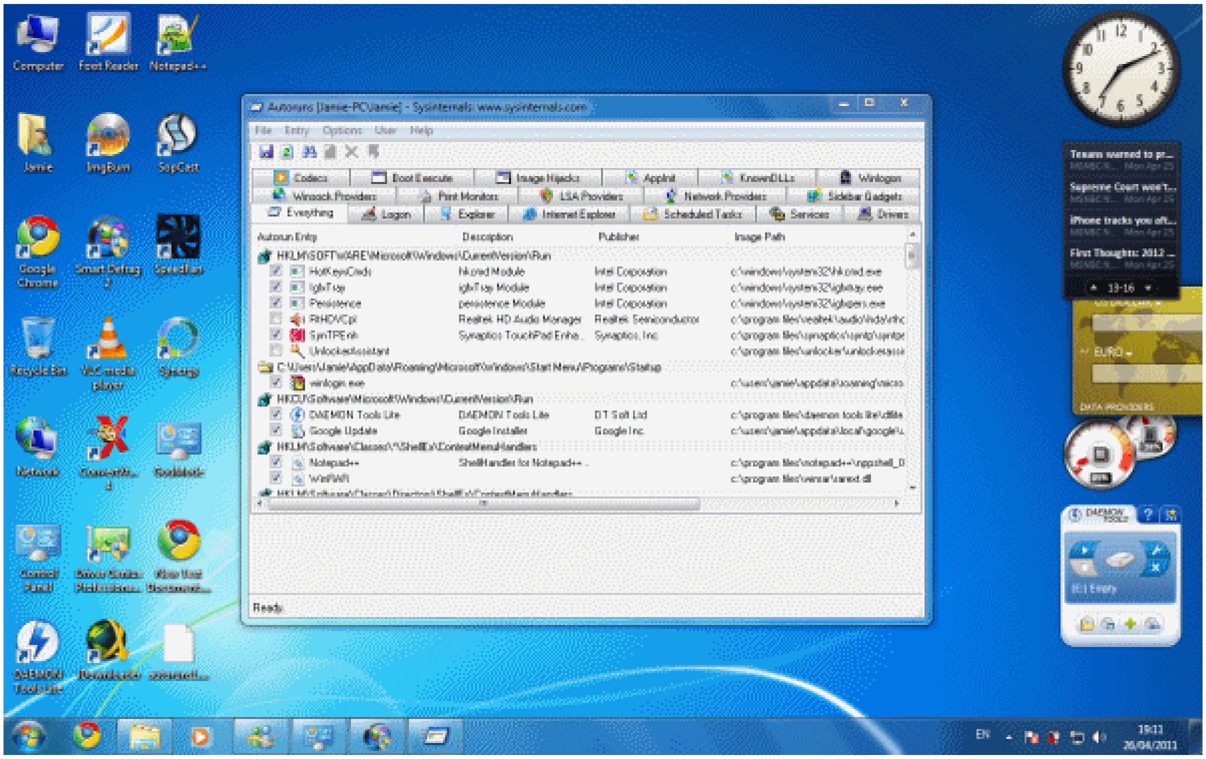
Analyze all Autorun / Auto-start programs in Windows

Your Windows operating system loads all kinds of programs and code automatically in many different ways. You know this already from just witnessing applications start-up and appear when you boot into Windows, particularly in the system tray on the Windows task bar. You might even have used Microsoft's built in **msconfig** to disable programs from running with Windows.

While knowing how to do this can help to stop resource-consuming programs from slowing down your boot (or once in a while help you to stop malicious software from running), it is far from perfect. The msconfig solution does not even scratch the surface and therefore we need a better alternative to be more effective at dictating what can load with, or within Windows automatically. The best alternative is regarded by many as Autoruns from Sysinternals.

What is Autoruns and where do I get it?



Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ HotKeysCmds	hkcmd Module	Intel Corporation	c:\windows\system32\hkcmd.exe
☑ IgfxTray	igfxTray Module	Intel Corporation	c:\windows\system32\igfxtray.exe
☑ Persistence	persistence Module	Intel Corporation	c:\windows\system32\igfxpers.exe
□ RtHDVCpl	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\hda\rthc
☑ SynTPEnh	Synaptics TouchPad Enha...	Synaptics, Inc	c:\program files\synaptics\syntp\syntpe
□ UnlockerAssistant			c:\program files\unlocker\unlockerassi
C:\Users\Jamie\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
☑ winlogin.exe			c:\users\jamie\appdata\roaming\micro
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
☑ DAEMON Tools Lite	DAEMON Tools Lite	DT Soft Ltd	c:\program files\daemon tools lite\dtlite
☑ Google Update	Google Installer	Google Inc	c:\users\jamie\appdata\local\google\u
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers			
☑ Notepad++	ShellHandler for Notepad++ ...		c:\program files\notepad++\nppshell_0
☑ WinRAR			c:\program files\winrar\rarext.dll
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers			

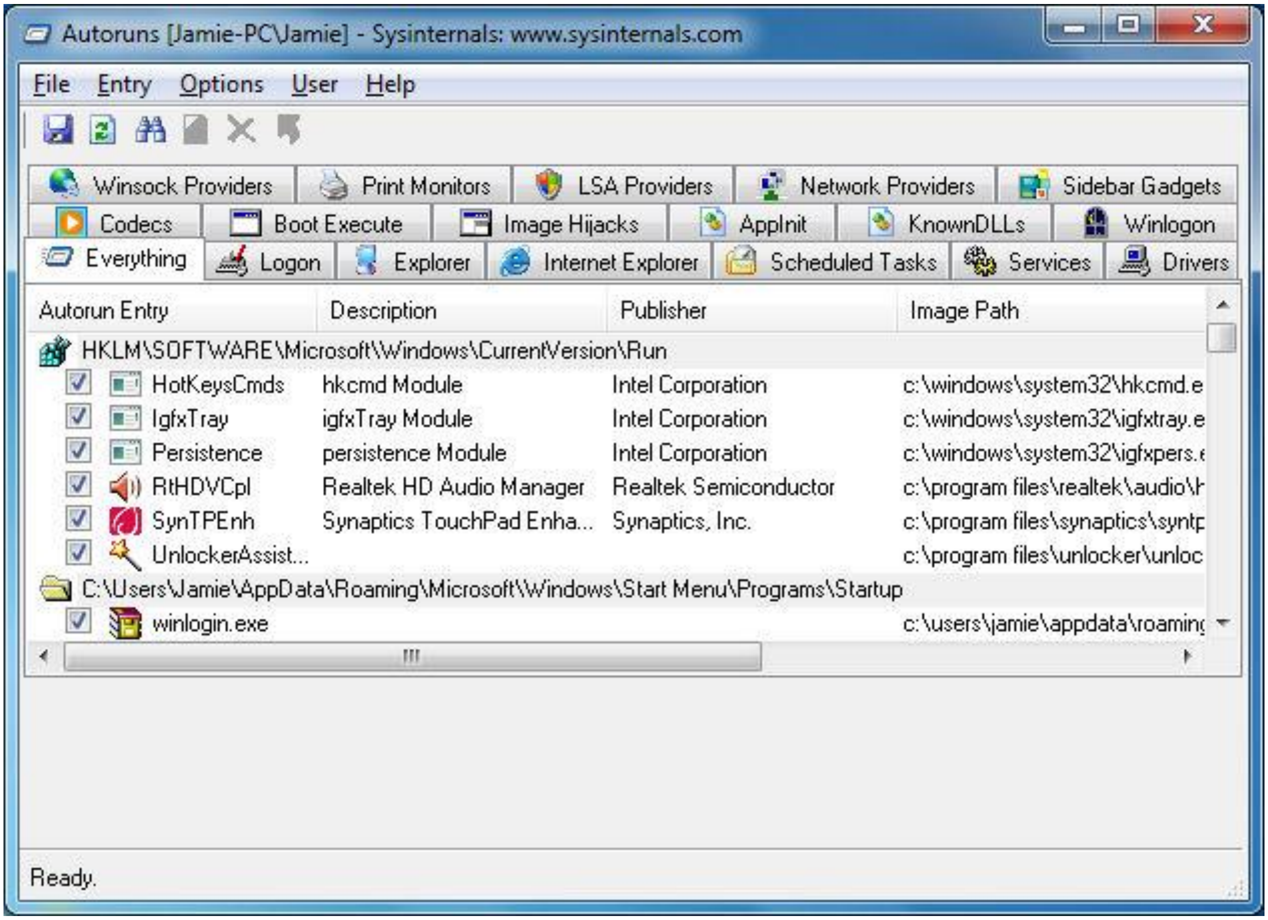
Sysinternal's Autoruns is available for free online for Windows.

- **Autoruns for Windows**: Download Autoruns for Windows (x86, x64)
- **Sysinternals Suite**: Download full Sysinternals Suite for Windows (Autoruns is included.)

