Where Windows Malware Hides and Other Tricks

(5/30/06)

By Roger A. Grimes
Author of Professional Windows Desktop and Server Hardening (WROX)

Categories Summary
Applications-6
File-32
Folders-14
Other-10
Registry Locations-92
Total-145

Area	Name	Function	Notes
Application	Archive files	Malware can be hidden or launched from within archive file formats.	1. Archive file formats, such as Pkzip, Cab, Stuff-it, and Tar manipulate/obscure the original file and can allow malicious files to bypass detection mechanisms. 2. Malware files can be hidden in nested archive files, and won't be detected unless detection mechanisms use recursive scanning; even then the key is how "deep" the recursive scanning will try. 3. Denial of service attacks and detection bypass have been successfully caused by overly large uncompressed file names, overly "deep" directory structures, etc. 4. Exploded archive files have also be used to overwrite other legitimate files in directories the user did not intend.
Application	Auto-run application files	Malware can launch from any auto-running file associated with a particular application.	1. Examples include: MS-Office auto-run macros 2. Archive files can also have auto-run files executed after the archive is opened.
Application	Embedded or linked files	Many applications and their file formats allow other document types to be embedded/executed	1. For instance, MS-Word files can have MS-Excel files embedded that are automatically executed when the Word file is opened.

Area	Name	Function	Notes
Application	Microsoft Word	Embedded scripting can be used to manipulate remote file systems; to write over, copy, and delete files on the system which opened the MS-Word file.	1. It has been demonstrated that a maliciously crafted MS-Word file can secretly send a named document to a remote intruder.
Application	Cross-site scripting (XSS)	HMTL-based forms and email allow malicious scripts to be embedded by a rogue hacker and executed on other computers who innocently view the HTML code.	Very common malware vector. Most only HTML-based email services have been the victim of one or more cross-site scripting attacks. Can only be defeated if HTML-based service prevents the insertion of malicious scripting into input fields that are later displayed to other viewers.
Application	Outlook	Malware can manipulate Outlook to send other recipients malicious emails.	Can be done by malware becoming an Add-in (ex. Hotbar adware) Can be done by manipulating SMTP server settings or HOST file and intercepting sent email. Can be done by adding malicious script as an unauthorized email signature (ex. JS.Fortnight worm). This exploit occurs more in Outlook Express than Outlook.
File	Alternate Data Streams	Malware can hide itself in the Alternate Data Streams (ADS) of a Windows file.	1. ADS example: regularfile.exe:malware.exe 2. If executed, ADS process (i.e. malware.exe) will appear as regularfile.exe:malware.exe in Task Manager in XP and above (but as regularfile.exe in 2000 and NT). 3. ADS files do not appear in Windows Firewall exception list, only regularfile.exe will appear. 4. There is no built-in Windows utility to show ADS files, but many companies, including www.sysinternals.com and Microsoft (Resource Kits), have tools to do so.
File	Any executable	Viruses can modify any executable, script file, or macro file to run.	1. Works in DOS and any version of Windows 2. Microsoft system executables cannot be modified in Win ME and W2K and above because of Windows File Protection (System File Protection in Win ME).

Area	Name	Function	Notes
File	Autoexec.bat	Loads real-mode programs prior to Windows loading	1. Works with DOS, Win 3.x, and Win 9x 2. Replaced by Autoexec.nt in NT and above, and even then only gets called when a DOS session is started. 3. Stored in root directory. 4. Not commonly used by malware today 5. If used by malware, malware often inserted dozens of blank lines to the end of the file and pushed malicious commands below the normal viewing area of the file to fool inspectors. 6. Win 9x looks for Autoexec when it starts, not necessarily Autoexec.bat; so an Autoexec.com could be run instead.
File	Autoexec.nt	File allows real-mode programs to be associated with specific 16-bit or 32-bit command shell sessions.	1. Works with NT family 2. Stored in %windir%\system32 3. Not common with malware
File	AUTORUN.INF	Autorun file, runs commands or programs referenced by open= or shellexecute= after inserting (or choosing to Autoplay) media storage (i.e. CD-ROM discs).	1. Works with Win 9x and above, and can work with any type of media. By default, doesn't work with most USB memory keys. 2. What media works with the Autorun.inf file can be modified using registry edits and third party apps (like TweakUI). 3. Not widely exploited by malware, but the potential exists.
File	Batch or Command files	Will run listed programs or commands	Batch file viruses will search for these types of files to infect. Although not rare, most malware programs do not use this vector anymore.
File	Boot.ini	File used by NT OS family to determine which OS to load and where OS located on disk	1. So far not successfully manipulated by malware, but is sometimes the target of payload damage attacks
File	Bootsect.dos	DOS boot sector on NT systems that dual boot with earlier versions of Windows or DOS.	1. Could be infected by viruses in early versions of Windows and DOS. 2. Pointed to by Boot.ini file in dual-boot scenarios in NT and above.

Area	Name	Function	Notes
			3. In reality, any type of code can be reference to run in the Boot.ini file (for example Recovery Console). 4. Not widely exploited by malware.
File	Command.com	Default DOS shell in Windows 9x and below	1. Could be infected by viruses in early versions of Windows and DOS. 2. Not possible in Win ME and W2K and above because of Windows File Protection
File	Config.nt	File allows real-mode programs or drivers to be associated with specific 16-bit or 32-bit command shell sessions.	1. Works with NT family 2. Stored in %windir%\system32 3. Not common with malware
File	Config.sys	Loads real-mode programs or drivers prior to Windows load	1. Works with DOS, Win 3.x, and Win9x. 2. Replaced by Config.nt file in newer OSs. 3. Stored in root directory. 4. Not commonly used by malware today 5. If used by malware, malware often inserted dozens of blank lines to the end of the file and pushed malicious commands below the normal viewing area of the file to fool inspectors.
File	Desktop.ini	Used to customize folder behavior. It is meant to allow users to customize folder appear and behaviors, but can be used to hide files and auto-launch programs when referred to folders are viewed.	1. Several worms (ex. WuKill, Rusty, Opposum, and Expobot) use Desktop.ini to launch their malicious executables when a related folder is viewed. 2. Can be used to hide files and auto-launch programs. 3. Desktop.ini is usually marked hidden. 4. Folder.htt is used instead of desktop.ini when desktop is in “Web view”. 5. MSDN link (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/Shell/programmersguide/shell_basics/shell_basics_extending/custom.asp)
File	DOSSTART.BAT	Would load listed real-mode programs when starting a command prompt session or	1. Works with Windows 3.x and Win 9x family. 2. Located in %Windir% 3. Superceded by registry key.

