Link: http://bytes.com/topic/windows/insights/860757-windows-autorun-faqs-overview

Windows Autorun FAQs: Overview

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

NOTE- This complete article on "Windows Autorun FAQs" applies theoretically to all Windows NT-based OSes till Windows Vista (and probably Vista's successors too). Much of the contents of this article are tested on Windows XP professional SP2 by the author. Some instances of this article may be altogether different/missing on Windows Vista, XP and other Windows NT systems, but I have tried to write a comprehensive article that may not apply in some newer versions of Windows OSes.

If you are familiar with the basics of Autoruns, you can skip this overview FAQs and read "Windows Autorun FAQs: Description".

Que-1: Before we start, can you please tell me the purpose of this article?
Ans: Well, autoruns play a critical role in any Windows OS. Harmless programs such as important system services, applications e.g. antivirus to malicious ones such as viruses, worms, backdoors etc. use autoruns for their working particularly in windows system. And so, a windows user may come across a situation where he may want to edit autoruns for his windows PC. This article provides an in depth description of autoruns. This article may prove to be useful both to an average windows user and a windows expert.

Que-2: Can you please define autoruns?
Ans: Oh yes...autoruns are the programs which are configured to startup automatically when your Windows system boots and you login to your system. In other words, the term autorun is used in reference to a feature that causes a certain file to open or a certain program to start automatically as soon as a computer with some Windows Operating System is booted up. Some of these you will see as small icons in the system notification area at the bottom right of your screen by the clock. For example:

Que-3: But why do we need autoruns?
Ans: Autoruns have many uses (and many mis-uses too....but we will talk about them later). For example: If you want a program e.g. antivirus to be executed when user logs in to a system then simply adding a entry corresponding to one of autostart locations will add the program to list of autoruns. Next time when you reboot your Windows OS, the program will be executed once the user logs in. To

explain further, I would like to quote Mark Russinovich.
Quoting Mark Russinovich (the co-author of Sysinternals Autoruns program along with Bryce Cogswell)- "Upon installation, many applications configure themselves to start automatically when you log on. Applications do this so that they can automatically check for updates, because they use system tray icons to interact with users, or because they add functionality to Windows components such as Windows Explorer. However, most such applications don't ask permission before inserting themselves in your logon process and almost never provide an interface to let you disable their autostart functionality. . . .".

Que-4: In your last answer, you made a reference to "autostart locations". What are they?
Ans: Well, autostart locations simply refer to the list of locations i.e folders, registry keys, files etc. which are searched by Windows OSes for any of autorun entries. See "Windows Autorun FAQs: List of autostart locations" for a list of all autostart locations.

Que-5: But someone told me that autoruns are viruses. Is that true?
Ans: NO - but some viruses use autoruns. If an autostart entry points to a virus or some other malicious file, then this autorun is certainly a virus. By an autorun virus I mean that the virus is executed when a user logs into Windows OS and the virus may then perform malicious activities to any extent depending on it's payload.

Que-6: Wait! wait....What is payload?
Ans: Hmm....SearchSecurity says- "Payload is the eventual effect of a software virus that has been delivered to a user's computer". Payload is code designed to do more rather than just spreading the worm which is another type of malicious file; it might delete files on a system, encrypt important file etc. In simple words, payload is the side-effect of a virus or any malicious file. And yes, even if you don't understand what 'payload' is, it does not matters much as it is not directly related to the present matter of discussion.

Que-7: I heard the term "Auto Starting Pests (ASPs)" somewhere. What does that mean?
Ans: Auto Starting Pest (or ASPs in short) simply refers to the malicious files executed when Windows starts i.e. ASPs are simply "malicious autorun programs". ASPs are also known as ASEPs or Auto Start Extensibility Points sometimes.

Que-8: What are services?
Ans: It is a program that runs invisibly in the background which load and start running whether or not anyone logs into the computer, unlike a program that is launched from one of autostart locations when a user log in to his system.
There are two ways to view Services on your computer. The first is to use msconfig program by typing msconfig.exe in the Run box in the Start Menu and then clicking the Services tab. If you want to simply look at the services which are running or stopped, this is a good option, but there's a better option. The

preferred way to make changes to services is to launch services.msc from the Run option on the Start Menu.
Looking at the Services window in services.msc you can see that it has columns for Name, Description, Status, Startup Type and Log On As. This provides a quick overview of all the services on your computer. Detailed information is available by right clicking any of the entries and then select Properties. For more details, visit link below:
Windows XP Services- A list of all the standard services

Continue reading the next part of article- "Windows Autorun FAQs: Description".

Other links:
1. Windows Autorun FAQs: List of autostart locations
2. Windows Autorun FAQs: Programs dealing with autoruns