

Prevent Computer Hijackings

As mentioned earlier on this page, I strongly recommend that you visit <http://www.microsoft.com/security/> on a regular basis to check for the latest in the ongoing battle between Microsoft and those who would hijack your browser.

For a start.....

Update to Internet Explorer 6. Most sites that try to hijack your home page will now trigger a 'do you want to do this' warning message that lets you stop the hijacking. The sneaky backgroundactivex downloads that are often used by hijack sites to install spyware will also trigger a 'do you want to do this' install window.

Make sure that your Java VM is at least version 3805 to protect against a vulnerability that allows website operators to change your home page and several other vulnerabilities.

[Where to get the JAVA VM](#)

The corresponding Technet article can be found here:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-013.asp>

The latest cumulative patch for Internet Explorer - issued 22 August 2002 - can be found here:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q323759>

Further details about the patch can be found here:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-047.asp>

Warning: The above critical update can cause problems when "connecting to terminal services from a Web Page" - more information here:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;q328002>

Patches generally CANNOT be removed.

You can install individual patches, or you can wait for the cumulative patches to be released, which occurs every month or so.

Some known problems caused by recent patches include:

Q319847 MS02-009 May Cause Incompatibility Problems Between VBScript and Third-Party Applications

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q319847>

Q318808 Security Update MS00-024 Causes Problems with the SHGetFolderPath() Function in Shfolder.dll

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q318808>

Hewlett Packard

Iexplore caused an invalid page fault in URLMON.DLL

<http://support.microsoft.com/support/kb/articles/q309/4/76.asp>

GP Fault in Module Gdi.exe Printing from Internet Explorer

<http://support.microsoft.com/support/kb/articles/q261/1/56.asp>

Table Borders May Not Print Properly in Internet Explorer [Q257036]

<http://support.microsoft.com/support/kb/articles/q257/0/36.asp>

Missing Text When Printing Web Pages to HP PhotoSmart P1000 [Q254772]

<http://support.microsoft.com/support/kb/articles/q254/7/72.asp>

Problems Printing to HP DeskJet if BD Denver Font Is Damaged [Q271582]

(Iexplore caused an invalid page fault in GDI.EXE)

<http://support.microsoft.com/support/kb/articles/q271/5/82.asp>

Easy Internet Access

Windows 95 Stops Responding with IOD Shockwave Installation [Q250777]

<http://support.microsoft.com/support/kb/articles/q250/7/77.asp>

FileBox Xtender (v1.50.02)

Doesn't work with IE6 - corrupting the file - open and file - save dialogue boxes

Netscape 4.06 Tuneup

Error Message with Netscape 4.06 TuneUp Installed [Q262900]

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q262900>

Trend Micro PC-cillin

The POP3 Server Information Does Not Change and Error Messages Appear in Outlook Express 5.5 - (Cannot log on using Secure Password authentication and Unable to locate the POP3 server you specified)

<http://support.microsoft.com/support/kb/articles/q312/3/47.asp>

The programme can also stop downloads from working if the Real Time Monitor is running in the background.

Encompass Monitor Service (Encmonitor)

Causes the following errors:

Monitor caused an Invalid Page Fault in module Kernel32.dll *or* Windows Sockets Initialization failed

<http://support.microsoft.com/support/kb/articles/q306/6/14.asp>

Eudora can interfere with the text display size in IE

Font Changes Size in Internet Explorer 5 Using Eudora Pro 4.1 or 4.2

<http://support.microsoft.com/support/kb/articles/Q226/7/97.asp>

New.Net and SaveNow

Causes the following errors:

IEXPLORE caused an invalid page fault in module Unknown *or* SAVENOW executed an invalid instruction in module Unknown

<http://support.microsoft.com/support/kb/articles/q302/4/63.asp>

Quickview Plus

"Invalid Page Fault in Module Urlmon.dll" Error Message When Starting Internet Explorer

<http://support.microsoft.com/support/kb/articles/q254/4/90.asp>

Juno Software

Causes the following error message:

Explorer.exe caused an invalid page fault in explorer.exe at 0157F: 00401F31

<http://support.microsoft.com/support/kb/articles/q296/2/11.asp>

he Trouble With Spyware & Advertising-Supported Software

Spyware is a generic term typically describing software whose purpose is to collect demographic and usage information from your computer, usually for advertising purposes. The term is also used to describe software that 'sneaks' onto the system or performs other activities hidden to the user. Spyware apps are usually bundled as a

hidden component in mis-labeled "freeware" and shareware applications¹ downloaded from the Internet--a spyware module may be active on your computer at this moment without your knowledge. These modules are almost always installed on the system secretly, suggesting that spyware companies know how users feel about such software and figure that the best/only way to ensure its widespread use is to prevent the end-user from discovering it.

Consumer Privacy Implications

Advertising-supported software, if done properly, is a unique and viable business model in which software developers can make money without requiring the end-user to pay for the software. However, the key words are if done properly, which is often not the case. While it may come as no surprise that adware uses your 'Net connection to download ads, you would have good reason to be concerned about the large amounts of data flowing in the *other direction*. Several adware applications have been known to secretly snoop around areas of your computer they don't belong, including your browser history.