Area	Name	Function	Notes
		when booting to a Command prompt session during Safe mode.	
File	HOSTS	Used to place static DNS resolution entries	1. Works with Win 9x and above 2. Located in %windir%\System32\drivers\etc in NT and above 3. Malware or adware will often modify this file to redirect user or program to bogus location when associated DNS entry is queried.
File	IERESET.INF	Used as the "initial" values when Internet Explorer is *reset*. Can be manipulated to place malicious entries.	1. Not used in the wild, yet. 2. Proposed by Andrew Aronoff of SilentRunners.org 3. Default security is Read & Execute by normal users, requires Admin rights to modify.
File	LMHOSTS	Used to place static NetBIOS resolution entries.	1. Works with Win 9x and above 2. Not commonly used by malware, but could be modified to do bogus NetBIOS name resolution redirection. 3. Located in %windir%\System32\drivers\etc in NT and above
File	Msdos.sys, Io.sys	Default boot files in earlier versions of Windows and DOS	1. Could be infected by viruses in Windows 3.x and DOS. 2. In Win9x, Msdos.sys is used as an editable configuration file, not as a system file. 3. In Win 9x, the original Msdos.sys and Io.sys files are renamed Io.dos and Msdos.dos. If you boot to DOS with Win 9x, the files were renamed Winboot.sys and Msdos.w40. Could end in other extensions including .Wos and .App. 4. In Win 9x, if Winboot.ini exists (it is normally deleted by the OS after a completed setup), it can override the use of Msdos.sys. 5. Not used in NT, 2000, and above, but may be present because of upgrades or dual booting situations. 6. Not very dangerous these days.
File	Non-printable characters in file	Several computer defense	1. It has been demonstrated on several antivirus

Area	Name	Function	Notes
	name	programs (e.g. antivirus) are unable to scan files using un-printable or extended ASCII characters in the name	programs (fortunately, not the most popular ones) that non-printable characters can fool or prevent computer defense programs from accurately detecting malware.
File	Normal.dot or any .dot file	Microsoft Word document template	2. Used by macro viruses 3. Not commonly manipulated anymore because default MS-Office security minimized success of macro viruses
File	Ntldr	NT family OS boot code loader	1. So far not successfully manipulated by malware, but is sometimes the target of payload damage attacks 2. Protected by Windows File Protection.
File	Long path name trick or program.exe trick	If long path names with space in the name are not included in quotes, many programs, will attempt a systematic execution search that could lead to the wrong file (possibly malicious) being executed.	For example look at the following command: C:\program files\windows media player\wmplayer If unquoted, Windows tries the following: 1st try Execute: c:\program.exe Arg1: files\windows Arg2: media Arg3: player\wmplayer 2nd try Execute: "c:\program files\windows.exe" Arg1: media Arg2: player\wmplayer 3rd try Execute: "c:\program files\windows media" Arg1: player\wmplayer 4th try Execute: "c:\program files\windows media player\mwplayer.exe" If c:\program.exe exists, it will be executed instead of the intended program. XP SP2 will actually warn you about files like c:\Program.bat, or c:\Program.exe, but not of

Area	Name	Function	Notes
			c:\program files\internet.exe. Example created by Bill Sanderson (bill_sanderson@msn.com).\ Familiar to earlier spawning (or twin) virus exploits in the days of MS-DOS and Windows 3.1x First noted by iDefense (http://www.idefense.com/application/poi/display?id=340&type=vulnerabilities&flashstatus=true)
File	Name tricks	Various tricks can fool unsuspecting users	1. File names can include unprintable and undisplayable characters, so that the real name is obscured. 2. Files can be called .exe, .com, etc. with no file name, just an extension. If a file is named something like \Program files\Internet Explorer\.exe, it might appear as Internet Explorer\ tricking users. Thanks to edupb2002@hotmail.com for this hint. 3. File names can contain what looks like multiple extensions (e.g. Readme.txt.exe) and only the last extension controls the file type. 4. File names can be extra long, pushing true name or extension off Task Manager column screen and other tools (e.g. Readme.txt .exe)
File	Internet shortcut trick	Can be used to override HOSTS and DNS resolution to run local code.	1. By creating an Internet shortcut on the desktop, malware can override DNS and HOSTS file resolution. 2. Example, create a desktop shortcut with the name of www.aol.com, but make it start notepad.exe. the program that it starts. Then to go Internet Explorer and type in www.aol.com. It will start Notepad instead www.aol.com. 3. Essentially, any desktop shortcut can be referenced by typing it in Internet Explorer, because of the

Area	Name	Function	Notes
			integration between IE and Windows Explorer. 4. Although I have not tested, some suggest this bug will not work in Windows Vista. 5. Thanks to Jose Antunes for this entry.
File	OLE2 document trick	OLE2-formatted documents will be opened in their correct associated application if no extension is chosen	5. Many applications, especially Microsoft applications, use the OLE2 file format, including Microsoft Office applications, MSHTA, SHS, and SHB files. 6. Files with an OLE2 format will be run by the related application (as indicated by the OLE2 file's embedded OLE2 Root Entry CLSID value) regardless of the file name or extension. Thus harmless.txt could really be a macro virus or hta malware script. 7. The OLE2 file format is also known as Compound Document file format. 8. OLE2 documents are essentially their own little file systems ("file system within a file"), resembling something like at FAT disk subsystem with their own root entries and subsections and files. 9. The OLE2 trick is used in the wild by spammers, etc. 10. The Root Entry CLSID can be found in OLE2 files following string label R.o.o.t. .E.n.t.r.y. 11. Only works in GUI, not on command-line.
File	Protected File Names	Several program names, when running, cannot be killed in Task Manager, complicating removal.	Windows Task Manager will not allow the following program names to be killed: Winlogon.exe, Lsass.exe, Csrss.exe, Smss.exe (there could be more). Task Manager protects any program (i.e. trojan) from being killed if it has one of those names, regardless of legitimacy or program location. It would be simple for MS to fix, but they haven't, and they have known for years.
File	Rasphone.pbk	Can be used to modify dial-up network settings, including	Located in %UserProfile%\Application Data\Microsoft\Network\Connections\Pbk folder.