Autoruns is a free utility developed by Sysinternals that quickly analyzes a Windows system to find programs that are set to automatically start on Windows boot or what extensions load into Windows processes such as Internet Explorer, and more. It covers the most common areas for malware to hide from detection, and so can be a powerful manual malware attacking tool. It can also be used to reduce the number of auto-start programs to increase system performance.

Autoruns needs to be run with Administrative privileges to make necessary changes. To do this, right click on autoruns.exe and click **Run as Administrator** (or**Run As** in Windows XP, choose an account with full Admin rights). For most Windows XP Admin accounts on personal computers, you won't need to do this, but you will in most cases if running Windows Vista or 7.

Run Autoruns - "Everything" Displayed



Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ HotKeysCmds	hkcmd Module	Intel Corporation	c:\windows\system32\hkcmd.e
☑ IgfxTray	igfxTray Module	Intel Corporation	c:\windows\system32\igfxtray.e
☑ Persistence	persistence Module	Intel Corporation	c:\windows\system32\igfxpers.e
☑ RtHDVCpl	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\h
☑ SynTPEnh	Synaptics TouchPad Enha...	Synaptics, Inc.	c:\program files\synaptics\syntp
☑ UnlockerAssist...			c:\program files\unlocker\unloc
C:\Users\Jamie\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
☑ winlogin.exe			c:\users\jamie\appdata\roaming

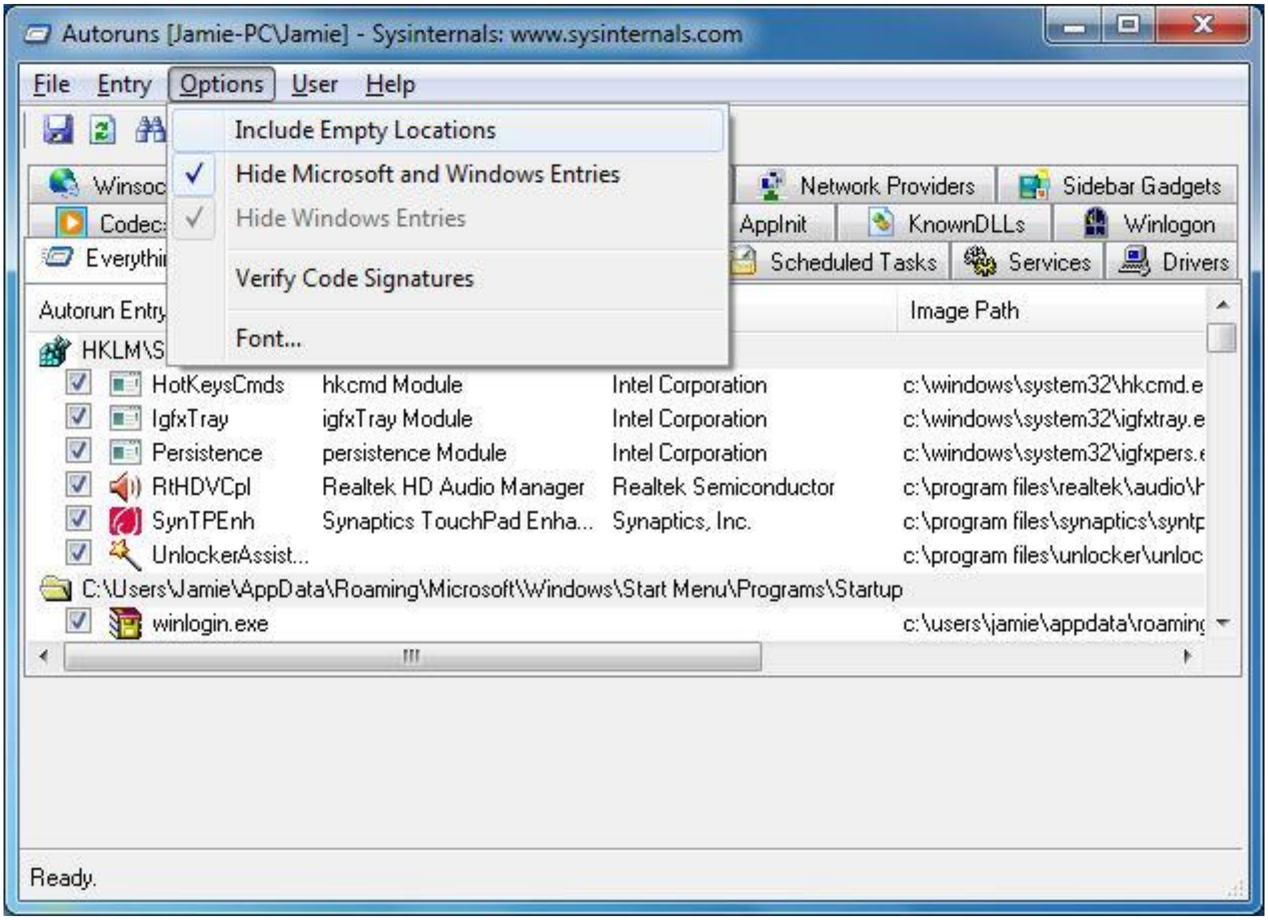
When you first run Autoruns, it will have the "Everything" tab opened automatically and you will see it start to get populated with all kinds of "autoruns". Everything here can be disabled (except Winsock) or deleted completely.

So where does this information come from? The truth is there are so many locations in the Windows registry and in the file system which can be used to execute a program. For example, there is a Startup folder in Windows which you can find in the Start Menu. Any application in that folder (or shortcut) will automatically execute on boot. Similarly, registry entries under the key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run will be run automatically at start-up too.

There are countless applications and extensions out in the wild for all kinds of programs that can be run in this way or a multitude of other ways in Windows. Autoruns scans through a very comprehensive index of these locations and reports back its findings to the user.

The user can then decide to disable/delete applications, save a log of the Autoruns on the system and then compare it later when a malware infection or something else has gone wrong. Quite simply, it is a very powerful tool that everyone can benefit from learning how to use.

Filter out Microsoft & Windows Results?



Autorun Entry			Image Path
HKLM\S			
☑ HotKeysCmds	hkcmd Module	Intel Corporation	c:\windows\system32\hkcmd.e
☑ IgfxTray	igfxTray Module	Intel Corporation	c:\windows\system32\igfxtray.e
☑ Persistence	persistence Module	Intel Corporation	c:\windows\system32\igfxpers.e
☑ RtHDVCpl	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\h
☑ SynTPEnh	Synaptics TouchPad Enha...	Synaptics, Inc.	c:\program files\synaptics\syntp
☑ UnlockerAssist...			c:\program files\unlocker\unloc
C:\Users\Jamie\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
☑ winlogin.exe			c:\users\jamie\appdata\roaming

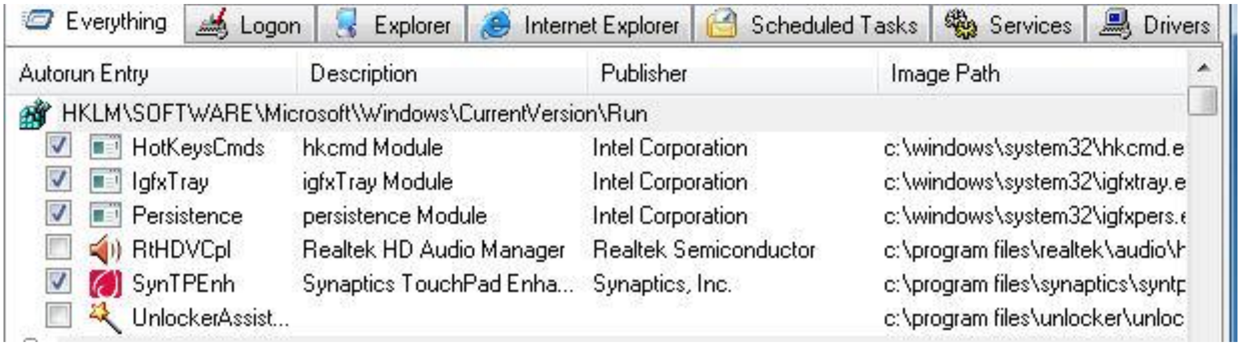
Autoruns will show a lot of results for autoruns related to Microsoft and Windows software. Of course, this can be very useful. However, if you are hunting for results from third-party software that you installed (or malware that was maliciously installed on the system), then you might want to filter out the Windows and Microsoft entries.

Click Options and you will see some choices. By default, results with Empty locations are not shown (because they should be ineffective anyway). Now you will see that you have two other options..

- **Hide Microsoft and Windows Entries -** This option is not selected by default. If selected, it will hide entries from both the Windows operating system, and other Microsoft entries.
- **Hide Windows Entries -** This option is selected by default. If kept selected, it will hide Entries related to the Windows operating system. If you decide to unselect the option, you should be warned that this will mean a lot more results will be shown than usual.

It is recommended that you do not show the Windows entries at least, but it is entirely your choice.

