Link: http://bytes.com/topic/windows/insights/860759-windows-autorun-faqs-list-autostart-locations

Windows Autorun FAQs: List of autostart locations

Author: Amber Jain (Email: ithinkminus _at_ gmail _dot_ com)

Linked from the Original article- "Windows Autorun FAQs: Description".

Que: Can you list all the autostart locations for windows?
Ans: Here is a comprehensive list of all autostart locations for Windows OSes:

NOTE : These are some abbreviations used in this list. Please note them carefully:
HKCU = HKEY_CURRENT_USER
HKLM = HKEY_LOCAL_MACHINE
HKCR = HKEY_CLASSES_ROOT
%windir% = C:\windows
%USERPROFILE% = C:\Documents and Settings\ambr
%ALLUSERSPROFILE% = C:\Documents and Settings\All Users

1. Folder:

1. C:\Documents and Settings\All Users\Start Menu\Programs\Startup
2.
3. C:\Documents and Settings\<USER_NAME>\Start Menu\Programs\Startup
4.
5. C:\WINDOWS\Tasks
6. This entry is for Task Scheduler for windows XP

Above mentioned autostart locations differ on Windows Vista. The locations on windows Vista are as follows:

1. C:\Windows\System32\Tasks
2. This entry is for Task Scheduler for windows Vista
3.
4. %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup
5.
6. %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

2. Files:

c:\autoexec.bat
c:\config.sys

%windir%\winstart.bat

%windir%\wininit.ini
NOTE: Usually used by setup programs to have a file run once and then get deleted.

%windir%\win.ini
The file looks something like:

1. [windows]
2. load=file.exe

windir\win.ini
The file looks something like:

1. [windows]
2. run=file.exe

windir\system.ini
The file looks something like:

1. [boot]
2. Shell=Explorer.exe file.exe

Note: Some of files that help auto-starting programs are available only in some older Windows OS. They are listed below:

windir\dosstart.bat ---> Used in Win95 or 98 when you select the "Restart in MS-DOS mode" in the shutdown menu.

windir\system\autoexec.nt

windir\system\config.nt

3. Registry:

1. HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
2. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup
3. HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Startup
4. HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logon
5. HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Logon
6. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

7. HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell
8. HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
9. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell
10. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
11. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman
12. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Runonce
13. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunonceEx
14. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run
15. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
16. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
17. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
18. HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
19. HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
20. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
21. HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
22. HKCU\Software\Microsoft\Windows\CurrentVersion\Run
23. HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
24. HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup\
25. HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Runonce
26. HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunonceEx
27. HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run
28. HKLM\SOFTWARE\Classes\Protocols\Filter
29. HKLM\SOFTWARE\Classes\Protocols\Handler
30. HKCU\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components
31. HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
32. HKCU\SOFTWARE\Microsoft\Active Setup\Installed Components
33. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
34. HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
35. HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
36. HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
37. HKCU\Software\Classes\*\ShellEx\ContextMenuHandlers
38. HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers
39. HKCU\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers
40. HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers

41. HKCU\Software\Classes\Folder\ShellEx\ContextMenuHandlers
42. HKLM\Software\Classes\Folder\ShellEx\ContextMenuHandlers
43. HKCU\Software\Classes\Directory\ShellEx\ContextMenuHandlers
44. HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers
45. HKCU\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers
46. HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers
47. HKCU\Software\Classes\Folder\Shellex\ColumnHandlers
48. HKLM\Software\Classes\Folder\Shellex\ColumnHandlers
49. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
50. HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
51. HKCU\Software\Microsoft\Ctf\LangBarAddin
52. HKLM\Software\Microsoft\Ctf\LangBarAddin
53. HKCU\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
54. HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved
55. HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
56. HKCU\Software\Microsoft\Internet Explorer\UrlSearchHooks
57. HKLM\Software\Microsoft\Internet Explorer\Toolbar
58. HKCU\Software\Microsoft\Internet Explorer\Explorer Bars
59. HKLM\Software\Microsoft\Internet Explorer\Explorer Bars
60. HKCU\Software\Microsoft\Internet Explorer\Extensions
61. HKLM\Software\Microsoft\Internet Explorer\Extensions
62. HKLM\System\CurrentControlSet\Services
63. HKLM\System\CurrentControlSet\Services
64. HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute
65. HKLM\System\CurrentControlSet\Control\Session Manager\SetupExecute
66. HKLM\System\CurrentControlSet\Control\Session Manager\Execute
67. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
68. HKLM\Software\Microsoft\Command Processor\Autorun
69. HKCU\Software\Microsoft\Command Processor\Autorun
70. HKLM\SOFTWARE\Classes\Exefile\Shell\Open\Command\(Default)
71. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
72. HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
73. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\System
74. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UIHost
75. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
76. HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Gina