Area	Name	Function	Notes
		which DNS servers (IpDnsAdress and IpDns2Address) the dial-up connection uses and to place unauthorized long distance calls.	Don't forget to look in AllUsers profile. Trojans and malicious "Dialer" programs frequently manipulate this phonebook file, including Flush.D trojan and HotPleasure Dialer. Can be present with Windows 9x and above PCs. Key is not present (or a threat) unless you use Dial-up networking.
File	SYSTEM.INI [boot] scrnsaver=	If referenced by 16-bit Windows applications, will load screensaver listed	Works with Windows 3.x and Win 9x family. Located in %Windir% Screensaver files usually end with .SCR, .EXE, or .DLL extensions. Common malware vector in the Win 9x days. Replaced by registry entry in NT family.
File	SYSTEM.INI [boot] shell=	If referenced by 16-bit Windows applications, will load command shell listed (e.g. explorer.exe).	1. Works with Windows 3.x and above 2. Located in %Windir% 3. Only referenced by 16-bit Windows programs. 4. Superseded by registry entries in NT and above
File	WIN.INI [windows] load=, run=	If referenced by 16-bit Windows applications, will execute programs listed. Run= loads programs in maximized state, load= runs programs in minimized state	1. Works with Windows 3.x and above 2. Located in %Windir% 3. Only referenced by 16-bit Windows programs. 4. Superseded by registry entries in NT and above
File	Wininit.ini	Contains pending file operations (e.g. rename, copy, etc.) to be executed on the next reboot of Windows	1. Works with Win 9x and NT, but not in W2K or above 2. Located in %windir% 3. Replaced by registry key in later version of Windows 4. For more information, see http://support.microsoft.com/kb/140570.
File	Winsock.dll or Winsock2 service provider dlls	Used by Windows for network communications	1. Often used by trojans for their dirty work. 2. Usually located in C:\%Windir%\System32 and protected by Windows File Protection in Win ME and W2K and above. Trojan versions may be located else where (e.g. %Windir%\System or %Windir% folder).

Area	Name	Function	Notes
			3. Trojan Winsock service providers can be added to Windows and can manipulate any network communications. a. Can be removed by Winsock service provider cleaners, like Lsp-fix.
File	WINSTART.BAT	Would load listed real-mode programs prior to Windows loading or when user exited command prompt session.	1. Works with Windows 3.x and Win 9x family. 2. Located in %Windir% 3. Superceded by registry key.
Folder	%Windir%\Favorites*.url %UserProfile%\Favorites*.url %Windir%\Favorites\Links*.url %UserProfile%\Favorites\Links*.url	Lists Favorites in Internet Explorer	1. Often manipulated by adware, but has also been manipulated by malware
Folder	%Windir%\Start Menu\Programs\Startup %Windir%\All Users\Start Menu\Programs\Startup %USERPROFILE%\Start Menu\Programs\Startup %ALLUSERSPROFILE%\Start Menu\Programs\Startup	Default Startup folders; any program or command listed in one of these folders will be automatically executed when the user logs on	1. Works with Win 3.x and above, depending on default location for the particular version of Windows. a. Default is C:\Documents and Settings\%userprofile%\Start Menu\Programs\Startup in Windows 2000 and above b. Default is C:\%windir%\%userprofile%\Start Menu\Programs\Startup in NT. c. Default is %windir%\Start Menu\Programs\Startup in Win 9x family. 2. Startup folder location determined by registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
Folder	Recycler	Recycle Bin's temporary storage location for deleted files and folders	1. Often used by malware to store malicious code 2. Earlier versions of antivirus scanners would often skip the Recycle Bin storage area, and hence,

Area	Name	Function	Notes
			escape detection.
Folder	System System32 %Windir%	Malware often writes itself to Windows system directories	Non-admins usually do not have permissions to write to System folders In Win ME and W2K and above, because of Windows File Protection, legitimate system files cannot be overwritten, deleted, renamed, or modified. But new files can be written if program has Write access. By default, most users have Read & Execute permissions to System folders.
Folder	System Volume Information	Can be used by hackers or malware to hide malicious programs	1. By default, only System account has access. 2. Does not have "auto-launching" capabilities, only a hiding place 3. Thanks to reader Eric Case for this entry
Folder	Tasks	Lists Task Scheduler Tasks	1. Works with Win 3.x and above 2. Located in %Windir%
Folder	Temporary Internet Files	Malicious files are often stored/hidden in Internet Explorer's Temporary Internet Files (TIF) folder.	1. In 2000 and above, TIF is C:\Documents and Settings\<logonname>\Local Settings\Temporary Internet Files 2. Can be modified in Internet Explorer 3. If malware exploits System account (i.e. using a buffer overflow) and uses IE or Wininet API's, the TIF location will be located under the Default User or Network Service profile directories (which is hidden by default).
Other	ActiveX Control	Installed ActiveX Control	1. If already installed, may be able to re-install other malware/spyware automatically even after removal. 2. May need to set Kill Bit to defeat.
Other	Defensively Positioned Dialog Boxes	Malware often uses various programming "tricks" to cover up legitimate warning boxes or to trick the user into accepting a command that allows malware to enter the system when it otherwise shouldn't.	1. For example, several different methods have been used in Internet Explorer, to cover up IE warning messages or legitimate warning dialog boxes with "fake" dialog boxes that cover up the legitimate dialog box. The trick causes the end-user to miss the warning or to allow a malicious process that they otherwise wouldn't. One example IE method is:

Area	Name	Function	Notes
			a. Detect that the user is typing on the keyboard. b. Redirect to a malicious ".bat" file. c. In a new thread, force the browser to consume a large amount of CPU resources via a simple loop statement. This causes the upcoming file download dialog to be delayed. d. The user eventually presses the "r" key which is a keyboard shortcut for opening the downloaded file. The download dialog has not yet been shown for the user when this event occurs. e. The loop statement stops causing the download dialog to be visible and the keyboard shortcut event is processed. f. The malicious ".bat" file is launched. 2. This can happen with any program, but attackers seem to focus on Internet browsers. Both Internet Explorer and Firefox have been victims of these types of attacks. 3. For an example, see http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2829
Other	Executable pathway	PATH statement determines what paths OS should try if file is not found in default directory it was called from (i.e. Frog.exe vs. C:\Program Files\Frog.exe)	1. Was a bigger problem in the latter days of DOS (.bat, .com, .exe). 2. Some malware programs (ex. Spawner or twin viruses) rely on defects in the way Windows executes files when only the relative file name or path is given (ex. Frog.exe vs. C:\Program Files\Frog.exe) 3. PATH statement can be set by DOS PATH command (located under Environmental variables in NT family) or by registry key. 4. In Win9x and earlier, autoexec.bat file could be modified to modify path statement. 5. Can still be a problem today a. For example, some malware places itself in default application directories, which the application executes instead of the

