

I think I have been hijacked.

# I think I have been hijacked.

---

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2008-05/msg00272.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2008-05/msg00272.html)

---

- *From:* At my wits end. <At my wits end.@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Mon, 26 May 2008 10:29:00 -0700
- 

Hello,

I am running windows xp on my Compaq Presario and Toshiba laptop, both about 2 years old, with internet explorer. Although I am "computer illiterate", I am learning some things through necessity. I would love to go back to the check my e-mail and google stage. Please note that I live alone, and the only extended visitor I have had, has been my 4 year old grandson. No one has had access to my computers, but me.

Recently, I have noticed that my computer is running very slow, and that my CPU is at 100% even when I just log on. I have been access to programs, had my settings changed, received alerts, and error alerts. I have had my firewall and spyware disabled, removed from my control panel, and programs I don't recognize added. I am unable to disable remote assistance. It is always running in my systems, even though I turn it off in properties. Although the icon has been removed, I did have a User2 file in my control panel. In advanced section of properties, I can see "users" that I have not initiated. An internet connection appears to have been added through a USB. \*\*I have been unable to download windows update, and internet explorer updates. These I try to keep on auto. When attempted it woud say updates incomplete.

Examples:

My C: drive is labeled C:SQ003706

Alert:

#1068, #1069

ONELIVECARE error ID 0018-80070641

Denied Access:

%STARTUPALL%\PowerMenu.Ink(Thong Nguyen):C:Program

Files\PowerMenu\PowerMenu.exe

SonicRecordNow!\shlext.dll

%SYSDIR%\actskin4.ocx

WINDOWS\system32\ShellvRTF.dll\ContextMenuExt.dll\DRIVERS\GEARAspWDM.sys

%SYSDIR%\hellvRTF.dll(xss)ShellvRTF\sychostr.exe-knetsvcs

\*\*Repeat windows comand with\sychost-kDcomLaunch

\*\*Repeat windows comand with\syshost-krpess

%WINDIR%\ContexMenuExt.dll

I think I have been hijacked.

I think I have been hijacked.

IE

WinRAR

User 2 program in control panel

Remote Assistance denied, and a password was set with "error failed due to login failure 1069", "error failed due to wrong password". Also noted\* in Dependencies, listed "RPC".

Backweb denied

Windows Install is on manual, but stopped, and access denied, password (not mine), protected.

Redirected:

ie.redirect.hp.com/svs/rdr?tye+38tp

http:\\shell.windows.com/fileassoc/microsoft.com/securitybulletins/200409\_ipegTool.msp

I have been on the phone with microsoft windows security almost every day for the last 4-5 days. Was advised to try system restore, unable, no restore date. It had been turned off. Advised to try standard recovery, completed successfully, but problem still existed. Advised full recovery, first unsuccessful, retried, second, third, and fourth successful. I have my recovery CD.

On Wednesday, 5-21-08, supposedly problem resolved, case closed by remote access assistance. On Friday, 5-23-08, supposedly problem resolved, case closed, by remote access assistance.

\*Note\* When case resolved on 5-23-08, remote assistance unable to access windows firewall properties (WHICH WAS TURNED OFF), However, when one looked in the control panel under security, all 3 were on. Tech decided the turned off one was for "old version of windows xp" and since windows xp3 had been successfully completed after 3+ hours, I was "protected". Other "users" were automatic system, (even though they had names and titles on some).

Sunday, 5-24-08, about 12:30. At 12:36pm it flashed "quickly" with a sign in box, (although I don't usually use this), and went to blue "welcome" page. At 1:47pm, went to black screen with sign in box with Compaq Owner, (me), and my password typed in, in background, and a TURN OFF STINSONDESKTOP, in the lower left hand corner. In foreground was a Logon message:...."Could not logon...make sure user name and domain are correct, then retype password again. Letters in password must be typed in correct case.....OK (to check)" I checked on OK, and went immediately, without having to sign on, to start page, color changed, with icons. The OneLiveCare bubble came up, clicked on it, and shortly received a message "OneLiveCare" has to close....sorry for inconvenience.....try again later.....," and "windows update incomplete....."

