The locations of viruses and trojans hiding during the boot process.

There are viruses and trojans that infiltrate your computer in a 'silently' way that you almost don't realize its change or harm. But then it will 'destroy' your system by entering some locations and is

1. START-UP folder:

Windows opens all programs from the Start Up folder in the Start Menu. This folder is very visible in the Programs section of the Start Menu.

Note that I did not say that Windows 'launches' every program in the Start Up folder. I said it 'opened'. There are important differences here.

Of course, the typical programs in the Start Up folder will run. But you can have their shortcuts in Start Up as documents, not programs.

For example, if you put a Word document in the Start Up folder, Word will run and automatically open it during system startup. If you place a WAV file, the music player will play that music when it starts up. And if you put a Web-page Favorites, Internet Explorer (or another browser of your choice), IE will run and open the Web page for you in the same way. (The examples cited here can easily place shortcuts as a WAV file, a Word document, etc.).

2. REGISTRY: Windows executes all commands in the 'Run' area of ??the Windows Registry. The components in 'Run' (and in other parts of the Registry listed below) can be programs or files that the computer opens as explained in Part 1 above.

3. REGISTRY: Windows executes all commands in the 'RunServices' area of ??the Registry.

4. REGISTRY: Windows executes all commands in the 'RunOne' section of the Registry.

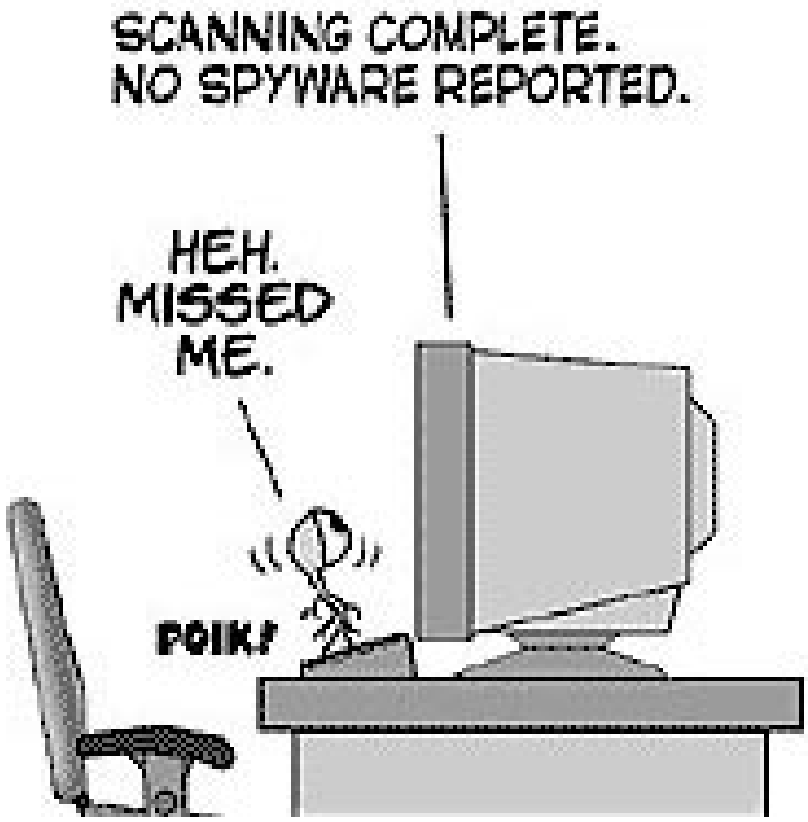
5. REGISTRY: Windows executes all commands in the 'RunServicesOne' area of ??the Registry. (Windows uses two 'Runone' areas only to run single-time programs, usually in the next system startup after installing a program).

6. REGISTRY: Windows executes commands in HKEY_CLASSES_ROOTexefileshellopencommand area "% 1"% * of the Registry. The embed command here will open when any executable file is executed.