Area	Name	Function	Notes
			legitimate program executable b. One trojan placed its malicious code in the user's My Documents folder. Because the malware was named after a legitimate MS-Word executable, MS-Word would always load it first instead of the legitimate version located under Program Files.
Other	Hidden files	Hidden (or system) files/folders will not appear to casual searches	1. Dir *.* /ah /s will search and reveal all hidden files 2. Many legitimate files are marked as hidden or system. Mostly concerned with hidden executables, script, or batch files in root, %Windir, or System32. 3. You can use Windows Explorer or Attrib.exe to unhide files.
Other	Layered Service Provider (LSP)	Malware can insert itself as a LSP program, which can intercept any network traffic heading into and out of a PC	1. Several trojan and spyware programs, such as Riler (http://securityresponse.symantec.com/avcenter/venc/data/trojan.riler.html) and Daqa (http://secunia.com/virus_information/10835/win32.daqa.a) use the LSP as a hiding place. 2. You can inspect and repair the LSP area using a program called LSP-Fix (http://www.cexx.org/lspfix.htm).
Other	System Restore	XP/ME Restore Feature may inadvertently restore malware located in older restore copies	1. Most AV and malware remove software programs suggest turning off this feature prior to any active cleanup 2. Is enabled by default, and is usually a good thing to have running unless you need the storage or CPU resources. 3. Can be enabled or disabled manually, by regedit, or by GPOs.
Other	Task Scheduler	Will run listed programs and commands	4. Sometimes used by malware to re-load malware at a predetermined time interval or to gain initial access 5. Some scheduled tasks are run in the System context allowing privilege escalation attacks.
Other	Trusted Publisher	Vendors listed here can	1. Be very cautious about which vendors are listed

Area	Name	Function	Notes
		execute programs without prompting end-user for approval.	here, allows them to execute any program without approval from end-user.
Other	Unusual folder/file names	Hackers and malware often use unusual names to hide malicious files and folders	1. Some tricks fool Windows-GUI, some command prompt, so both. 2. Be wary of sound-alikes (svchosts.exe, win.exe, win32.exe, service.exe, users32.dll etc.). 3. Be wary of legitimate file names located in the wrong directory (for example, svchost.exe located in %windir% instead of System32). 4. Overly long file names that make file name appear to be blank or push file name or extension off screen. 5. Files with multiple extensions (e.g. malware.txt.ext) 6. Files with incorrect extensions can still be executed at command prompt. 7. Files with non-standard character sets (http://weblogs.asp.net/robert_hensing/archive/2005/01/10/350359.aspx). 8. Files with incorrect extensions (i.e. a readme.txt that is really a .dll file or vice-versa). 9. Files with invalid dates (i.e. before 1/1/1980 or well into future). a. Windows Search GUI's date filter will not find files with dates before 1/1/1980.
Other	URL Monikers	URL Monikers can be added to Internet Explorer to load associated programs when a particular keyword is typed.	1. Internet Explore can be modified to allow keywords typed in the URL to launch associated programs 2. Also known as URL handlers 3. For more information, see http://msdn.microsoft.com/library/default.asp?url=/workshop/networking/moniker/monikers.asp 4. Malicious coded web sites or HTML emails can launch programs to them manipulate malicious data files.

Area	Name	Function	Notes
			5. For example, AOL's Instant Messenger program, AIM, installs a url handler called AIM://. It has been used to load buffer overflows known to be successful with particular programs. 6. Associated program need only be installed, not even used, to be launched. 7. HKCR\<urlhandler>\shell\open\command is registry location for URL handlers
Registry	HKLM\Software\Classes\<fileext>NeverShowExt HKCR\<fileext>NeverShowExt HKCU\Software\Classes\<fileext>NeverShowExt	Real file extensions can be hidden	1. Although most users know that Windows allows registered file extensions to be hidden (the default), most users don't know about the "super hidden" extension attribute which allows selected files (dozens of files types including SHS, SHB, SHC, LNK, PIF, XNK, and several shortcut and CLSID files) to hide their extensions even if you told Windows not to hide file extensions. 2. The super hidden file attribute can be enabled by creating a NeverShowExt registry entry under HKCR\<fileext>. 3. Overrides the related AlwaysShowExt if it is present. 4. To disable, search for and delete any occurrence of the NeverShowExt key under HKLM or HKCR.
Registry	HKLM\System\CurrentControlSet\Control\WOW\cmdline HKLM\System\CurrentControlSet\Control\WOW\wowcmdline	Allows 16-bit DOS and Windows apps to be launched from these keys	1. Thanks to Andrew Aronoff of www.silentrunners.org for this entry.
Registry	HKLM\Software\Classes\Folder\shellex\ColumnHandlers	Launch point for programs	2. Reported by Andrew Aronoff of www.silentrunners.org
Registry	HKCU\Control Panel\Desktop Scrnsave.exe=	Will load listed programs or commands when screensaver is configured	3. Not commonly used by malware 4. Used by Petch trojan (http://securityresponse.symantec.com/avcenter/venc/data/w32.petch.b.html).
Registry	HKCU\Software\Microsoft\Internet Explorer\Main\Start Page	Configures Internet Explorers Startup page or search bars	Commonly manipulated by adware and spyware