Had a family dinner to attend.

Last night at app. 7-8pm, turned computer on. It started relatively normal. No extended period of waiting on blue "welcome" page.

OneLiveCare bubble was up, clicked on it, and received an alarming box:  
PC at RISK: Windows LiveOneCare  
URGENT: Virus and spyware monitoring off.....PC is at risk.....

I think I have been hijacked.

I think I have been hijacked.

URGENT: Go to help center OneCare couldn't turn on virus and spyware monitoring.....PC is at risk.....

BACKUP FILES: Changed files.....reconfigure PC.....

INSTALL: Missing updates from microsoft.....PC at risk from internet.....Visit microsoft for security updates.

At first, IE "couldn't display page...", had to put browser on auto detect.

At that time, I was \*\*redirected to:

[http://shell.windows.com/fileassoc/microsoft.com/securitybulletins/200409\\_ipeg\\_Tool.msp](http://shell.windows.com/fileassoc/microsoft.com/securitybulletins/200409_ipeg_Tool.msp).

This website had the \*\*windows\*\* logo on it, but it did not look like any microsoft/windows site I have every visited. That is when I noticed the "redirect" in the address bar. \*\*The curser started moving without me and attempted, successfully? to click on a number in a box..80???. I existed this website, manually went to the microsoft update website, attempted to download the suggested updates through "express", after microsoft scanned to see what I needed.

Received notice: Won't update .NET FRAMEWORK 1.1 (Security)

Won't update JunkMail Filter

Wont update Cumulative Security Update

I immediately called the microsoft security "hotline". They wanted to redo the same things they had done. I had already logged 70+hours on my cell phone, and was tired. And I didn't think they could resolve the problem, and asked for the "security expert", I had been advised would be available if they could not resolve the problem. They don't work on weekends or holidays, so they scheduled a "call back" for Tuesday.

In the interim, I happened upon this help center on my laptop, which is infected, but not to the extent of the desktop. After reading some threads, I went to the "hijackthis" website recommended in a thread with a similar problem and received the following logs.

Can you help? I am disgusted with windows/microsoft, the security flaws are too great, and the help I've received to date too little.

I did not add my e-mail address in my profile. If you need it, would you please request it privately.

In anticipation of your assistance, or at a minimum, a place to vent, thank you

JoyceElaine

\*\*\*\*\*Trend Micro HijackThis v2.0.2/FIRST LOG \*\*\*\*\*

See bottom for version history.

The different sections of hijacking possibilities have been separated into the following groups.

I think I have been hijacked.

I think I have been hijacked.

You can get more detailed information about an item by selecting it from the list of found items OR highlighting the relevant line below, and clicking 'Info on selected item'.

- R – Registry, StartPage/SearchPage changes
- R0 – Changed registry value
- R1 – Created registry value
- R2 – Created registry key
- R3 – Created extra registry value where only one should be
- F – IniFiles, autoloading entries
- F0 – Changed inifile value
- F1 – Created inifile value
- F2 – Changed inifile value, mapped to Registry
- F3 – Created inifile value, mapped to Registry
- N – Netscape/Mozilla StartPage/SearchPage changes
- N1 – Change in prefs.js of Netscape 4.x
- N2 – Change in prefs.js of Netscape 6
- N3 – Change in prefs.js of Netscape 7
- N4 – Change in prefs.js of Mozilla
- O – Other, several sections which represent:
  - O1 – Hijack of auto.search.msn.com with Hosts file
  - O2 – Enumeration of existing MSIE BHO's
  - O3 – Enumeration of existing MSIE toolbars
  - O4 – Enumeration of suspicious autoloading Registry entries
  - O5 – Blocking of loading Internet Options in Control Panel
  - O6 – Disabling of 'Internet Options' Main tab with Policies
  - O7 – Disabling of Regedit with Policies
  - O8 – Extra MSIE context menu items
  - O9 – Extra 'Tools' menuitems and buttons
  - O10 – Breaking of Internet access by New.Net or WebHancer
  - O11 – Extra options in MSIE 'Advanced' settings tab
  - O12 – MSIE plugins for file extensions or MIME types
  - O13 – Hijack of default URL prefixes
  - O14 – Changing of IERESSET.INF
  - O15 – Trusted Zone Autoadd
  - O16 – Download Program Files item
  - O17 – Domain hijack
  - O18 – Enumeration of existing protocols and filters
  - O19 – User stylesheet hijack
  - O20 – AppInit\_DLLs autorun Registry value, Winlogon Notify Registry keys
  - O21 – ShellServiceObjectDelayLoad (SSODL) autorun Registry key
  - O22 – SharedTaskScheduler autorun Registry key
  - O23 – Enumeration of NT Services
  - O24 – Enumeration of ActiveX Desktop Components