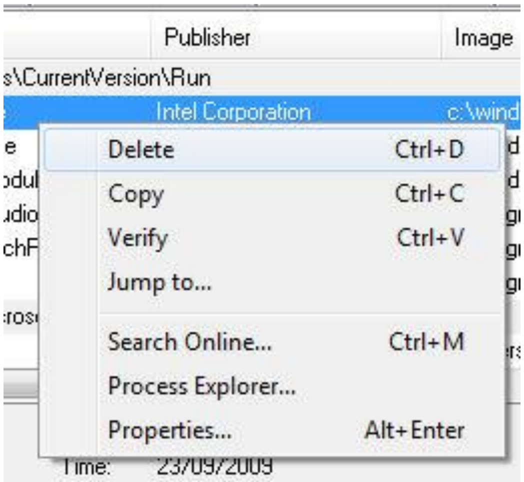
To Disable or Delete?



	Autorun Entry	Description	Publisher	Image Path
	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑	HotKeysCmds	hkcmd Module	Intel Corporation	c:\windows\system32\hkcmd.e
☑	IgfxTray	igfxTray Module	Intel Corporation	c:\windows\system32\igfxtray.e
☑	Persistence	persistence Module	Intel Corporation	c:\windows\system32\igfxpers.e
□	RtHDVCpl	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\h
☑	SynTPEnh	Synaptics TouchPad Enha...	Synaptics, Inc.	c:\program files\synaptics\syntp
□	UnlockerAssist...			c:\program files\unlocker\unloc

Autouns allows you to either delete or disable entries. Both will stop the selected application or extension from being loaded automatically but if you opt to delete the entry you should know that this is a permanent change. So how do you do either? Well if you just want to disable an option to stop it from automatically loading, you can do so by simply deselecting the option. Look at the picture above this text and see how some of the Autoruns have been disabled by clicking the checkbox next to the image name.

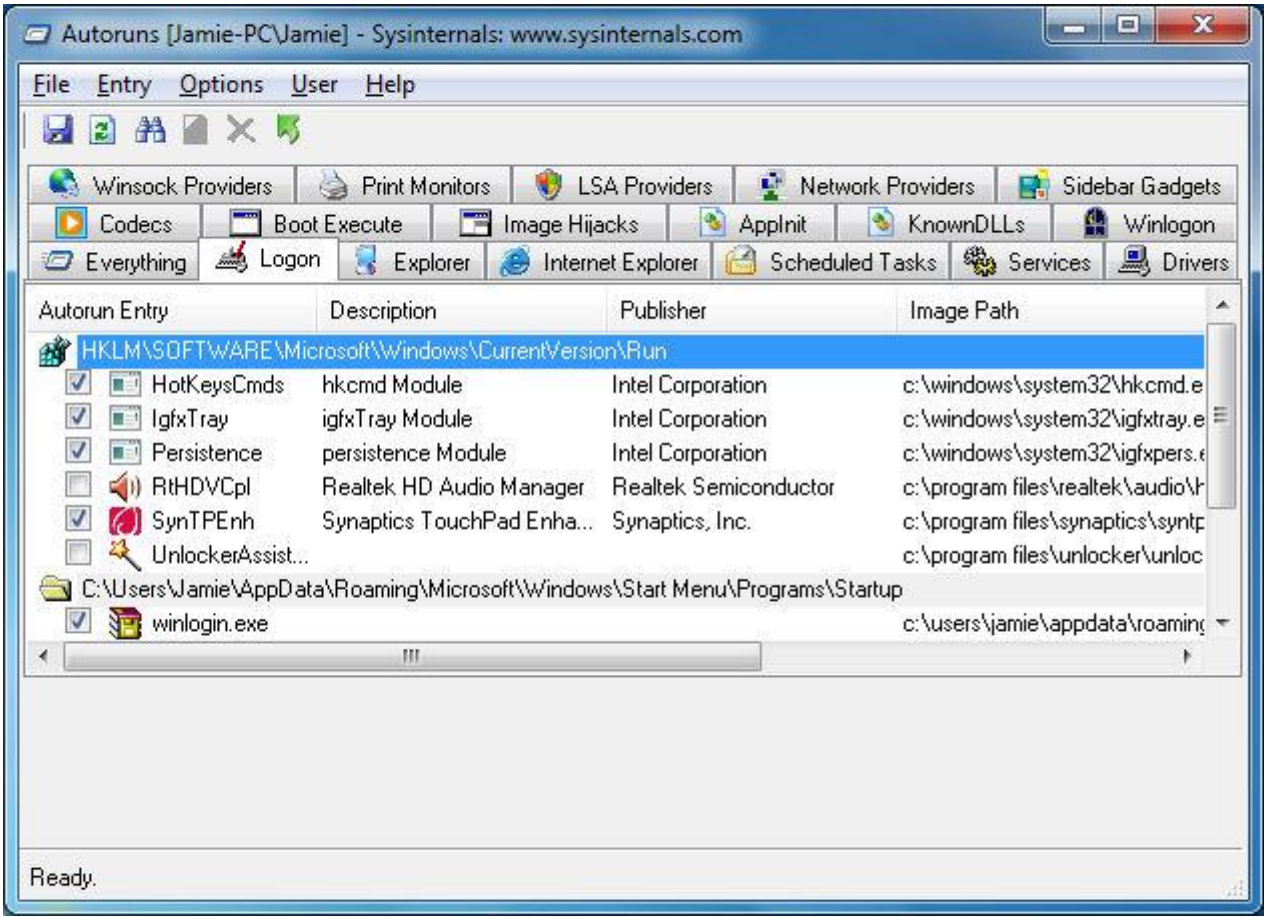
Any entries that you decide to simply disable can be restored by simply running Autoruns and selecting the option again.



If you should find an entry that you certainly do not want to remain checked, then you can just right click on the program and select Delete from the menu that appears. If you do this, Autoruns will make a permanent change. This could either be done by removing a file or editing an entry in the Windows registry. Autoruns can not Undo this change, and performing a comparison (we will see later) does not show deleted entries.

Note that you will need to have Autoruns running with Administrative privileges to delete an entry.

What are these results? "Logon"


Autoruns [Jamie-PC\Jamie] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Winsock Providers | Print Monitors | LSA Providers | Network Providers | Sidebar Gadgets
Codecs | Boot Execute | Image Hijacks | AppInit | KnownDLLs | Winlogon
Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers
Ready.

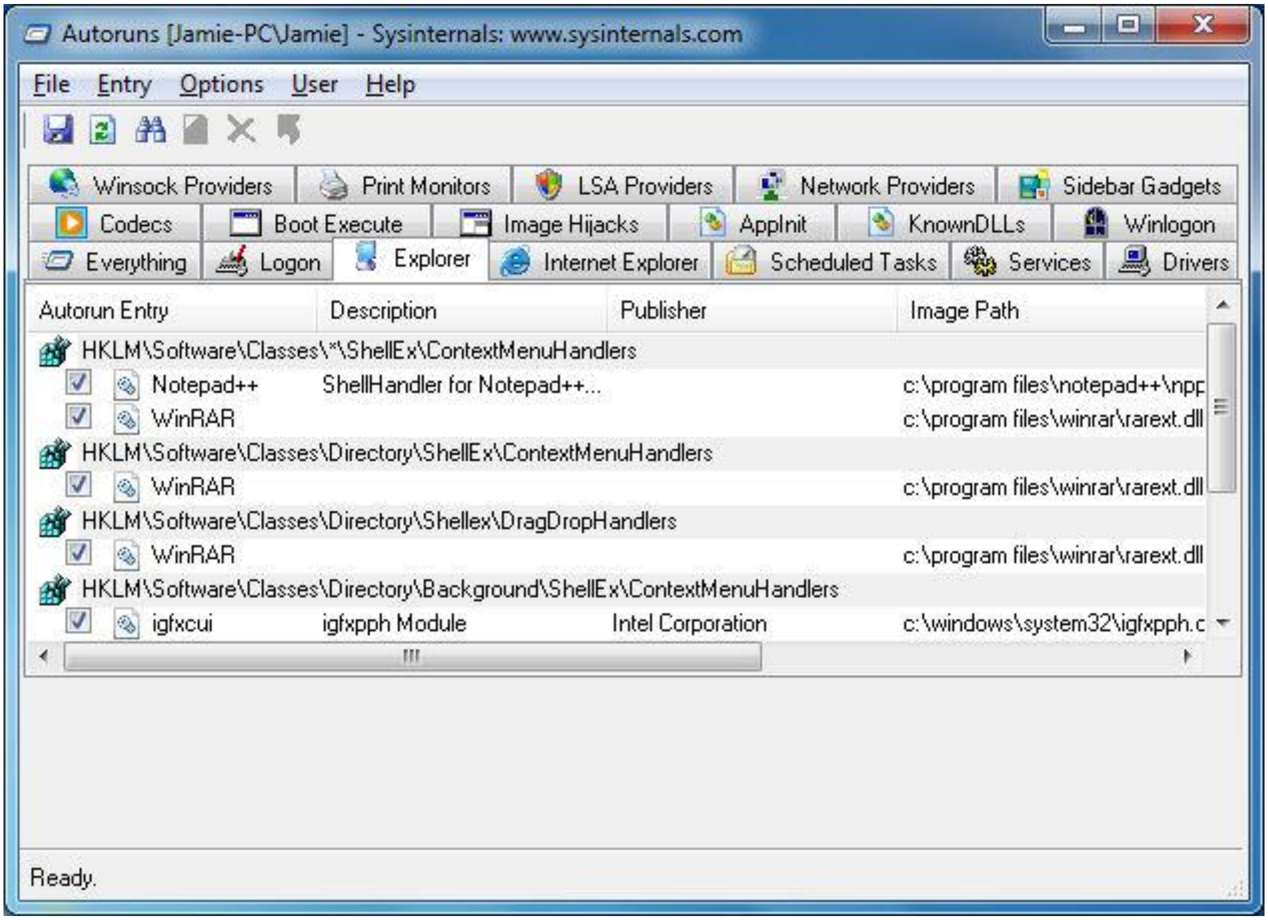
Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ HotKeysCmds	hkcmd Module	Intel Corporation	c:\windows\system32\hkcmd.e
☑ IgfxTray	igfxTray Module	Intel Corporation	c:\windows\system32\igfxtray.e
☑ Persistence	persistence Module	Intel Corporation	c:\windows\system32\igfxpers.e
□ RtHDVCpl	Realtek HD Audio Manager	Realtek Semiconductor	c:\program files\realtek\audio\h
☑ SynTPEnh	Synaptics TouchPad Enha...	Synaptics, Inc.	c:\program files\synaptics\syntp
□ UnlockerAssist...			c:\program files\unlocker\unloc
C:\Users\Jamie\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup			
☑ winlogin.exe			c:\users\jamie\appdata\roaming

