolder\somefile.txt /alldrives

To remove a folder on all drives use just the folder name like this:
:FILES
somefolder /alldrives

If you want to remove all copies from all locations on all drives then include the /s switch like this:
:FILES
somefile.txt /s /alldrives
or
somefolder /s /alldrives
or
somefolder\somefile.txt /s /alldrives

/C - to run a DOS command line command

It is unlikely that this switch will be used often. Other switches/commands cover most things... for example to copy a file you would usually use the /replace switch rather than a DOS command. Nevertheless there may be occasions when it would be useful. For example, you might want to stop a service temporarily (rather than delete it - which the :Services command is intended to facilitate) in which case you can use a DOS command.
Example:
:files
net stop <service> /c
<do something here>
net start <service> /c

/D - to delete the file instead of moving it
Example:
:FILES
%programfiles%*.dll /D

This will delete all files found matching the specification instead of moving them. A common place to use this is with .tmp files but it can be used with any file or folder move. Be careful!

/E - To extract a specified file from a .cab file.
Example:
:FILES
C:\WINDOWS\Driver Cache\i386\sp3.cab:atapi.sys /E

It will always be extracted to the root of the system drive, there is no option to extract it anywhere else. From there, you can use the /replace switch to replace the current active file with extracted file. This will always be a two-step process because the active file might not be able to immediately be replaced and in that case a reboot will be required and the /replace step will take care of that.

The full process to extract a file and replace the current active file in the drivers folder would go like this:
Example:
:files
C:\WINDOWS\Driver Cache\i386\sp3.cab:atapi.sys /e
C:\WINDOWS\system32\drivers\atapi.sys|c:\atapi.sys /replace

Note: Always make sure to put the extraction step before the replace step or it will not work.

/lsp - To delete a file from the LSP stack.
Example:
:Files
helper32.dll /lsp
winhelper86.dll /lsp

For each line, OTL will go through the entire stack, remove any entries that include that file, and if any are removed will rebuild the stack.

/replace

<original file>|<new file> /replace

Example:

:files
C:\WINDOWS\System32\drivers\atapi.sys|c:\atapi.sys /replace

If the file cannot be replaced immediately (it might be in-use) then a reboot will be required to finish the move.

The original and new files do not need to have the same name or even be the same type.

Note: Care this works differently to FCopy:: in ComboFix i.e. the new file comes last - the other way around to ComboFix.

Note 2: If you are attempting to move a file from a cab file it will have to be extracted before you can replace the bad file - see /E above.

/S - to recurse sub-folders and remove all files found that match the specification
Example:
:FILES
c:\windows*.dat /S

This will remove all .dat file in the c:\windows folder and all sub-folders

/U - to only move files or folders with Unicode characters in their names
Example:

:FILES
c:\windows\?ystem32 /U
%commonprogramfiles%\s?stem /U
c:\windows\expl?rer.exe /U /S

Each of these commands will only move the file or folder that has Unicode characters in the position of the ? and will not touch any legitimate files or folders with a name matching the pattern. You will normally see files or folders like this with a Purity infection (where you can simply use the [purity] command in the :commands section) but there could be other files or folders that require this type of move also.

Any of these switches can be mixed and matched to meet the specific needs of the situation.

CleanUp

Use CleanUp in OTL when clearing away. This is preferable to downloading OTC which should only be used when no other OldTimer tool is on the machine.

Here is a list of the tools that CleanUp removes:

avenger.*
Avenger
bfu.zip
BFU
combofix.*
combo-fix.*
ComboFix*.txt
ComboFix
erdnt\subs
QooBox
catchme
catchme.exe
fdsv.exe
grep.exe
mbr.exe
moveex.exe
nircmd.exe
pev.exe
sed.exe
swreg.exe
Swsc.exe
Swxcacls.exe
VFind.exe
WS2Fix.exe
zip.exe
tmp.reg
dds.*
dss.exe
Deckard
deljob.exe
deljob
logit.txt
FindAWF.exe
AWF.txt

fixwareout.exe
fixwareout
fsbl.exe
fsbl*.log
gmer.*
gmer_uninstall.cmd
gmer
haxfix.*
killbox.exe
!Killbox
NoLop.*
NoLopOLD.txt
delete.bat
OTH.*
OTListIt2.exe
OTListIt.txt
Extras.txt
_OTListIt
OTL.*
OTLPE.exe
_OTL
OTMoveIt.exe
OTMoveIt2.exe
OTMoveIt3.exe
OTM.*
_OTMoveIt
_OTM
OTScanIt.exe
OTScanIt
OTScanIt2.exe
OTScanIt2
OTS.*
_OTScanIt
_OTS
OTViewIt.*
MBRFix*.*
rustbfix.exe
Rustbfix
Runscanner.*
*.run
Runscanner
sdfix.exe
SDFix
Silent Runners.vbs
SmitfraudFix.exe
SmitfraudFix
dumphive.exe
iedfix.exe
rapport.txt
vacfix.exe
vcclsid.exe
404fix.exe

SysInsite
VundoFix.*
VundoFix Backups
win32delfkil.exe
_backupD
windelf.txt
winpfind.exe
WinPfind
WinPFind3u.exe
WinPFind3u
WinPFind35u.exe
WinPFind35u
RSIT.exe
RSIT
LopSD.exe
lopR.txt
Lop SD
Rooter.*
Rooter$
exeHelper.com
exeHelperlog.txt
SystemLook.*
CKScanner.exe
ckfiles.txt
Defogger.exe
Defogger*.log
TDSSKiller
TDSSKiller.*
RogueKiller.exe
RKreport*.txt
RK_Quarantine
GooredFix.exe
GooredFix.txt
aswMBR.exe
aswMBR.txt
Flash_Disinfector.exe
WVCheck.exe
WVCheck*.txt
MBRCheck.exe
MBRCheck*.txt
FSS.exe
FSS.txt
frst
frst.txt
frst.exe
frst64.exe
results.txt
search.txt
minitoolbox.exe
cleanup.txt