Command-line parameters:

- \* /autolog – automatically scan the system, save a logfile and open it
- \* /ihatewhitelists – ignore all internal whitelists
- \* /uninstall – remove all HijackThis Registry entries, backups and quit
- \* /silentautolog – the same as /autolog, except with no required user intervention

I think I have been hijacked.

I think I have been hijacked.

\* Version history \*

[v2.00.0]

- \* AnalyzeThis added for log file statistics
- \* Recognizes Windows Vista and IE7
- \* Fixed a few bugs in the O23 method
- \* Fixed a bug in the O22 method (SharedTaskScheduler)
- \* Did a few tweaks on the log format
- \* Fixed and improved ADS Spy
- \* Improved Itty Bitty Procman (processes are frozen before they are killed)
- \* Added listing of O4 autoruns from other users
- \* Added listing of the Policies Run items in O4 method, used by SmitFraud trojan
- \* Added /silentautolog parameter for system admins
- \* Added /deleteonreboot [file] parameter for system admins
- \* Added O24 – ActiveX Desktop Components enumeration
- \* Added Enhanced Security Configuration (ESC) Zones to O15 Trusted Sites check

[v1.99.1]

- \* Added Winlogon Notify keys to O20 listing
- \* Fixed crashing bug on certain Win2000 and WinXP systems at O23 listing
- \* Fixed lots and lots of 'unexpected error' bugs
- \* Fixed lots of improper functioning bugs (i.e. stuff that didn't work)
- \* Added 'Delete NT Service' function in Misc Tools section
- \* Added ProtocolDefaults to O15 listing
- \* Fixed MD5 hashing not working
- \* Fixed 'ISTSVC' autorun entries with garbage data not being fixed
- \* Fixed HijackThis uninstall entry not being updated/created on new versions
- \* Added Uninstall Manager in Misc Tools to manage 'Add/Remove Software' list
- \* Added option to scan the system at startup, then show results or quit if nothing found

[v1.99]

- \* Added O23 (NT Services) in light of newer trojans
- \* Integrated ADS Spy into Misc Tools section
- \* Added 'Action taken' to info in 'More info on this item'

[v1.98]

- \* Definitive support for Japanese/Chinese/Korean systems
- \* Added O20 (AppInit\_DLLs) in light of newer trojans
- \* Added O21 (ShellServiceObjectDelayLoad, SSODL) in light of newer trojans
- \* Added O22 (SharedTaskScheduler) in light of newer trojans
- \* Backups of fixed items are now saved in separate folder
- \* HijackThis now checks if it was started from a temp folder
- \* Added a small process manager (Misc Tools section)

[v1.96]

- \* Lots of bugfixes and small enhancements! Among others:
- \* Fix for Japanese IE toolbars
- \* Fix for searchwww.com fake CLSID trick in IE toolbars and BHO's
- \* Attributes on Hosts file will now be restored when scanning/fixing/restoring it.
- \* Added several files to the LSP whitelist

I think I have been hijacked.

I think I have been hijacked.