Area	Name	Function	Notes
	HKCU\Software\Microsoft\Internet Explorer\Main\Search Page HKCU\Software\Microsoft\Internet Explorer\Main\Search Bar		
Registry	HKCU\Software\Microsoft\Internet Explorer\SearchURL	Redirects any URLs typed in Internet Explorer to defined URL	1. Commonly manipulated by adware and spyware
Registry	HKCU or HKLM \Software\Internet Explorer\Explorer Bars	Malicious adware\spyware could create new menu bars in Internet Explorer.	1. Also allows new entries to made to standard menu bars. 2. Available in IE 4.x and above. 3. Commonly manipulated by adware and spyware 4. Menu bar will be a CLSID subkey listed under Explorer Bars 5. Used by Hotbar adware (http://securityresponse.symantec.com/avcenter/venc/data/adware.hotbar.html)
Registry	HKLM\Software\Classes\CLSID\{CLSID}\Implemented Categories\{00021493-0000-0000-C000-000000000046} HKLM\Software\Classes\CLSID\{CLSID}\Implemented Categories\{00021494-0000-0000-C000-000000000046}	…93 defines a vertical Explorer bar …94 defines a horizontal Explorer bar	1. Commonly manipulated by adware and spyware
Registry	HKCU\ or HKLM\Software\Internet Explorer\Extensions	Adware/spyware can add buttons to IE that connect directly to malicious programs and scripts.	1. Available in IE 5.x and above. 2. http://msdn.microsoft.com/library/default.asp?url=/workshop/browser/ext/overview/overview.asp 3. Commonly manipulated by adware and spyware, including Adblock.
Registry	HKCU\Software\Microsoft\OLE	Used to register Windows OLE programs	1. Available with Win 3.x and above 2. Not a common malware vector 3. Used by Bropia trojan (http://www.sarc.com/avcenter/venc/data/w32.brop

Area	Name	Function	Notes
			ia.j.html).
Registry	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load	Runs commands or programs after user logs on	1. Works with all versions of Windows NT and above 2. Replaces Win 9x's Win.ini Load= functionality. 3. Executes programs in minimized state
Registry	HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\run	Runs commands or programs after user logs on	1. Works with all versions of Windows NT and above 2. Replaces Win 9x's Win.ini Run= functionality. 3. Executes programs in maximized state.
Registry	HKCU or HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell HKCU or HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell	Runs commands or programs after user logs on	1. Works with all versions of Windows NT and above 2. Replaces Win 9x's System.ini Shell= functionality. 3. Should only have 'Explorer.exe" as data value, if any value is displayed. Should not include a directory path. Some malware have pointed to bogus Explorer.exe (not located in %Windir%. Should not have additional programs before or after Explorer.exe unless program is known to be legitimate.
Registry	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\System	Runs programs after user logs on	1. Key is present by default, but assigned no value.
Registry	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman	Runs programs in Task Manager after user logs on	Key not present by default.
Registry	HKCU or HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run	Runs programs after user logs on, when Windows default shell (explorer.exe) runs for the first time during every logon	1. Works with W2K and above 2. Not unusual to find legitimate programs, like Microsoft's ctfmon.exe listed here. 3. Does not require reboot. 4. Does not execute commands if explorer.exe is executed manually. 5. W2K will run any sub key with any program listed under this key. Discovered by Andrew Aronoff of SilentRunners.org.

Area	Name	Function	Notes
Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell	Runs programs or commands after user logs on, but before desktop is displayed.	1. Works with W2K and above 2. Shell subkey may not exist by default. 3. Does not require reboot after modification. 4. If malware creates Shell key, and does not launch Windows shell, too, desktop will not be visible. You can still use Task Manager to run commands, including regedit.exe 5. Similar System key exists under HKLM\; but Shell subkey does not get executed.
Registry	HKCU or HKLM\Software\Microsoft\Windows\CurrentVersion\Run	Runs programs or commands after user logs on	1. Works with all versions of Windows 9x and above. 2. Not run in Safe mode unless value is prefixed by an * (asterisk). 3. Often contains many legitimate programs. 4. Most popular registry auto-run key for malware by a huge percentage. 5. W2K will run any sub key with any program listed under this key. Discovered by Andrew Aronoff of SilentRunners.org. 6. Non-admin users cannot modify HKLM version. 7. Run key also appears in the HK_U\.Default registry profile area, but does not copy over to new profiles. 8. Cannot be disabled by holding down Shift or Alt keys as sometimes reported.
Registry	HKCU or HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce	Runs programs or commands after user logs on for the first time only after the key is created.	1. Works with all versions of Windows 9x and above. 2. HKLM\RunOnce runs entries synchronously (in undefined order)-there is a defined order and all other keys and processing must wait for this key to process and clear before they can load. All other Run keys run entries asynchronously, which means they can load on top of each other. 3. HKCU version will run once for any user given the key. 4. HKLM version will only run value for users with admin permissions to key. Regular users will not run the value, although they can read it. 5. RunOnce key also appears in the HK_U\.Default

Area	Name	Function	Notes
			registry profile area, but does not copy over to new profiles. 6. Non-admin users cannot modify HKLM version. 7. Not run if in Safe mode in W2K and above unless value name begins with an asterisk. 8. If an exclamation point begins key value, then key will not be deleted until successful completion of program or command. 9. Holding down Shift key does not prevent execution. 10. W2K will run any sub key with any program listed under this key. Discovered by Andrew Aronoff of SilentRunners.org.
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup	Runs programs or commands after Setup's first-boot activities or after anytime Add/Remove wizard is used when user logs on for the first time only after the key is created. (Can be stored as part of the Default Users profile.)	1. Works in all versions of Windows. 2. Not run if in Safe mode. 3. Holding down Shift key does not prevent execution. 4. If an exclamation point begins key value, then key will not be deleted until successful completion of program or command.
Registry	HKCU or HKLM \Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad	Runs commands or programs after user logs on, although typically points to the CLSID of the associated .DLL file. Links programs to explorer.exe process.	1. Legitimate programs often located here, including Microsoft's webcheck.exe and systray.exe. 2. HKCU more popular than HKLM 3. Data value is CLSID of associated program as registered in HKCR\ 4. Download.Ject trojan, Spyware Eblaster (http://securityresponse.symantec.com/avcenter/venc/data/spyware.eblaster.html) and the Webber trojan (http://www.sophos.com/virusinfo/analyses/trojwebbera.html) use this key.
Registry	HKCU or HKLM\Software\Policies\Microsoft\Windows\System\Scripts	Runs scripts on computer startup/shutdown or user logon/logoff	1. Works with Windows 2000 and above. 2. Scripts may be passed down by group policies and located in different registry keys. 3. Not a common location for malware.