DLL

77. HKCU\Control Panel\Desktop\Scrnsave.exe
78. HKLM\System\CurrentControlSet\Control\BootVerificationProgram\ImagePath
79. HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9
80. HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors
81. HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders
82. HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages
83. HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
84. HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages
85. HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order
86. HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load
87. HKCR\batfile\shell\open\command
88. HKCR\comfile\shell\open\command
89. HKCR\exefile\shell\open\command
90. HKCR\htafile\shell\open\command
91. HKCR\piffile\shell\open\command
92. HKLM\Software\Classes\batfile\shell\open\command
93. HKLM\Software\Classes\comfile\shell\open\command
94. HKLM\Software\Classes\exefile\shell\open\command
95. HKLM\Software\Classes\htafile\shell\open\command
96. HKLM\Software\Classes\piffile\shell\open\command
97. HKLM\System\CurrentControlSet\Control\Class\{4D36E96B-E325-11CE-BFC1-08002BE10318}\UpperFilters
98. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet
99. HKLM\Software\Microsoft\Windows NT\CurrentVersion\InitFileMapping
100. HKLM\Software\Microsoft\Windows NT\CurrentVersion\Aedebug
101. HKLM\Software\Classes\CLSID\{CLSID}\Implemented Categories\{00021493-0000-0000-C000-000000000046}
102. HKLM\Software\Classes\CLSID\{CLSID}\Implemented Categories\{00021494-0000-0000-C000-000000000046}
103. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bat\Application
104. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.cmd\Application
105. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.com\Application
106. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\Application
107. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hta\Application
108. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.pif\Application
109. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.scr\Application

110. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.bat\ProgID
111. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.cmd\ProgID
112. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.com\ProgID
113. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\ProgID
114. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hta\ProgID
115. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.pif\ProgID
116. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.scr\ProgID

4. Registry Shell Spawning:

1. [HKCR\exefile\shell\open\command] @="\"%1\" %*"
2. Executed whenever a .EXE file (Executable) is run.
3.
4. [HKCR\comfile\shell\open\command] @="\"%1\" %*"
5. Executed whenever a .COM file (Command) is run.
6.
7. [HKCR\batfile\shell\open\command] @="\"%1\" %*"
8. Executed whenever a .BAT file (Batch Command) is run.
9.
10. [HKCR\htafile\Shell\Open\Command] @="\"%1\" %*"
11. Executed whenever a .hta file (HTML Application) is run.
12.
13. [HKCR\piffile\shell\open\command] @="\"%1\" %*"
14. Executed whenever a .PIF file (Portable Interchange Format) is run.
15.
16. [HKLM\Software\CLASSES\batfile\shell\open\command] @="\"%1\" %*"
17. Executed whenever a .BAT file (Batch Command) is run.
18.
19. [HKLM\Software\CLASSES\comfile\shell\open\command] @="\"%1\" %*"
20. Executed whenever a .COM file (Command) is run.
21.
22. [HKLM\Software\CLASSES\exefile\shell\open\command] @="\"%1\" %*"
23. Executed whenever a .EXE file (Executable) is run.
24.
25. [HKLM\Software\CLASSES\htafile\Shell\Open\Command] @="\"%1\" %*"
26. Executed whenever a .hta file (HTML Application) is run.
27.
28. [HKLM\Software\CLASSES\piffile\shell\open\command] @="\"%1\" %*"
29. Executed whenever a .PIF file (Portable Interchange Format) is run.

NOTE: 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 Unknown Starting Method and is currently used by Subseven.

NOTE- Subseven (also known as Sub7) is the name of a popular backdoor program. For more information visit wikipedia.