- \* Fixed some issues with incorrectly re-encrypting data, making R0/R1 go undetected until a restart

- \* All sites in the Trusted Zone are now shown, with the exception of those on the nonstandard but safe domain list

[v1.95]

- \* Added a new regval to check for from Whazit hijack (Start Page\_bak).

- \* Excluded IE logo change tweak from toolbar detection (BrandBitmap and SmBrandBitmap).

- \* New in logfile: Running processes at time of scan.

- \* Checkmarks for running StartupList with /full and /complete in HijackThis UI.

- \* New O19 method to check for Datanotary hijack of user stylesheet.

- \* Google.com IP added to whitelist for Hosts file check.

[v1.94]

- \* Fixed a bug in the Check for Updates function that could cause corrupt downloads on certain systems.

- \* Fixed a bug in enumeration of toolbars (Lop toolbars are now listed!).

- \* Added imon.dll, drwhook.dll and wspirtda.dll to LSP safelist.

- \* Fixed a bug where DPF could not be deleted.

- \* Fixed a stupid bug in enumeration of autostarting shortcuts.

- \* Fixed info on Netscape 6/7 and Mozilla saying '%shitbrowser%' (oops).

- \* Fixed bug where logfile would not auto-open on systems that don't have ..log filetype registered.

- \* Added support for backing up F0 and F1 items (d'oh!).

[v1.93]

- \* Added mclsp.dll (McAfee), WPS.DLL (Sygate Firewall), zklspr.dll (Zero Knowledge) and mxavlsp.dll (OnTrack) to LSP safelist.

- \* Fixed a bug in LSP routine for Win95.

- \* Made taborder nicer.

- \* Fixed a bug in backup/restore of IE plugins.

- \* Added UltimateSearch hijack in O17 method (I think).

- \* Fixed a bug with detecting/removing BHO's disabled by BHODemon.

- \* Also fixed a bug in StartupList (now version 1.52.1).

[v1.92]

- \* Fixed two stupid bugs in backup restore function.

- \* Added DiamondCS file to LSP files safelist.

- \* Added a few more items to the protocol safelist.

- \* Log is now opened immediately after saving.

- \* Removed rd.yahoo.com from NSBSD list (spammers are starting to use this, no doubt spyware authors will follow).

- \* Updated integrated StartupList to v1.52.

- \* In light of SpywareNuker/BPS Spyware Remover, any strings relevant to reverse-engineers are now encrypted.

- \* Rudimentary proxy support for the Check for Updates function.

[v1.91]

- \* Added rd.yahoo.com to the Nonstandard But Safe Domains list.

- \* Added 8 new protocols to the protocol check safelist, as well as showing the file that handles the protocol in the log (O18).

- \* Added listing of programs/links in Startup folders (O4).

- \* Fixed 'Check for Update' not detecting new versions.

[v1.9]

I think I have been hijacked.

I think I have been hijacked.

- \* Added check for Lop.com 'Domain' hijack (O17).
  - \* Bugfix in URLSearchHook (R3) fix.
  - \* Improved O1 (Hosts file) check.
  - \* Rewrote code to delete BHO's, fixing a really nasty bug with orphaned BHO keys.
  - \* Added AutoConfigURL and proxyserver checks (R1).
  - \* IE Extensions (Button/Tools menuitem) in HKEY\_CURRENT\_USER are now also detected.
  - \* Added check for extra protocols (O18).
- [v1.81]
- \* Added 'ignore non-standard but safe domains' option.
  - \* Improved Winsock LSP hijackers detection.
  - \* Integrated StartupList updated to v1.4.
- [v1.8]
- \* Fixed a few bugs.
  - \* Adds detecting of free.aol.com in Trusted Zone.
  - \* Adds checking of URLSearchHooks key, which should have only one value.
  - \* Adds listing/deleting of Download Program Files.
  - \* Integrated StartupList into the new 'Misc Tools' section of the Config screen!
- [v1.71]
- \* Improves detecting of O6.
  - \* Some internal changes/improvements.
- [v1.7]
- \* Adds backup function! Yay!
  - \* Added check for default URL prefix
  - \* Added check for changing of IERESet.INF
  - \* Added check for changing of Netscape/Mozilla homepage and default search engine.
- [v1.61]
- \* Fixes Runtime Error when Hosts file is empty.
- [v1.6]
- \* Added enumerating of MSIE plugins
  - \* Added check for extra options in 'Advanced' tab of 'Internet Options'.
- [v1.5]
- \* Adds 'Uninstall & Exit' and 'Check for update online' functions.
  - \* Expands enumeration of autoloading Registry entries (now also scans for ..vbs, .js, .dll, rundll32 and service)
- [v1.4]
- \* Adds repairing of broken Internet access (aka Winsock or LSP fix) by New.Net/WebHancer
  - \* A few bugfixes/enhancements
- [v1.3]
- \* Adds detecting of extra MSIE context menu items
  - \* Added detecting of extra 'Tools' menu items and extra buttons
  - \* Added 'Confirm deleting/ignoring items' checkbox
- [v1.2]
- \* Adds 'Ignorelist' and 'Info' functions
- [v1.1]
- \* Supports BHO's, some default URL changes
- [v1.0]