Area	Name	Function	Notes
Registry	HKLM\Software\Classes\<filettype>\shell\open\command HKCR\<filettype>\shell\open\command Examples: HKLM\Software\Classes\batfile\shell\open\command HKLM\Software\Classes\comfile\shell\open\command HKLM\Software\Classes\exefile\shell\open\command HKLM\Software\Classes\htafile\shell\open\command HKLM\Software\Classes\piffile\shell\open\command HKLM\Software\Classes\ShellScrap\shell\open\command	Can be modified to run additional commands or programs when a particular file type is executed	1. Works on Windows 9x and above 2. HKLM\Software\Classes\<filetype> and HKCR\<filetype> are aliases of each other. If you change the value in one, you change it in the other. 3. Most common malware modifications listed, although any file type can be modified. 4. Most common modification is made to the exefile type. For example: a. Value should always be: "%1" %* 5. PrettyPark worm (http://securityresponse.symantec.com/avcenter/venc/data/prettypark.worm.html) changed value to: FILES32.VXD "%1" %* 6. Whenever an exe file was executed, it would execute the malicious Files32.vxd worm program, too. 7. If entire data value is deleted instead of original value being replaced, it caused execution problems with exe files.
Registry	HKCU or HKLM\Software\Microsoft\Active Setup\Installed Components\<program's name or CLSID>	Loads programs on PC startup	1. Works with Windows 98 and above 2. Look for Stubpath= value 3. Contains many/mostly legitimate programs. 4. Common method used by malware a. For example, Prorat trojan (http://www.sophos.com/virusinfo/analyses/trojproratd.html). 5. HKCU doesn't usually launch anything. The HKLM Version value is compared at launch to the Version value under HKCU. If the HKLM value is greater, the executable is launched and the HKCU version value is updated. At next boot, the executable doesn't launch again unless the HKCU Version value is deleted or the HKLM value is incremented. (Thanks to Andrew Aronoff of SilentRunners.org) 6. Difficult to discern what is legitimate vs. malicious

Area	Name	Function	Notes
			in this key. 7. Programs run in this key run in System context. Thanks to Martin Zugec for this hint.
Registry	HKCU or HKLM\Software\Microsoft\Command Processor\Autorun	Runs program or command when: a. Cmd.exe is executed. b. Windows is started in Safe Mode with Command Prompt c. Batch file (.bat) or command (.cmd) is executed.	1. Works with NT and above 2. Replaces previous functionality of Dosstart.bat. 3. Does not run when Command.com is executed. 4. Can be disabled when running cmd.exe manually by typing in cmd.exe /d. 5. Modification of this key does not require a reboot to be effective.
Registry	HKLM\Software\Microsoft\Internet Explorer\Search HKLM\Software\Microsoft\Internet Explorer\UrlSearchHooks	Determines how Internet Explorer searches for unknown entries	1. Works with Internet Explorer 5.x and above. 2. Both keys contain legitimate values, but often commandeered by spyware and adware. 3. Search subkey contains references to http://ie.search.msn.com by default.
Registry	HKLM\Software\Microsoft\Internet Explorer\Styles	Lists Internet Explorer style sheets	1. Can be created or manipulated by adware/malware to display malicious web sites or popups.
Registry	HKLM\Software\Microsoft\Internet Explorer\Toolbar	Loads new menu bars for Internet Explorer or modifies existing toolbars	1. Works with all versions of Internet Explorer 5.x and above. 2. Commonly exploited by adware
Registry	HKCU\Software\Internet Explorer\Toolbar\ShellBrowser HKCU\Software\Internet Explorer\Toolbar\WebBrowser	Malicious adware\spyware could create new menu bars in Internet Explorer.	1. Commonly manipulated by adware and spyware 2. Menu bar will be a CLSID subkey listed under Toolbars
Registry	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs	All the DLLs that are specified in this value are loaded by each Microsoft Windows-based application that is running in the current log on session using User32.dll API library (which is used by most programs).	1. Works with Windows NT and above 2. Not usually populated by legitimate programs, but can be. 3. Common method used by malware and adware a. For example, CoolWebSearch Adware (http://securityresponse.symantec.com/avcenter/venc/data/adware.cwsmsconfd.b.html).
Registry	HKLM\Software\Microsoft\Windo	Loads Windows logon user	Works with Windows NT and above

Area	Name	Function	Notes
	ws NT\CurrentVersion\Winlogon\GinaDLL	interface, loaded interface passes interactive user's logon credentials to Winlogon.exe	Microsoft's default data value is Msgina.dll Has been a target of trojan attacks, attempting to capture end-user logon credentials. PC Anywhere program will modify value to be Awgina.dll. Novell logon client will modify as well.
Registry	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify	Used to run a particular program when a predefined event (ex. Screensaver stops or starts, user logs on or off) occurs.	1. Works with NT and above 2. Many legitimate programs are stored here. 3. Not a common malware location, but is used. 4. For example, Haxor backdoor trojan rootkit (http://securityresponse.symantec.com/avcenter/venc/data/backdoor.)haxdoor.b.html).
Registry	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit	Specifies the programs that Winlogon runs when a user logs on.	1. By default, Winlogon runs %Windir\System32\Userinit.exe, which runs logon scripts, reestablishes network connections, and then starts Explorer.exe, the Windows user interface. 2. Not a common malware startup location, has been exploited in the wild. a. For example, Petch trojan (http://securityresponse.symantec.com/avcenter/venc/data/w32.petch.b.html).
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects	Programs are loaded when Internet Explorer loads; programs loaded are also known as Add-Ins.	1. Works with an OS that can run Internet Explorer 5.x and above. 2. Commonly exploited key 3. Several programs help list and/or modify BHOs, including IE XP SP2 and above.
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler	Task scheduler programs that are launched when Windows starts.	1. Works with W2K and above. 2. For example, Bookmarker trojan (http://securityresponse.symantec.com/avcenter/venc/data/trojan.bookmarker.c.html) or SpyFalcon.
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User	Determines location of Startup folders (i.e. Startup programs) and other common folders (ex. My Documents, My Favorites) for All Users profile	1. Works with Windows 9x and above 2. Used by malware to change Startup folder behavior. Malware can place itself in the newly created Startup folder to be executed when user logs on, but if user checks normal Startup folders, malicious program will not be listed.