Looking at the results under the "Everything" tab can be a bit overwhelming. If you have an idea of what you are looking for, then filtering your results to any of the bunch of tabs offered by the program might save you some time.

The first one we will look at is Logon. The results you will see here are programs that are set to launch automatically when you Logon to Windows. It gathers these results from the Run keys in the Registry (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKCU\Software\Microsoft\Windows\CurrentVersion\Run) or the RunOnce keys. It also checks the StartUp folder and standard application launch locations.

If you are looking to stop a program from running as soon as you Logon, then this is where it will likely be listed by Autoruns.

What are these results? "Explorer"



Autorun Entry	Description	Publisher	Image Path
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers			
☑ Notepad++	ShellHandler for Notepad++...		c:\program files\notepad++\npp
☑ WinRAR			c:\program files\winrar\rarext.dll
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers			
☑ WinRAR			c:\program files\winrar\rarext.dll
HKLM\Software\Classes\Directory\Shellex\DragDropHandlers			
☑ WinRAR			c:\program files\winrar\rarext.dll
HKLM\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers			
☑ igfxcui	igfxpph Module	Intel Corporation	c:\windows\system32\igfxpph.c

Th Explorer shell is also capable of calling on features that you might not like to have active on your system. Autoruns will scan Explorer shell extensions (extensions that would offer more options when you right-click a file, for example), browser helper objects (also known as BHOs), toolbars that are shown in Explorer, shell execution hooks and active setup executions.

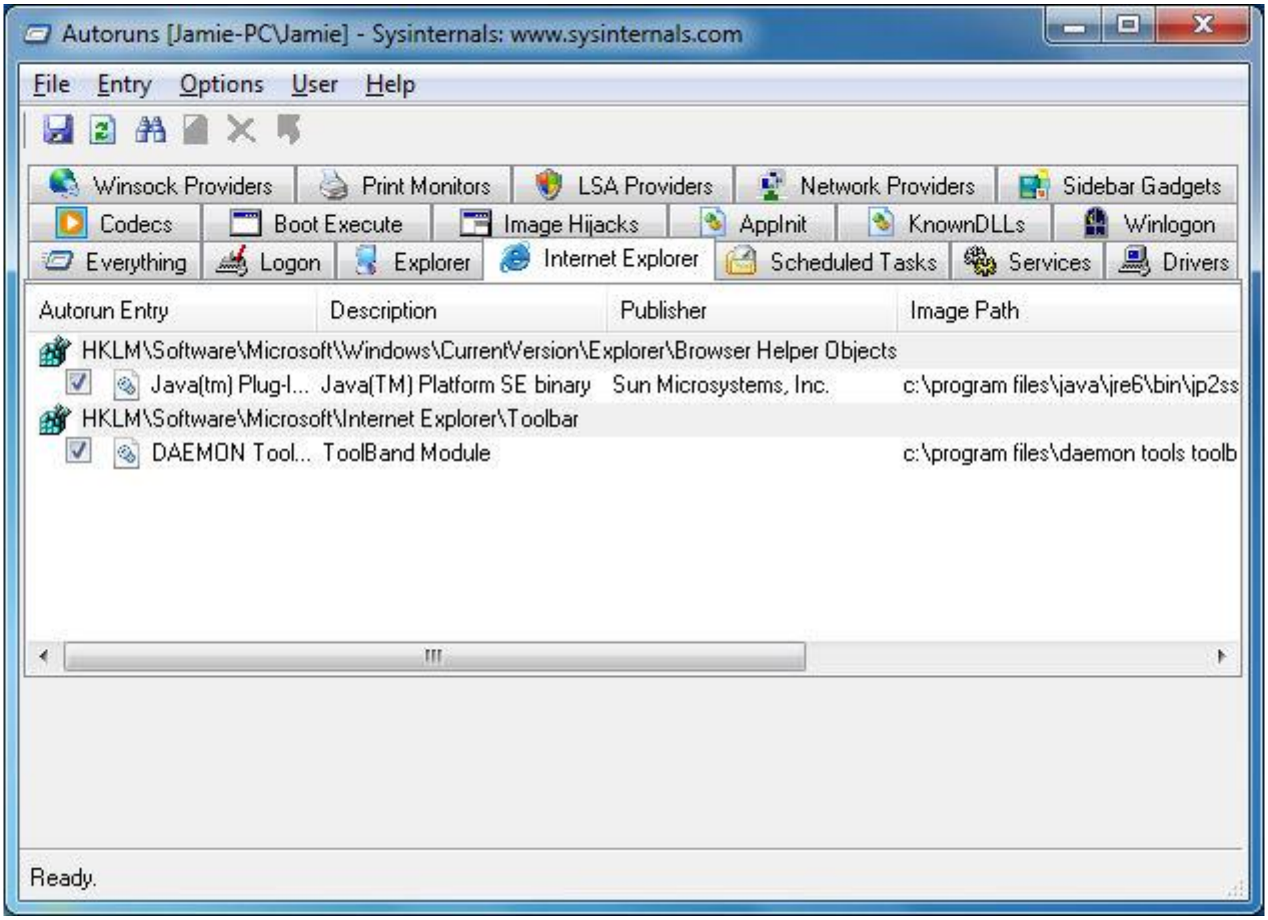
Slow performance from the Explorer shell can often be related to a bad shell extension. If you look at the picture above this text, you can see an entry for Notepad++ under the Registry key HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers. Now note that if you have Notepad++ installed, and you right-click on a text document (or a bunch of other types of documents), you will see an option to "Edit with Notepad++".

To have a look at the source of any result, simply right click it in Autoruns and click Jump To. If the source is a folder containing a references file, then it will launch a folder in Explorer. If the source is a registry value, then it will load the Registry Edition (regedit.exe) and automatically navigate to the relevant key.

If you experience slow performance with the Explorer shell (if context menus take a long time to load, or if folders freeze or take a long time to show contents, for example), then you can try simply disabling all third-party explorer shell extensions. Reboot, and if the problem is gone, you will have identified that a shell extension is to blame. Try then re-enabling extensions one by one and rebooting (or logging out of your user account and logging back in) and you can identify which is responsible for the problem.

It is also interesting to note here that if you right click on an entry that appears to cause a problem (or arouses suspicion for any reason), you have an option to Search Online. This will launch your default browser and use your default search engine to look for the entry. This might provide you with some extra clues as to the problem (known malware, buggy software that can be fixed with an update etc.)

What are these results? "Internet Explorer"



Autorun Entry	Description	Publisher	Image Path
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects			
☑ Java(tm) Plug-I...	Java(TM) Platform SE binary	Sun Microsystems, Inc.	c:\program files\java\jre6\bin\jp2ss
HKLM\Software\Microsoft\Internet Explorer\Toolbar			
☑ DAEMON Tool...	ToolBand Module		c:\program files\daemon tools toolb

Ready.