I think I have been hijacked.

I think I have been hijacked.

\* Original release

A good thing to do after version updates is clear your Ignore list and re-add them, as the format of detected items sometimes changes.

\*\*\*\*\*ANALYSIS\*\*\*\*\*

\* Trend Micro HijackThis v2.0.2 \*

See bottom for version history.

The different sections of hijacking possibilities have been separated into the following groups.

You can get more detailed information about an item by selecting it from the list of found items OR highlighting the relevant line below, and clicking 'Info on selected item'.

- R – Registry, StartPage/SearchPage changes
- R0 – Changed registry value
- R1 – Created registry value
- R2 – Created registry key
- R3 – Created extra registry value where only one should be
- F – IniFiles, autoloading entries
- F0 – Changed inifile value
- F1 – Created inifile value
- F2 – Changed inifile value, mapped to Registry
- F3 – Created inifile value, mapped to Registry
- N – Netscape/Mozilla StartPage/SearchPage changes
- N1 – Change in prefs.js of Netscape 4.x
- N2 – Change in prefs.js of Netscape 6
- N3 – Change in prefs.js of Netscape 7
- N4 – Change in prefs.js of Mozilla
- O – Other, several sections which represent:
  - O1 – Hijack of auto.search.msn.com with Hosts file
  - O2 – Enumeration of existing MSIE BHO's
  - O3 – Enumeration of existing MSIE toolbars
  - O4 – Enumeration of suspicious autoloading Registry entries
  - O5 – Blocking of loading Internet Options in Control Panel
  - O6 – Disabling of 'Internet Options' Main tab with Policies
  - O7 – Disabling of Regedit with Policies
  - O8 – Extra MSIE context menu items
  - O9 – Extra 'Tools' menuitems and buttons
  - O10 – Breaking of Internet access by New.Net or WebHancer
  - O11 – Extra options in MSIE 'Advanced' settings tab
  - O12 – MSIE plugins for file extensions or MIME types
  - O13 – Hijack of default URL prefixes
  - O14 – Changing of IERESSET.INF
  - O15 – Trusted Zone Autoadd
  - O16 – Download Program Files item
  - O17 – Domain hijack

I think I have been hijacked.

I think I have been hijacked.

- O18 – Enumeration of existing protocols and filters
- O19 – User stylesheet hijack
- O20 – AppInit\_DLLs autorun Registry value, Winlogon Notify Registry keys
- O21 – ShellServiceObjectDelayLoad (SSODL) autorun Registry key
- O22 – SharedTaskScheduler autorun Registry key
- O23 – Enumeration of NT Services
- O24 – Enumeration of ActiveX Desktop Components

Command-line parameters:

- \* /autolog – automatically scan the system, save a logfile and open it
- \* /ihatewhitelists – ignore all internal whitelists
- \* /uninstall – remove all HijackThis Registry entries, backups and quit
- \* /silentautolog – the same as /autolog, except with no required user intervention

