All Known and (so called) Unknown Autostart Methods

1. Autostart folder

C:\windows\start menu\programs\startup {english}
C:\windows\Menu Démarrer\Programmes\Démarrage {french}
C:\windows\All Users\Menu Iniciar\Programas\Iniciar { Portuguese, Brasilian }

This Autostart Directory is saved in :

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]
  Startup="C:\windows\start menu\programs\startup"
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders]
  Startup="C:\windows\start menu\programs\startup"
- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders]
  "Common Startup"="C:\windows\start menu\programs\startup"
- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Shell Folders]
  "Common Startup"="C:\windows\start menu\programs\startup"

By setting it to anything other then *C:\windows\start menu\programs\startup* will lead to execution of **ALL and EVERY** executable inside set directory.

Addendum : as of 10/03/2001 Subseven 2.2 now uses this method.

2. Win.ini

[windows]
load=file.exe
run=file.exe

3. System.ini

[boot]
Shell=Explorer.exe file.exe

4. c:\windows\winstart.bat

Note behaves like an usual BAT file. Used for copying deleting specific files. Autostarts everytime.

5. Registry

- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
  "Whatever"="c:\runfolder\program.exe"
- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
  "Whatever"="c:\runfolder\program.exe"
- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
  "Whatever"="c:\runfolder\program.exe"
- [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
  "Whatever"="c:\runfolder\program.exe"
- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\000x]
  "RunMyApp"="||notepad.exe"
  The format is: "DllFileName|FunctionName|CommandLineArguements" -or- "||command parameters"

  Microsoft Windows 98 Microsoft
  Windows 2000 Professional
  Microsoft Windows 2000 Server
  Microsoft Windows 2000 Advanced Server
  Microsoft Windows Millennium Edition

  http://support.microsoft.com/support/kb/articles/Q232/5/09.ASP

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
  "Whatever"="c:\runfolder\program.exe"
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
  "Whatever"="c:\runfolder\program.exe"

6. c:\windows\wininit.ini

'Often Used by Setup-Programs when the file exists it is run ONCE and then is deleted by windows
Example content of wininit.ini :

[Rename]
NUL=c:\windows\picture.exe

' This example sends c:\windows\picture.exe to NUL, which means that it is being deleted. This requires no interactivity with the user and runs totaly stealth.

7. Autoexec.bat

Starts everytime at Dos Level.

8. Registry Shell Spawning

[HKEY_CLASSES_ROOT\exefile\shell\open\command] @="%1" %*
[HKEY_CLASSES_ROOT\comfile\shell\open\command] @="%1" %*
[HKEY_CLASSES_ROOT\batfile\shell\open\command] @="%1" %*
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command] @="%1" %* [HKEY_CLASSES_ROOT
\piffile\shell\open\command] @="%1" %*

[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] @="%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] @="%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] @="%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command] @= "%1" %*
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command] @="%1" %*

The key should have a value of Value <"%1" %*>, if this is changed to <server.exe "%1 %*">, the server.exe is executed **EVERYTIME** an exe/pif/com/bat/hta is executed.

Known as *Unkown Starting Method* and is currently used by *Subseven.*

9. Icq Inet

[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test]
"Path"="test.exe"
"Startup"="c:\\test"
"Parameters"=""
"Enable"="Yes"

[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\
This key includes all the APPS which are executed IF ICQNET Detects an Internet Connection.

10. Explorer start-up

Windows 95,98,ME
Explorer.exe ist started through a system.ini entry, the entry itself contains no path information so if c:\explorer.exe exist it will be started instead of c:\$winpath\explorer.exe.

Windows NT/2000
The Windows Shell is the familiar desktop that's used for interacting with Windows. During system startup, Windows NT 4.0 and Windows 2000 consult the "Shell" registry entry, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell, to determine the name of the executable that should be loaded as the Shell.
By default, this value specifies Explorer.exe.

The problem has to do with the search order that occurs when system startup is in process. Whenever a registry entry specifies the name of a code module, but does it using a relative path, Windows initiates a search process to find the code. The search order is as follows:

- Search the current directory.
- If the code isn't found, search the directories specified in HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Control\Session Manager\Environment\Path, in the order in which they are specified.
- If the code isn't found, search the directories specified in HKEY_CURRENT_USER \Environment\Path, in the order in which they are specified.
  More info : http://www.microsoft.com/technet/security/bulletin/fq00-052.asp
  Patch : http://www.microsoft.com/technet/support/kb.asp?ID=269049

General :
If a trojan installs itself as c:\explorer no run keys or other start-up entries are needed. If c:\explorer. exe is a corrupted file the user will be locked out of the system. Affects all windows version as of today.

10. Active-X Component

- HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components\KeyName StubPath=C:\PathToFile\Filename.exe

Believe it or not, this does start filename.exe **BEFORE** the shell and any other Program normaly started over the Run Keys.

Misc Information

[HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap] @="Scrap object" "NeverShowExt"=""

The *NeverShowExt* key has the function to HIDE the real extension of the file (here) SHS. This means if you rename a file as "Girl.jpg.shs" it displays as "Girl.jpg" in all programs including Explorer. Your registry should be full of *NeverShowExt* keys, simply delete the key to get the real extension to show up.