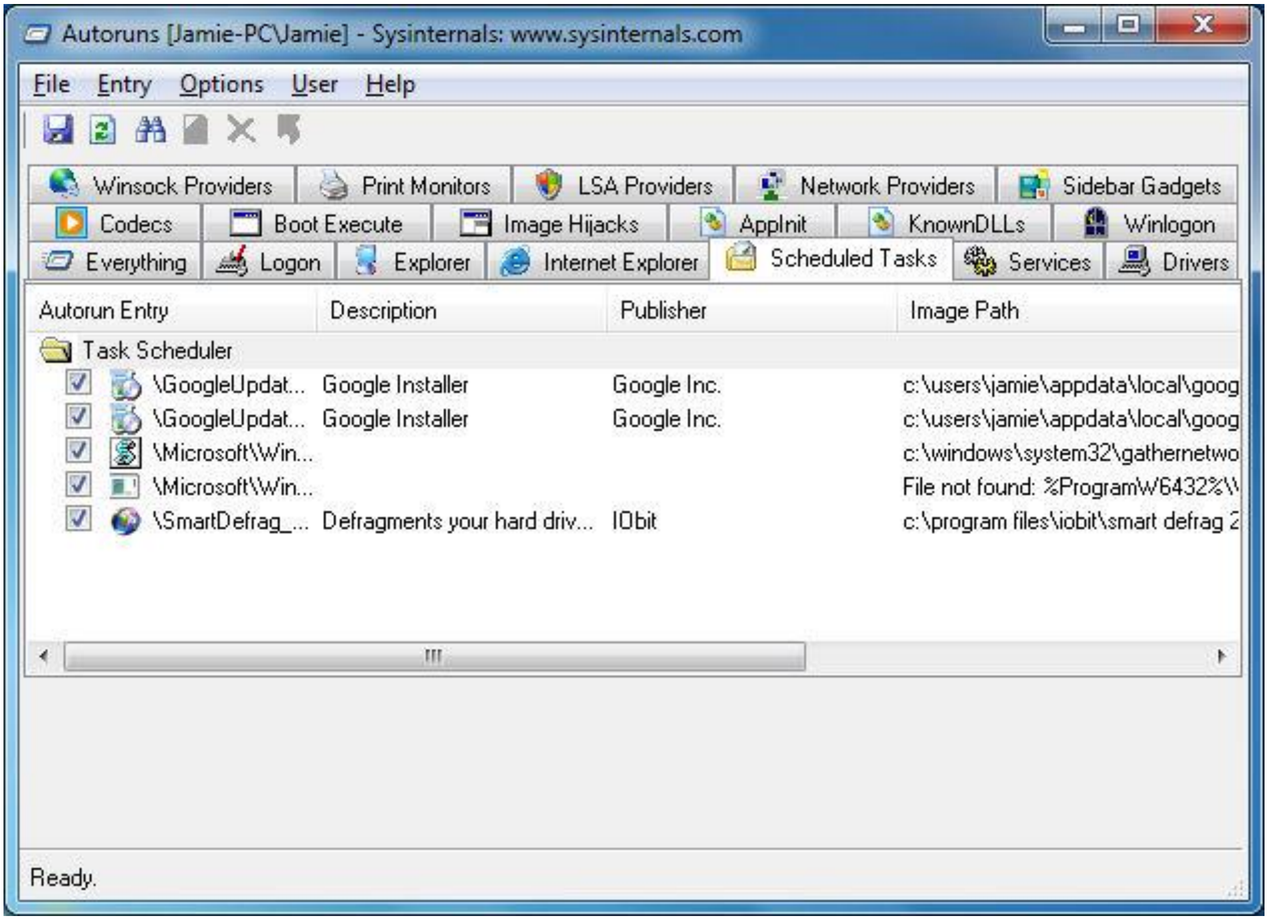
While it has seen its market share drop considerably in recent years, Microsoft's Internet Explorer is still the most widely used Internet browser (not mobile). Like other browsers, Internet Explorer can use extensions. These offer more features and support to the browser when in installed in most cases, but there are problematic and frankly annoying extensions too that can be installed for Internet Explorer and set to automatically be utilized.

The same applies to Browser Helper Objects (BHOs) and, of course, toolbars. Toolbars are often installed by a user at their own will. Popular toolbars include the Yahoo Toolbar, Google Toolbar and the Bing Toolbar. A lot of times however, toolbars are installed by accident or are delivered in a drive-by fashion by installers or of course, by malware. It is not always obvious to users how to stop these from displaying.

Autoruns examines the system for BHOs, Toolbars and Extensions and shows the results. Again, you can disable or delete any result that you want. This might even help you with Internet Explorer instability problems if you disable entries one by one and try launching the browser and seeing if the problem persists (remember to reboot browser).

To remove a BHO or Extension it is suggested to close all Explorer windows (this includes folders) while trying to remove the entry. Looking at the picture of the results above, you can see a Java bowser helper object (plug-in) and a toolbar installed by the Daemon Tools installer.

What are these results? "Scheduled Tasks"



	Autorun Entry	Description	Publisher	Image Path
	Task Scheduler			
☑	\GoogleUpdat...	Google Installer	Google Inc.	c:\users\jamie\appdata\local\goog
☑	\GoogleUpdat...	Google Installer	Google Inc.	c:\users\jamie\appdata\local\goog
☑	\Microsoft\Win...			c:\windows\system32\gathernetwo
☑	\Microsoft\Win...			File not found: %ProgramW6432%\\
☑	\SmartDefrag_...	Defragments your hard driv...	IObit	c:\program files\iobit\smart defrag 2

The Task Scheduler in Windows is responsible for carrying out periodic tasks that could relate to optimization or security, for example. In Autoruns, only tasks configured to start at boot or login are shown.

There are a few good examples in the picture above. The first, and most obvious results, are for the Google Update Installer processes. These are on my system because I have Google software installed (Chrome) that rely on the background update processes.

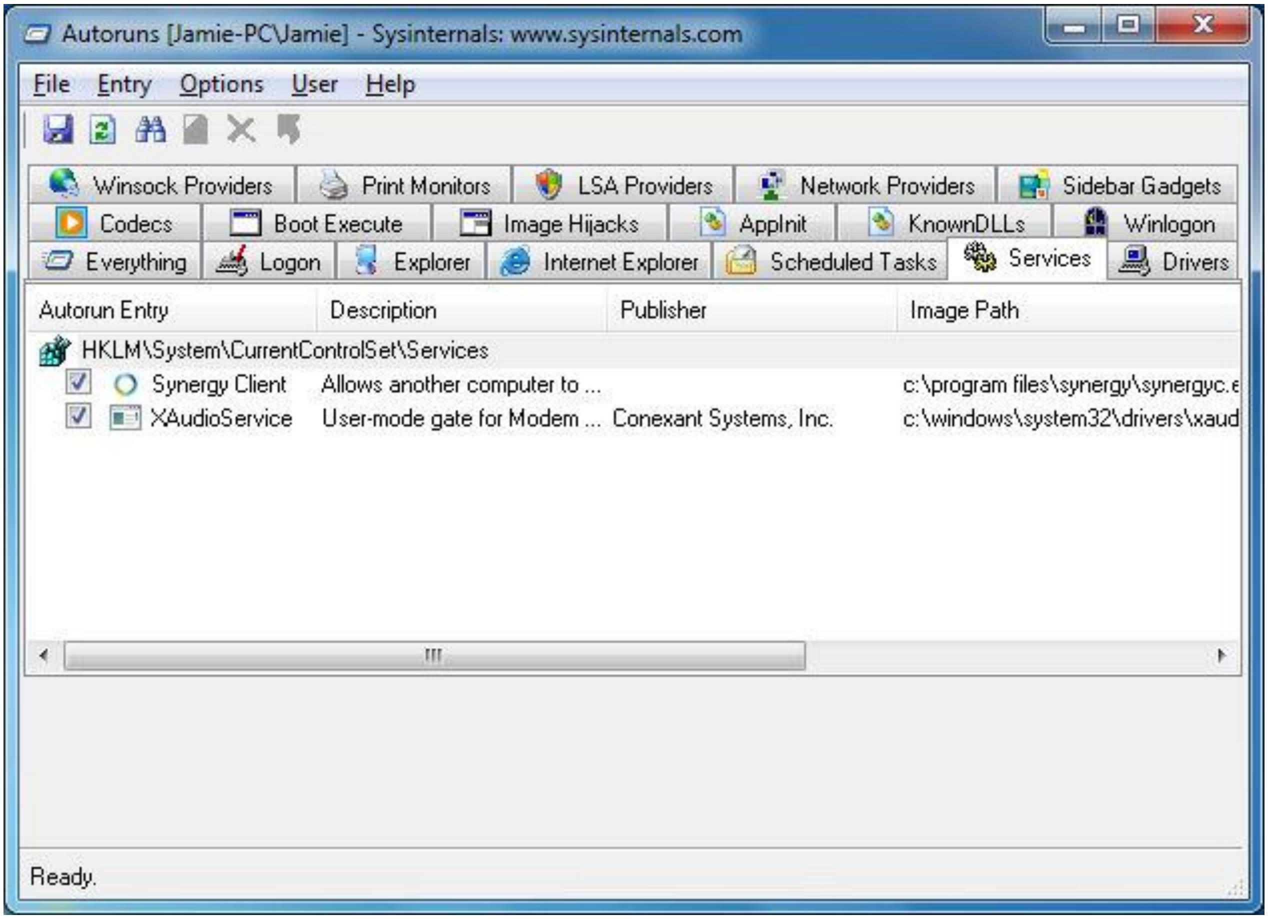
Another thing I would like to point out is the third entry. The picture does now show the full title of the Autorun entry. It is "\Microsoft\Windows\NetTrace\GatherNetworkInfo" and it lists an image path (location of file) as "c:\windows\system32\gathernetworkinfo.vbs." A visual basic file like this might arouse your suspicion, but this is actually just a component of the Network and Sharing Center in Windows 7. So this serves as a lesson that file names are not always to be used to judge whether a file is safe or not.