\* Version history \*

[v2.00.0]

- \* AnalyzeThis added for log file statistics
- \* Recognizes Windows Vista and IE7
- \* Fixed a few bugs in the O23 method
- \* Fixed a bug in the O22 method (SharedTaskScheduler)
- \* Did a few tweaks on the log format
- \* Fixed and improved ADS Spy
- \* Improved Itty Bitty Procman (processes are frozen before they are killed)
- \* Added listing of O4 autoruns from other users
- \* Added listing of the Policies Run items in O4 method, used by SmitFraud trojan
- \* Added /silentautolog parameter for system admins
- \* Added /deleteonreboot [file] parameter for system admins
- \* Added O24 – ActiveX Desktop Components enumeration
- \* Added Enhanced Security Configuration (ESC) Zones to O15 Trusted Sites check

[v1.99.1]

- \* Added Winlogon Notify keys to O20 listing
- \* Fixed crashing bug on certain Win2000 and WinXP systems at O23 listing
- \* Fixed lots and lots of 'unexpected error' bugs
- \* Fixed lots of improper functioning bugs (i.e. stuff that didn't work)
- \* Added 'Delete NT Service' function in Misc Tools section
- \* Added ProtocolDefaults to O15 listing
- \* Fixed MD5 hashing not working
- \* Fixed 'ISTSVC' autorun entries with garbage data not being fixed
- \* Fixed HijackThis uninstall entry not being updated/created on new versions
- \* Added Uninstall Manager in Misc Tools to manage 'Add/Remove Software' list
- \* Added option to scan the system at startup, then show results or quit if nothing found

[v1.99]

- \* Added O23 (NT Services) in light of newer trojans
- \* Integrated ADS Spy into Misc Tools section
- \* Added 'Action taken' to info in 'More info on this item'

[v1.98]

I think I have been hijacked.

I think I have been hijacked.

- \* Definitive support for Japanese/Chinese/Korean systems
- \* Added O20 (AppInit\_DLLs) in light of newer trojans
- \* Added O21 (ShellServiceObjectDelayLoad, SSODL) in light of newer trojans
- \* Added O22 (SharedTaskScheduler) in light of newer trojans
- \* Backups of fixed items are now saved in separate folder
- \* HijackThis now checks if it was started from a temp folder
- \* Added a small process manager (Misc Tools section)

[v1.96]

- \* Lots of bugfixes and small enhancements! Among others:
- \* Fix for Japanese IE toolbars
- \* Fix for searchwww.com fake CLSID trick in IE toolbars and BHO's
- \* Attributes on Hosts file will now be restored when scanning/fixing/restoring it.
- \* Added several files to the LSP whitelist
- \* Fixed some issues with incorrectly re-encrypting data, making R0/R1 go undetected until a restart
- \* All sites in the Trusted Zone are now shown, with the exception of those on the nonstandard but safe domain list

[v1.95]

- \* Added a new regval to check for from Whazit hijack (Start Page\_bak).
- \* Excluded IE logo change tweak from toolbar detection (BrandBitmap and SmBrandBitmap).
- \* New in logfile: Running processes at time of scan.
- \* Checkmarks for running StartupList with /full and /complete in HijackThis UI.
- \* New O19 method to check for Datanotary hijack of user stylesheet.
- \* Google.com IP added to whitelist for Hosts file check.

[v1.94]

- \* Fixed a bug in the Check for Updates function that could cause corrupt downloads on certain systems.
- \* Fixed a bug in enumeration of toolbars (Lop toolbars are now listed!).
- \* Added imon.dll, drwhook.dll and wspirida.dll to LSP safelist.
- \* Fixed a bug where DPF could not be deleted.
- \* Fixed a stupid bug in enumeration of autostarting shortcuts.
- \* Fixed info on Netscape 6/7 and Mozilla saying '%shitbrowser%' (oops).
- \* Fixed bug where logfile would not auto-open on systems that don't have ..log filetype registered.
- \* Added support for backing up F0 and F1 items (d'oh!).