Some other similar entries include:

1. HKCR\vbsfile\shell\open\command\
2. Executed whenever a .VBS file (Visual Basic Script) is run.
3.
4. HKCR\vbefile\shell\open\command\
5. Executed whenever a .VBE file (Encoded Visual Basic Script) is run.
6.
7. HKCR\jsfile\shell\open\command\
8. Executed whenever a .JS file (Javascript) is run.
9.
10. HKCR\jsefile\shell\open\command\
11. Executed whenever a .JSE file (Encoded Javascript) is run.
12.
13. HKCR\wshfile\shell\open\command\
14. Executed whenever a .WSH file (Windows Scripting Host) is run.
15.
16. HKCR\wsffile\shell\open\command\
17. Executed whenever a .WSF file (Windows Scripting File) is run.
18.
19. HKCR\scrfile\shell\open\command\
20. Executed whenever a .SCR file (Screen Saver) is run.

5. Active-X Component:

1. [HKLM\Software\Microsoft\Active Setup\Installed Components\KeyName]
2. StubPath=C:\PathToFile\Filename.exe

You may be amazed but this does start filename.exe before windows explorer (explorer.exe) and any other Program is normally started from run keys.

6. Miscellaneous:

1. HKLM\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog\Catalog_Entries
2. Layered Service Providers, executed before user login.

3.
4. HKLM\System\Control\WOW\cmdline
5. Executed when a 16-bit Windows executable is executed.
6.
7. HKLM\System\Control\WOW\wowcmdline
8. Executed when a 16-bit DOS application is executed.
9.
10. HKLM\Software\Policies\Microsoft\Windows NT\SystemRestore
11. Windows XP and Vista only
12.
13. [Local Fixed Disk]\AUTORUN.INF open=, shellexecute=
14. Excluding Windows Me and Windows XP SP2.
15.
16. [Local Fixed Disk]\[Any Folder with \u201cS\u201d Attribute]\DESKTOP.INI [.ShellClassInfo] CLSID= / UICLSID=
17. This launch point is checked by answering \u201cNo\u201d at the script's first message box and then \u201cYes\u201d at the message box that follows it or with the \u201c-supp\u201d or \u201c-all\u201d command line parameters.
18.
19. HKLM\System\CurrentControlSet\Services\Winsock2\Parameters\NameSpace_Catalog5\Catalog_Entries
20.
21. HKLM\System\CurrentControlSet\Services\Winsock2\Parameters\Protocol_Catalog9\Catalog_Entries

An entry which may be of interest to some is:

1. [HKLM\Software\CLASSES\ShellScrap] @="Scrap object"
2. "NeverShowExt"=""

<u>NOTE</u>: The NeverShowExt key has the function to HIDE the real extension of the file (here) SHS. This means if you rename a file as "Game.exe.shs" it displays as "Game.exe" in all programs including Explorer.

7. Hijack points:

These locations can be used to redirect the desktop, network and Internet Explorer.

1. %WINDIR%\INF\IERESET.INF
2. **<u>Note</u>**: Internet Explorer 5.01, 5.5 & 6.0 only

1. %WINDIR%\HOSTS
2. %WINDIR%\System32\drivers\etc\HOSTS

3. HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath
4. HKLM\Software\Microsoft\Windows\CurrentVersion\URL\Prefixes
5. HKLM\Software\Microsoft\Windows\CurrentVersion\URL\DefaultPrefix
6. HKLM\Software\Microsoft\Internet Explorer\AboutURLs
7. HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
8. HKLM\Software\Microsoft\Internet Explorer\Main
9. HKLM\Software\Microsoft\Internet Explorer\Search
10. HKLM\Software\Microsoft\Windows\CurrentVersion\Policies
11. HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
12. HKCU\Software\Policies\Microsoft\Windows
13. HKCU\Software\Policies\Microsoft\Internet Explorer
14. HKCU\Software\Microsoft\Windows\CurrentVersion\Policies
15. HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
16. HKCU\Software\Microsoft\Internet Explorer\URLSearchHooks
17. HKCU\Software\Microsoft\Internet Explorer\SearchURL
18. HKCU\Software\Microsoft\Internet Explorer\Main
19. HKCU\Software\Microsoft\Internet Explorer\Desktop\Components
20.

Other links:

1. Windows Autorun FAQs: Overview
2. Windows Autorun FAQs: Description
3. Windows Autorun FAQs: Programs dealing with autoruns