The last example, and for some reasons the most important, is the SmartDefrag entry. Smart Defrag is software from IObit that defragments hard drives in the background to keep performance optimal (and possibly prolong the life of a hard drive). The interesting thing is that I have no defragmenting task scheduled and I also don't have automatic defragmenting turned on.

So why does it still appear? The truth is some software will autorun on logon this way. If I were to go to Smart Defrag settings and uncheck the option that reads "Load automatically at Windows startup", and then hit F5 in Autoruns to refresh (check the system again), this entry would disappear.

So why is this important? Firstly it shows you that you can find applications that will fully load at startup listed under Scheduled Tasks and not just background tasks. Secondly, you should also take note that this Smart Defrag autorun is NOT detected under Startup in Microsoft's msconfig utility that comes with Windows. This is one reason why Autoruns is preferred to msconfig, it simply is more reliable for showing an accurate picture of what starts with Windows than the Microsoft utility. Unfortunately, msconfig is used a lot to manage startup programs, services etc. by professionals, when such a great free alternative exists.

What are these results? "Services"

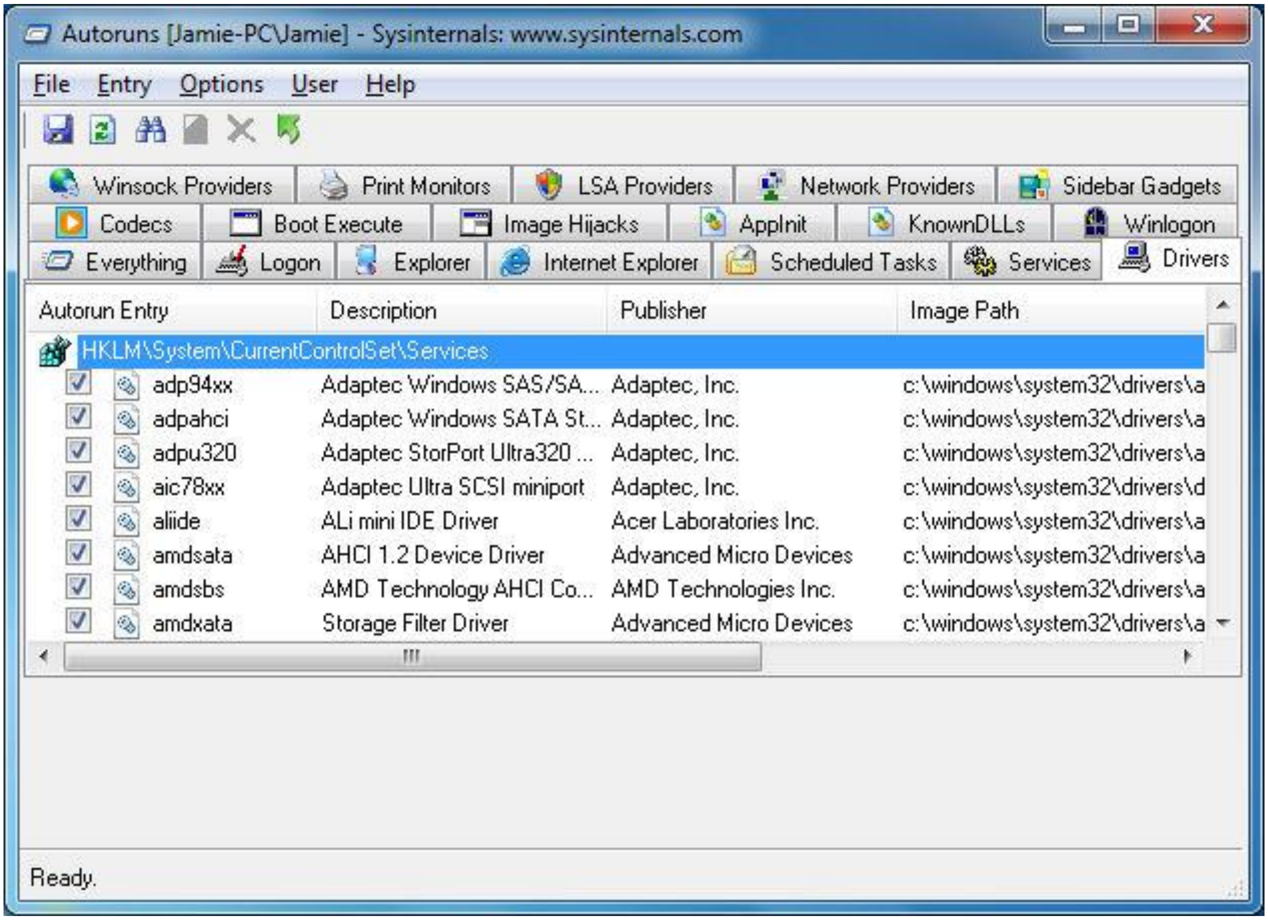


Autorun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Services			
☑ Synergy Client	Allows another computer to ...		c:\program files\synergy\synergyc.e
☑ XAudioService	User-mode gate for Modem ...	Conexant Systems, Inc.	c:\windows\system32\drivers\xaud

Autoruns will display all Windows services configured to start automatically on system boot. The picture above shows results with Microsoft & Windows Entries filtered out. This lets me see third-party services configured to start with the operating system. We can see the XAudioService and the Synergry Client, which allows me to use the laptop this picture was taken from as a second screen.

If you were to take off the Microsoft and Windows Filter, this list would suddenly get a lot bigger. Be careful about disabling third-party services as peripherals or other components may rely on the Windows service to be utilized correctly. If you do not have Microsoft and Windows results filtered out, be extremely careful. Do not disable or delete Windows services if you are not aware of the consequence of doing so.

What are these results? "Drivers"



Autorun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Services			
☑ adp94xx	Adaptec Windows SAS/SA...	Adaptec, Inc.	c:\windows\system32\drivers\a
☑ adpahci	Adaptec Windows SATA St...	Adaptec, Inc.	c:\windows\system32\drivers\a
☑ adpu320	Adaptec StorPort Ultra320 ...	Adaptec, Inc.	c:\windows\system32\drivers\a
☑ aic78xx	Adaptec Ultra SCSI miniport	Adaptec, Inc.	c:\windows\system32\drivers\d
☑ aliide	ALi mini IDE Driver	Acer Laboratories Inc.	c:\windows\system32\drivers\a
☑ amdsata	AHCI 1.2 Device Driver	Advanced Micro Devices	c:\windows\system32\drivers\a
☑ amdsbs	AMD Technology AHCI Co...	AMD Technologies Inc.	c:\windows\system32\drivers\a
☑ amdxata	Storage Filter Driver	Advanced Micro Devices	c:\windows\system32\drivers\a