Area	Name	Function	Notes
	Shell Folders \Startup \Common Startup		3. Malware modifying these keys will often then execute programs and commands found in default Startup folders so user is not suspicious.
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks	Contains the list of the COM objects, listed by GUID, that trap execute commands	1. Must contain %Windir%\System32\Shell32.dll API program 2. Other listed programs must be deemed suspicious
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx	Runs programs or commands after user logs on, in a controlled order. Runs listed value each time any user logs on until a user with admin permissions to registry key logons on, then it deletes the value after running.	1. Works with all versions of Windows 9x and above. 2. Not run in Safe mode unless value is prefixed by an * (asterisk). 3. Only runs values under subkeys (does not run values placed directly under key) 4. Non-admin users cannot normally modify. 5. For more information (http://support.microsoft.com/?kbid=232509&sd=RMVP)
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices	Runs service after boot up prior to user logging on.	1. Works only in Win 9x family 2. There is also a HKCU version of the same key, but it doesn't appear to be used or able to launch anything.
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce	Runs service once after boot up prior to user logging on, and then deletes itself.	1. Works only in Win 9x family 2. If value is preceded by an exclamation point, deletion will not occur unless command is successfully completed. 3. There is also a HKCU version of the same key, but it doesn't appear to be used or able to launch anything.
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved	Lists programs that will run with associated file types	1. Works with Windows 9x and above 2. Usually contains dozens of legitimate programs 3. Most programs listed will be located in %Windir%\System32 or C:\Program Files 4. Difficult to tell what is and isn't malicious
Registry	HKLM\System\CurrentControlSet\Control\MPRServices	Can be used to launch programs during predefined events	1. Used by Win 9x family. 2. Similar to HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify registry key used by NT and above systems.

Area	Name	Function	Notes
			3. Used by Haxdoor.B backdoor trojan (http://securityresponse.symantec.com/avcenter/venc/data/backdoor.)haxdoor.b.html).
Registry	HKLM\System\CurrentControlSet\Control\SafeBoot	Used by Windows to determine what programs, services, and drivers are loaded in a Safe mode boot.	1. Although not common, can be manipulated by malware to either prevent Safe mode from being run (i.e. values are deleted) or to add malware program to a Safe mode boot sequence. 2. SafeBoot\Minimal used by Toxbot (http://securityresponse.symantec.com/avcenter/venc/data/w32.toxbot.c.html) 3. Used by Petch trojan (http://securityresponse.symantec.com/avcenter/venc/data/w32.petch.b.html) to delete all Safe mode listings.
Registry	HKLM\System\CurrentControlSet\Control\SafeBoot\Option\ "UseAlternateShell"=1	Can be used to run another shell besides Windows Explorer.	1. If this value exists, then the shell listed at HKLM\System\CurrentControlSet\Control\SafeBoot\AlternateShell will be launched at boot instead of Windows Explorer. 2. Works on Windows 2000 and above. 3. Thanks to Andrew Aronoff of SilientRunners.org and Tony K. of the Netherlandsfor the hint.
Registry	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	Allows another program (or debugger) to be executed instead when another program is started	4. Key lists all the programs that have been defined to have alternate programs start instead. 5. Normal to have dozens of legitimate entries here. 6. Used by a few malware programs, including Zellome worm and StartPage.O trojan. 7. Thanks to Andrew Aronoff of SilientRunners.org for the hint.
Registry	HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute	Programs or commands will be executed upon next reboot	1. Works with NT and above 2. Replaces some of the functionality of Wininit.ini of earlier Windows versions.
Registry	HKLM\System\CurrentControlSet\Control\Session Manager\Environment\Path	Determines what directories to check for commands or programs typed in without specific path statement (i.e. Frog.exe vs. C:\Program	1. Some malware programs rely on defects in the way Windows searches for and executes files when only the file name (ex. Frog.exe vs. C:\Program Files\Frog.exe) is given. 2. PATH statement can be set by DOS PATH

Area	Name	Function	Notes
		Files\Frog.exe)	command (located under Environmental variables in NT family) or by registry key. 3. Should contain by default: %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem; 4. Can contain other legitimate non-default entries (ex. C:\Program Files\Network Associates;) 5. Not commonly used by malware, but can still be a problem today a. For example, some malware places itself in default application directories, which the application executes instead of the legitimate program executable 6. One trojan placed its malicious code in the user's My Documents folder. Because the malware was named after a legitimate MS-Word executable, MS-Word would always load it first instead of the legitimate version located under Program Files.
Registry	HKLM\System\CurrentControlSet\Control\Session Manager\Environment\PathExt	Determines what file extensions are tried if program name is typed in without an extension (i.e. Frog vs. Frog.exe)	1. Some malware programs (ex. Spawner or twin viruses) rely on defects in the way Windows executes files when only the file name (ex. Frog.exe vs. C:\Program Files\Frog.exe) is given. 2. Not commonly used by malware today. 3. Should be the following by default: .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
Registry	HKLM\System\CurrentControlSet\Control\Session Manager\FileRenameOperations	Contains pending file operations (e.g. rename, copy, etc.) to be executed on the next reboot of Windows	1. Works with NT and above 2. Replaced older Wininit.ini file
Registry	HKLM\System\CurrentControlSet\Control\Session Manager\StartPage	Configures Internet Explorers Startup page	1. Commonly manipulated by adware and spyware
Registry	HKLM\System\CurrentControlSet\Enum\Root	Used to registry legacy Windows services	1. Not normally used by legitimate programs today. 2. Not commonly used by malware 3. Used by Wallz worm

Area	Name	Function	Notes
			(http://securityresponse.symantec.com/avcenter/venc/data/w32.wallz.html).
Registry	HKLM\System\CurrentControlSet\Services	Will load program as service (i.e. prior to user being logged in)	1. Works with NT and above 2. Common malware vector 3. Difficult to determine what is and isn't malicious using this key alone
Registry	HKCR\Protocols\Filters or HKLM\Software\Classes\Protocols\Filters	Malware program can load itself when a MIME file attachment (ex. Text/xml) is executed	For example, can be used so malicious program is loaded each time a text file is viewed in IE instead of Notepad. Frequently used by spyware and adware Programs listed by CLSID below keys. Used by StartPage.I trojan. Both keys are just aliases for each other. Thanks to Andrew Aronoff of SilentRunners.org for this hint.
Registry	HKLM\System\CurrentControlSet\Control\Class\{4D36E96B-E325-11CE-BFC1-08002BE10318}\UpperFilters	Malware program can modify I/O from input devices	1. Used by some keylogging trojans (ex.InvisibleKey Spyware) to capture data from keyboard driver. 2. By default several the same keys will exist. 3. Do not delete or manipulate this value, because it often contains legitimate information, without backing up registry first. 4. Thanks to Andrew Aronoff of SilentRunners.org for this hint.
Registry	HKLM\System\CurrentControlSet\Services\Winsock2\Parameters\NameSpace_Catalog5\Catalog_Entries HKLM\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog9\Catalog_Entries	Allows trojan or worm to install itself as a Layered Service Provider so that it can monitor network traffic	1. Used by many trojans, spyware, and adware programs. 2. Many legitimate keys are located here. Can be difficult to find unauthorized programs. 3. Commercial Guardian Monitor spyware program and Redfall trojan uses this method. 4. Thanks to Andrew Aronoff of SilentRunners.org for this hint.
Registry	HKLM\System\CurrentControlSet\Print\Monitors	Malware can install itself as a print monitor to send unsolicited messages to client.	1. Registry key normally used by Windows to install new printers, their drivers, and print management programs. Normally contains one or more valid drivers representing current or past installed printers or printer ports.