There may be other files:

[HKEY_CLASSES_ROOTexefileshellopencommand] = ""% 1 "% *"
[HKEY_CLASSES_ROOTcomfileshellopencommand] = ""% 1 "% *"
[HKEY_CLASSES_ROOTbatfileshellopencommand] = ""% 1 "% *"
[HKEY_CLASSES_ROOThtafileShellOpenCommand] = ""% 1 "% *"
[HKEY_CLASSES_ROOTpiffileshellopencommand] = ""% 1 "% *"
[HKEY_LOCAL_MACHINESoftwareCLASSESbatfileshellopencommand] = ""% 1 "
% * "
[HKEY_LOCAL_MACHINESoftwareCLASSEScomfileshellopencommand] = ""% 1 "
% * "
[HKEY_LOCAL_MACHINESoftwareCLASSESexefileshellopencommand] = ""% 1 "
% * "
[HKEY_LOCAL_MACHINESoftwareCLASSEShtafileShellOpenCommand] = ""% 1 "
% * "
[HKEY_LOCAL_MACHINESoftwareCLASSESpiffileshellopencommand] = ""% 1 "
% * "

If the keys do not have the value **""% 1 "% *"** above and are changed in some way, such as **"" somefilename.exe% 1 "% *"** they will automatically call a specified file.



7. File BATCH: Windows executes all the commands in the Winstart BAT files located in the Windows folder. (Most users and most Windows proficient people don't know this file. It may not exist in your system, but you can create it easily. Note that one The version number of Windows calls the Windows folder 'WinNT'). The full file name is: ***WINSTAR.BAT*** .

8. INITIALIZATION file: Windows executes commands at the 'RUN =' line in the WIN.INI file located in the Windows (or WinNT) folder.

9. INITIALIZATION file: Windows executes commands at the 'LOAD =' line in the WIN.INI file located in the Windows (or WinNT) folder.

It also runs commands at ' *shell* = ' in ***System.ini*** or ***c: windowssystem.ini*** .

[boot]
shell = explorer.exe C: windowsfilename

The file name in the way ***explorer.exe*** will start whenever Windows starts.

With Win.ini, file names can be reserved for a significant space, each stored on one line. It reduces the possibility that file names may be found. Usually the full path of the file is in this entry, otherwise check back in the Windows directory.

10. RELAUCHING: Windows restarts programs that are in use when the system is **shut** down. Windows cannot do this with most non-Microsoft programs. But it does it easily with Internet Explorer and with Windows Explorer, the file and folder management program built into Windows. If you are opening Internet Explorer

when the operating system is off, Windows will reopen the same page after you restart the system. (If this does not happen on your computer, someone has turned off this feature. Using *Tweak UI* , the Microsoft Windows free *UI* management program to re-enable settings' *Remember Explorer settings* 'or under some other name in your Windows version).

11. TASK SCHEDULER: Windows executes commands automatically in *Windows Task Scheduler* (or any other scheduler that adds or replaces *Task Scheduler*). *Task Scheduler* is an official part of all Windows versions, except for the first version of Windows 95. But if *Microsoft Plus Pack* is installed, Windows 95 also has *Task Scheduler* .

12. SECONDARY INSTRUCTIONS: Windows programs that start at startup can freely launch 'child' programs within it. Technically, these are not programs launched by Windows. But they are often not distinguishable from normal auto-running programs if they are started immediately after the 'parent' program runs.

13. Method C: EXPLORER.EXE

C: EXPLORER.EXE

Windows downloads the *explorer.exe* program (always placed in the Windows directory) during the boot process. However, if *c: explorer.exe* exists it will be executed instead of Windows *explorer.exe* . If *c: explorer.exe* is interrupted, the user is actually locked out of their system after they restart.

If *c: explorer.exe* is a trojan, it will be executed. Unlike other methods that automatically restart the computer in other viruses, it does not need any changed files or registers. This file simply has to be renamed: *c: explorer.exe* .

14. Additional methods:

The methods automatically restart Additional machines. The first two methods are used by Trojan SubSeven 2.2.

HKEY_LOCAL_MACHINESoftwareMicrosoftActive SetupInstalled Components
HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentversionexplorerUsershell folders

Icq Inet
[HKEY_CURRENT_USERSoftwareMirabilisICQAgentAppstest]
"Path" = "test.exe"
"Startup" = "c: test"
"Parameters" = ""
"Enable" = "Yes"

[HKEY_CURRENT_USERSoftwareMirabilisICQAgentApps]
Ph?n m?m này xác ??nh các ?ng d?ng s? ???c th?c hi?n n?u ICQNET Detects Internet Connection.

[HKEY_LOCAL_MACHINESoftwareCLASSESShellScrap] = "Scrap object"
"NeverShowExt" = ""

This key changes your file extension.

search for similar articles on tips and guides. Thank you for reading and for following us regularly.