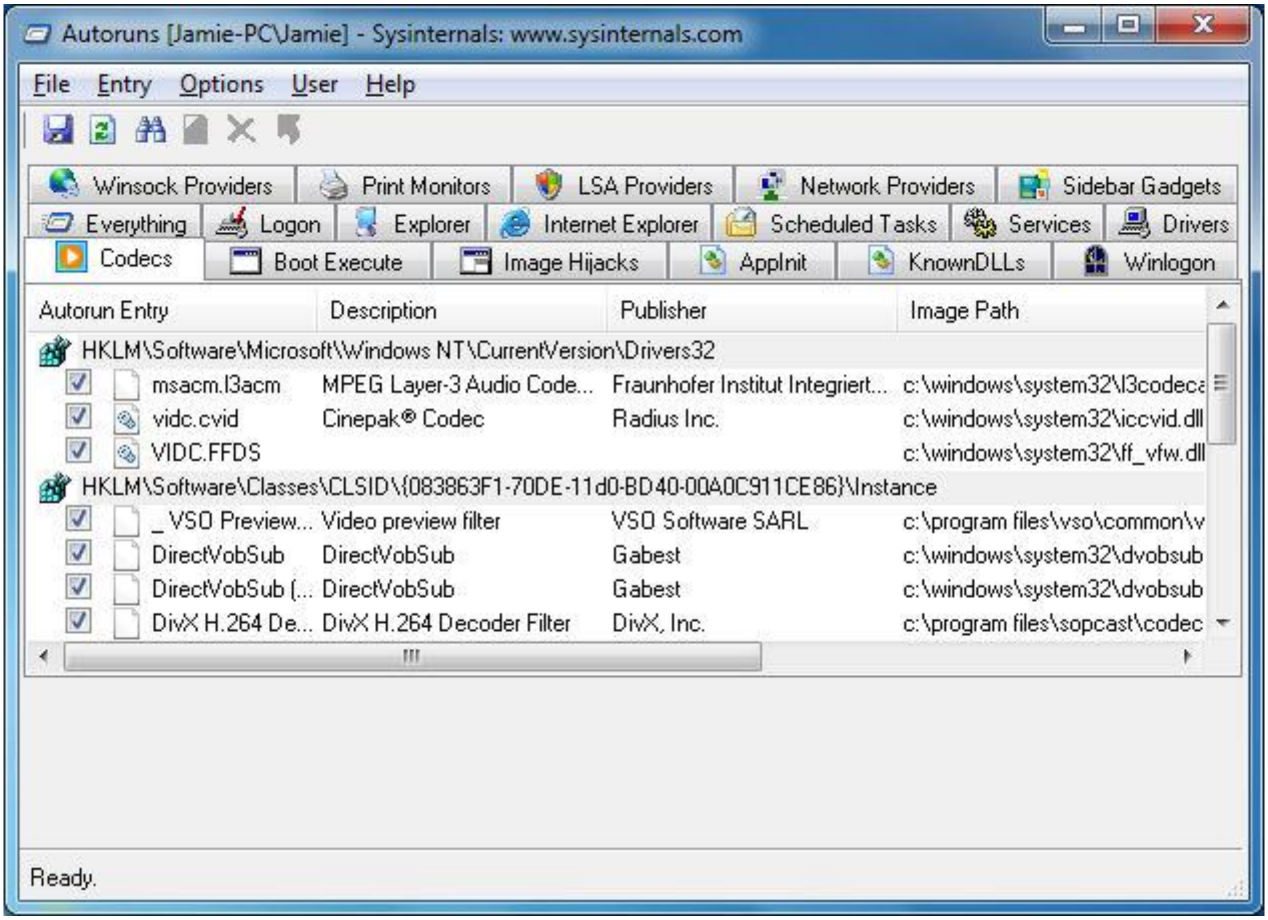
Ready.

Autoruns will display all kernel-mode drivers that are registered on the system with the exception of disabled drivers. Here you should filter out Microsoft and Windows results and you will see a comprehensive list of drivers required for all of your hardware to function properly with Windows.

You will see results from AMD, Intel, Broadcom, NVIDIA and more. You can generally get a lot of information here on what the drivers are, but it is not uncommon for drivers to have no available Description and to have no publisher listed. It can be useful to use the web search options when right-clicking a result if you need to look for information about a particular driver.

As with Services, be very careful about making changes here.

What are these results? "Codecs"



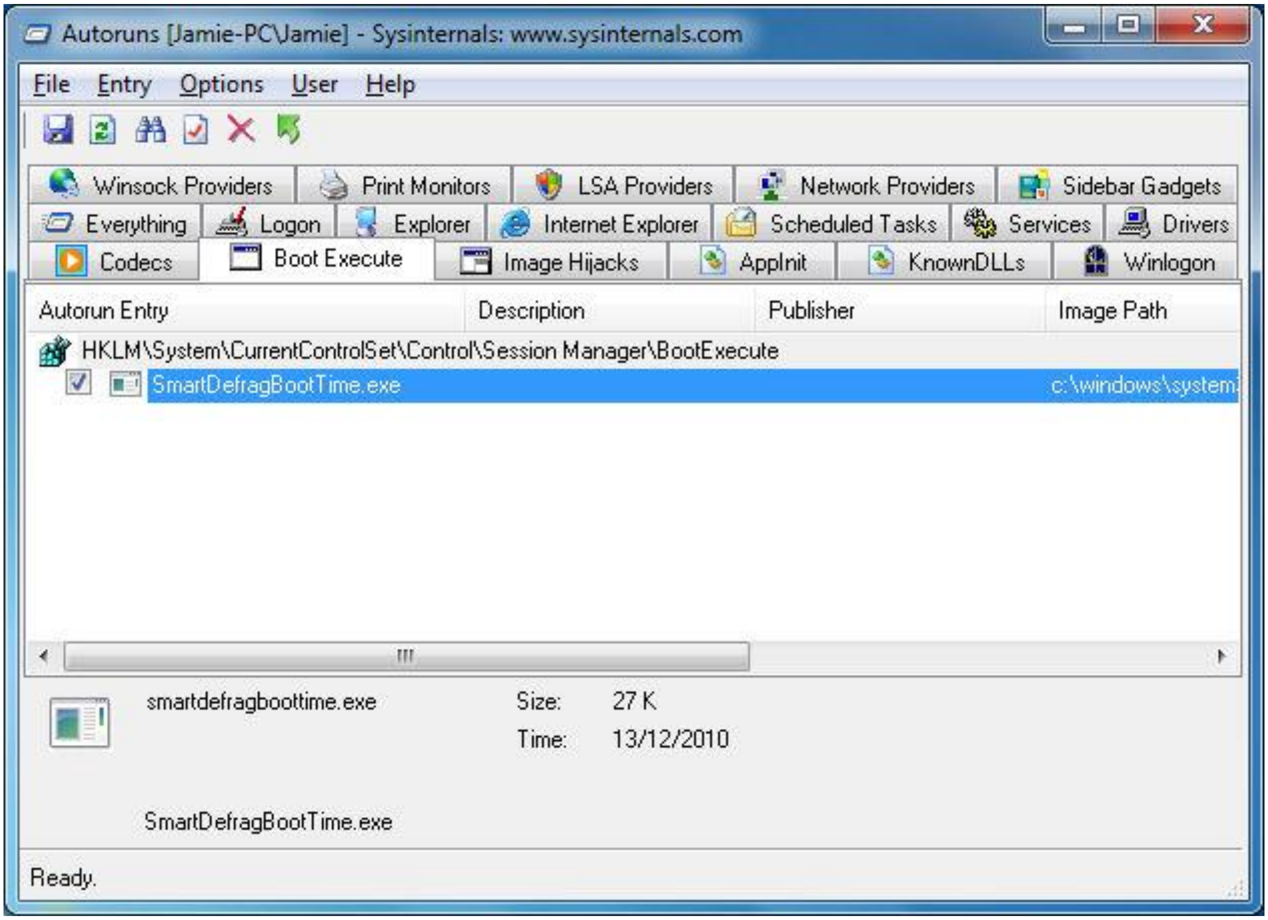
Autorun Entry	Description	Publisher	Image Path
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Drivers32			
☑ msacm.l3acm	MPEG Layer-3 Audio Code...	Fraunhofer Institut Integriert...	c:\windows\system32\l3codeca
☑ vidc.cvid	Cinepak® Codec	Radius Inc.	c:\windows\system32\iccvid.dll
☑ VIDC.FFDS			c:\windows\system32\ff_vfw.dll
HKLM\Software\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance			
☑ _VSO Preview...	Video preview filter	VSO Software SARL	c:\program files\vso\common\v
☑ DirectVobSub	DirectVobSub	Gabest	c:\windows\system32\dvobsub
☑ DirectVobSub (...	DirectVobSub	Gabest	c:\windows\system32\dvobsub
☑ DivX H.264 De...	DivX H.264 Decoder Filter	DivX, Inc.	c:\program files\sopcast\codec

Autoruns can go through codecs, typically used in the decoding and encoding of multimedia content. Codecs and/or DirectShow filters are vital for DirectShow-based multimedia players such as Windows Media Player. The first result showed in my example (Microsoft and Windows results filtered out) is an "MPEG Layer-3 Audio Codec for MSACM" from the Fraunhofer Institute - an MP3 codec.

Codecs and filters will also be present for video formats like DivX or filters for subtitle display might also be shown.

Autoruns can be useful if you are experiencing trouble playing back a certain type of content, since you can disable codecs or delete the reference to them if you wish.