Area	Name	Function	Notes
			2. Malware can install itself as a print monitoring program and then communicate or manipulate client. 3. Not a commonly used key. 4. Used by Aurora adware program (http://sarc.com/avcenter/venc/data/adware.aurora.html). 5. Reported by Andrew Aronoff of SilentRunners.vbs and Peter L in October 2005.
Registry	HKLM\Software\Microsoft\Office\Outlook\Addins	Malware can add itself as an Outlook Add-in and manipulate incoming or outgoing email	May contain legitimate entries, such as anti-spam or anti-virus software plug-ins. Common malicious example is Hotbar adware.
Registry	HKCU\Identities\<Identity>\Software\Microsoft\Outlook Express\<version>\Signatures	Malware can add a malicious script to Outlook Express email signatures that retrieves malware automatically when opened by recipient.	1. Documented in Outlook Express, but may be able to be exploited in Outlook and other email clients as well. 2. Used by Kak and JS.Fortnight worms.
Registry	HKCU\Software\Microsoft\Internet Explorer\Desktop\Components\<#> \Flags \Source \SubscribedURL	Can be hijacked by adware to redirect IE to unauthorized locations and malware.	1. Source and Subscribed values are set to About:Home by default. 2. Hint provided by Andrew Aronoff of SilentRunners.org
Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell State	Registry value controls many aspects of the desktop environment	1. Including whether Active Desktop is enabled, and whether file extensions are visible. 2. Not very commonly manipulated by malware presently. 3. Hint provided by Andrew Aronoff of SilentRunners.org
Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Active Desktop	Controls Active Desktop settings.	1. Active Desktop, if enabled, opens up more potential attack vectors. 2. Not present by default on most systems 3. Not very commonly manipulated by malware presently.

Area	Name	Function	Notes
			4. Hint provided by Andrew Aronoff of SilentRunners.org
Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	Controls Windows Explorer settings.	1. Not very commonly manipulated by malware presently. 2. Hint provided by Andrew Aronoff of SilentRunners.org
Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System	Allows control of desktop system and some administrative tools	1. Often used to disable Task Manager (DisableTaskMgr=0x1), Registry Editor (DisableRegistryTools = 0x1), and Control Panel (NoDispCPL= 0x1). 2. Key not present by default on most systems 3. Commonly manipulated by malware. Examples include HackerWacker keystroke logger spyware, Ronoper worm, and Ting adware. 4. Hint provided by Andrew Aronoff of SilentRunners.org
Registry	HKLM\Software\Microsoft\Windows\CurrentVersion\URL\DefaultPrefix HKLM\Software\Microsoft\Windows\CurrentVersion\URL\Prefixes\Search HKLM\Software\Microsoft\Windows\CurrentVersion\URL\Prefixes\Search	Adds any string value as a prefix for any URL typed in the browser, effectively redirecting all typed in URLs to unauthorized web site first	1. Commonly used by Adware. Examples include: SmartSearch and WorldSearch adware, JS.Fornight adware worm, and Popdis Trojan. 2. Default values are supposed to be *http://* 3. Hint provided by Andrew Aronoff of SilentRunners.org
Registry	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath	Can be used to point to a new, unauthorized HOSTS file instead of the HOSTS file in the normal location (i.e. \%SystemRoot%\Drivers\Etc)	1. Used by trojans (ex. Qhosts) and adware (ex. TMKSoft.XPlugin) 2. Value is also added to ControlSet001 and ControlSet002 by some trojans (ex. Qhosts). 3. Hint provided by Andrew Aronoff of SilentRunners.org
Registry	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\NameServer	Can be used to point to a new, unauthorized DNS server	1. Used by a few malware programs including Qhosts trojan.

Area	Name	Function	Notes
Registry	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\	Sets overall TCP/IP communications values including DHCP, DNS, and TCP/IP stack. These values used unless a specific value is set under the \Interfaces subkeys on a particular interface.	1. Many subvalues on this key could be changed to cause problems. 2. For example, could be used to set new default Gateway, used to change normal DNS resolution order, etc. 3. Many legitimate settings present by default. 4. Many values can be modified to strength a Windows computer against denial of service attacks.
Registry	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<interface CLSID>	Controls all TCP/IP communications including DHCP, DNS, and TCP/IP stack.	1. Many subvalues on this key could be changed to cause problems. 2. For example, could be used to set new default Gateway, used to change normal DNS resolution order, etc. 3. Many legitimate settings present by default. 4. Used by Qhosts and Flush.D trojans. 5. Look at CurrentControlSet001 and 002, as some trojans modify those values to (ex. Qhosts).
Registry	HKLM\System\CurrentControlSet\Services\VxD\MSTCP\NameServer	Can be used to force client to use unauthorized DNS server	1. Key not present by default 2. Used by Qhosts and Flush.D trojans.
Registry	Malformed registry key names 1. Overly long registry key names (over 255 characters in XP and above, over 232 in W2K) Registry key names ending in \0	Malformed registry key names cannot be correctly displayed in Regedit.exe and other tools, but Windows will still execute.	6. Overly long registry key names can be created by malware. If so, keys might be difficult to detect, but will still run. 7. Can be detected by newest versions of Hijackthis, Autoruns, etc. 8. Announced by Andre Protas in August 2005. 9. Ending a registry key name in \0 makes it untouchable by regedit and other tools (http://www.sysinternals.com/Information/TipsAndTrivia.html#HiddenKeys).