As much as current spyware modules do to steal away users' privacy, they have the potential to do even more. Spyware exists as an *independent, executable program on your system*, and has the capability to do anything any program can do, including monitor keystrokes, arbitrarily scan files on your hard drive, snoop other applications such as word-processors and chat programs, read your cookies, change your default homepage, interface with your default Web browser to determine what Web sites you are visiting, and monitor various aspect of your behaviour, "phoning home" from time to time to report this information back to the spyware's author. It can even notify the spyware company of any attempts to modify or remove it from the system. All the information obtained by the spyware can be used by the spyware author for marketing purposes, or sold to other companies for a profit.

In short, spyware can spy on any aspect of your computer use, and is not limited in the ways Web sites are when it comes to gathering personal data. While a Web site can gather limited demographic and statistical data automatically provided by the Web browser and Internet protocols, and read cookies set by its own domain, spyware can "see" and disclose any data on, entering or exiting your computer. This information can then be used for just about any purpose, even sold to the highest bidder!

User-Hostile Behaviour

Many adware apps install separate advertising components on your system, that run--downloading ads and wasting system resources--even if you're not using the software that installed them. Often, these components remain installed and continue to perform their unsightly duties *even after the associated app has been uninstalled!* Some adware companies have even gone so far as to create "Advertising Trojan Horses", virus-like software programs that stealthily install themselves on your computer to perform unwanted advertising functions and violate your privacy *whether you've installed the advertising-supported software or not*. Advertising trojans make clandestine connections to adservers behind your back, consume precious network bandwidth and may compromise the security of your data. The latest versions of these "ad-viruses" operate in full stealth and are nearly impossible to detect without advanced knowledge of the system environment. These include the TimeSink/Conducent TSADBOT and the Aureate advertising trojans. One spyware module has been known to spoof a Windows system process so that it cannot be terminated and does not appear on Windows' End Task (Ctrl-Alt-Del) dialogue.

Spyware modules have been implicated in computer problems including system slowdown, Illegal Operation errors, browser crashes, and even the "Blue Screen Of Death". While normal system stability has usually returned when the interfering spyware modules were deleted, one spyware product in particular will *disable your Internet access if you try to delete it!*

Potential Violations of Child Protection Laws

Most spyware-infested software is targeted toward adults. However, the user that sits down at the computer can be of any age, and the spyware modules have no good way of knowing who is at the machine and what legal protections are provided to him or her. In particular, laws in the United States prohibit the collection of personal information from children under 13 without the written permission of a parent or guardian. However, most spyware does not make any provisions for users whom they are not legally permitted to collect data from, a huge potential problem when it comes to laws such as the U.S. Child Online Privacy Protection Act (COPPA).

Security Issues

Again, since a spyware program is an independent executable program residing on your PC, it will have all the privileges of the user that installed it. On the majority of single-user systems, including Windows 95 and 98, these privileges allow software to read, write and delete files, download and install other software, change the default homepage, interrogate other devices attached to the system, or even format the hard drive. While multi-user systems such as Windows NT can limit the spyware's abilities somewhat, it can still do anything the user who installed it can--a scary thought indeed if an application containing spyware was unknowingly installed by someone with Administrator privileges.

Some spyware modules include a number of insecure features, including so-called AutoInstall or AutoUpdate functions that can secretly download and install ANY arbitrary program on the user's system. This opens the door for further abuse of the system by malicious crackers or additional spyware programs! In particular, competent security experts including Gibson Research Corp. have proven how simple it is for a malicious user to hijack this capability to upload and run ANY program on a user's system!

Software License (dis)Agreement

Some aspects of spyware activity are legally questionable. While software installing a spyware module should disclose this fact to the user and offer the option of refusing, any such disclosure is often buried in a long and densely-worded License Agreement, slipped in among page after page of mind-numbing legal jargon on such topics as copyright, distribution, disassembly, reverse-engineering, government and restricted rights, disclaimer of fitness for a particular purpose, and similar topics of little relevance to the average user². Additionally, the actual spyware notice is often written in such a roundabout, flowery and disingenuous manner that a reasonable user would have no reason to take special interest in it³. To most users, a phrase such as *"may include software that will occasionally notify you of important news"* is NOT equivalent to *"will place a stealthy Trojan Horse on your system that you can't get rid of, which will collect information about you and send it to us, and allow us to bother you with targeted advertisements all day"*. Once the spyware has been "disclosed" and the spyware company can argue that the user has "agreed" with it by continuing beyond the License Agreement, it is much more immune from potential lawsuits from users who accepted the license and installed the software, blissfully unaware of the spy that would now be living on their computers. Some spyware companies do not mention the spyware at all, often pointing the finger at the company whose software utilizes it for not disclosing it. (How convenient!)

1 While the most common culprits are shareware and "freeware" apps, paid-for commercial software has been known to contain spyware as well.

2 The majority of a software License Agreement refers to government users, corporations, distributors and software hackers. It can be safely assumed that a majority of users have no interest in disassembling their software, porting it to other operating systems or hardware architectures, or other such activities extensively droned on about in the License Agreement.

3 See Steve Gibson's explanation and example of "Fine Print Funny Business": <http://grc.com/oo/fineprint.htm> . (Note that the example Steve gives eventually does, albeit in dense wording, disclose what's going on. Be aware that many spyware agreements are even less forthcoming about the nature of their software!)

All trademarks are hereby acknowledged as the property of their respective owners." So don't even THINK about suing me :)