[v1.93]

- \* Added mclsp.dll (McAfee), WPS.DLL (Sygate Firewall), zklsp.dll (Zero Knowledge) and mxavlsp.dll (OnTrack) to LSP safelist.
- \* Fixed a bug in LSP routine for Win95.
- \* Made taborder nicer.
- \* Fixed a bug in backup/restore of IE plugins.
- \* Added UltimateSearch hijack in O17 method (I think).
- \* Fixed a bug with detecting/removing BHO's disabled by BHODemon.
- \* Also fixed a bug in StartupList (now version 1.52.1).

[v1.92]

- \* Fixed two stupid bugs in backup restore function.
- \* Added DiamondCS file to LSP files safelist.
- \* Added a few more items to the protocol safelist.

I think I have been hijacked.

I think I have been hijacked.

- \* Log is now opened immediately after saving.
  - \* Removed rd.yahoo.com from NSBSD list (spammers are starting to use this, no doubt spyware authors will follow).
  - \* Updated integrated StartupList to v1.52.
  - \* In light of SpywareNuker/BPS Spyware Remover, any strings relevant to reverse-engineers are now encrypted.
  - \* Rudimentary proxy support for the Check for Updates function.
- [v1.91]
- \* Added rd.yahoo.com to the Nonstandard But Safe Domains list.
  - \* Added 8 new protocols to the protocol check safelist, as well as showing the file that handles the protocol in the log (O18).
  - \* Added listing of programs/links in Startup folders (O4).
  - \* Fixed 'Check for Update' not detecting new versions.
- [v1.9]
- \* Added check for Lop.com 'Domain' hijack (O17).
  - \* Bugfix in URLSearchHook (R3) fix.
  - \* Improved O1 (Hosts file) check.
  - \* Rewrote code to delete BHO's, fixing a really nasty bug with orphaned BHO keys.
  - \* Added AutoConfigURL and proxyserver checks (R1).
  - \* IE Extensions (Button/Tools menuitem) in HKEY\_CURRENT\_USER are now also detected.
  - \* Added check for extra protocols (O18).
- [v1.81]
- \* Added 'ignore non-standard but safe domains' option.
  - \* Improved Winsock LSP hijackers detection.
  - \* Integrated StartupList updated to v1.4.
- [v1.8]
- \* Fixed a few bugs.
  - \* Adds detecting of free.aol.com in Trusted Zone.
  - \* Adds checking of URLSearchHooks key, which should have only one value.
  - \* Adds listing/deleting of Download Program Files.
  - \* Integrated StartupList into the new 'Misc Tools' section of the Config screen!
- [v1.71]
- \* Improves detecting of O6.
  - \* Some internal changes/improvements.
- [v1.7]
- \* Adds backup function! Yay!
  - \* Added check for default URL prefix
  - \* Added check for changing of IERESSET.INF
  - \* Added check for changing of Netscape/Mozilla homepage and default search engine.
- [v1.61]
- \* Fixes Runtime Error when Hosts file is empty.
- [v1.6]
- \* Added enumerating of MSIE plugins
  - \* Added check for extra options in 'Advanced' tab of 'Internet Options'.
- [v1.5]
- \* Adds 'Uninstall & Exit' and 'Check for update online' functions.
  - \* Expands enumeration of autoloading Registry entries (now also scans for

I think I have been hijacked.

I think I have been hijacked.

..vbs, .js, .dll, rundll32 and service)

[v1.4]

\* Adds repairing of broken Internet access (aka Winsock or LSP fix) by New.Net/WebHancer

\* A few bugfixes/enhancements

[v1.3]

\* Adds detecting of extra MSIE context menu items

\* Added detecting of extra 'Tools' menu items and extra buttons

\* Added 'Confirm deleting/ignoring items' checkbox

[v1.2]

\* Adds 'Ignorelist' and 'Info' functions

[v1.1]

\* Supports BHO's, some default URL changes

[v1.0]

\* Original release

A good thing to do after version updates is clear your Ignore list and re-add them, as the format of detected items sometimes changes.