What are these results? "Boot Execute"



Autorun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute			
☑ SmartDefragBootTime.exe			c:\windows\system

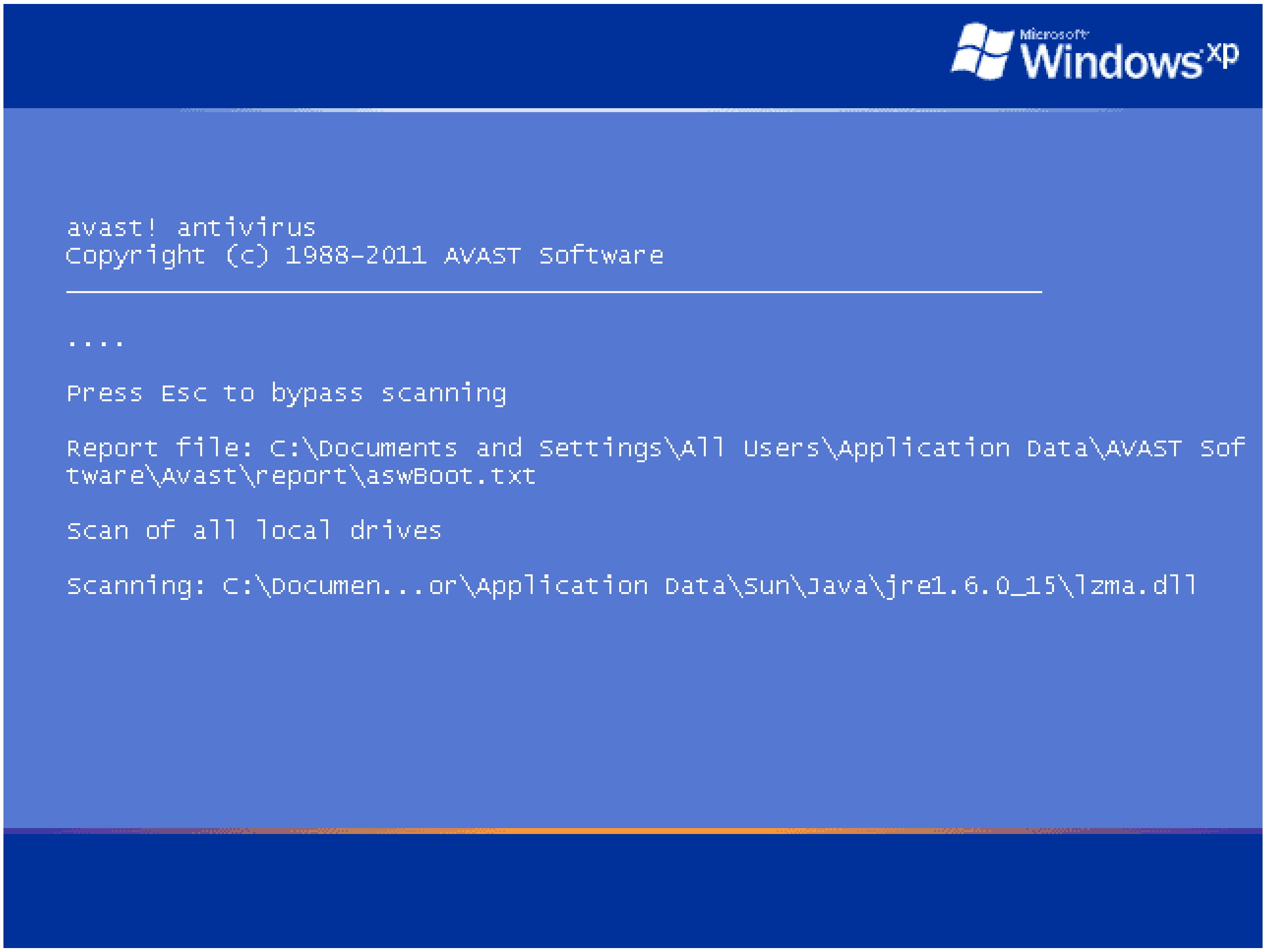
smartdefragbootime.exe

Size: 27 K
Time: 13/12/2010

SmartDefragBootTime.exe

Autoruns will display native images that run very early in the Windows boot process. With Microsoft and Windows entries filtered it is likely that you would see nothing at all. I set SmartDefrag to perform a boot time defrag of the pagefile, $MFT and registry files. The defrag operation would take place early in the Windows boot because when Windows is fully loaded, you would be unable to defragment any of these system files properly since they are protected and in use.

In order for Smart Defrag to do this, it has to execute a defragmenting utility very early in the boot process. It can do this by editing the HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute key in the Windows registry. That happens to be the main source checked by Autoruns under Boot Execute. It is listed in the picture above as SmartDefragBootTime.exe.



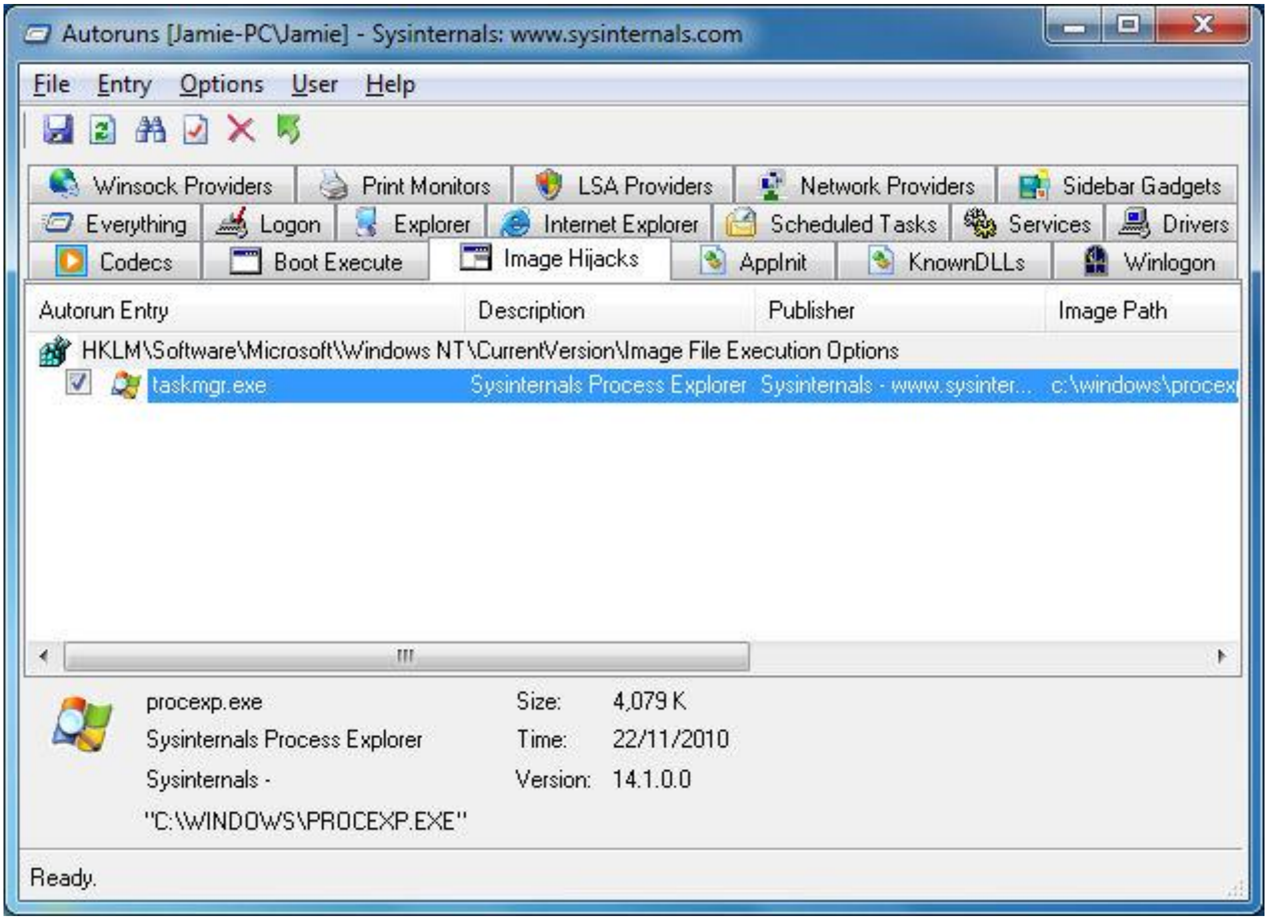
```
avast! antivirus
Copyright (c) 1988-2011 AVAST Software

....

Press Esc to bypass scanning

Report file: C:\Documents and Settings\All Users\Application Data\AVAST Sof
tware\Avast\report\aswBoot.txt

Scan of all local drives

Scanning: C:\Documen...or\Application Data\Sun\Java\jre1.6.0_15\lzma.dll
```

The image shown above is an example of a boot-time process. It is the Boot Time Scan feature of the Avast! Anti-Virus suite, running mid-boot of Windows XP. It loads early in boot before most malicious software loads, making it more vulnerable to the security product. This scheduled scan would also be visible in Autoruns and could be disabled or removed.

With Microsoft and Windows Entries left unfiltered, you would also see a reference to the autochk utility, which checks hard drives connected to the system to see if they are marked as "dirty". If so, it tells you that one of your drives needs to be tested and gives you a number of seconds to decline by hitting a key.. something I'm sure we've all seen before.

Of course, this could also be targeted by malicious software to load up junk nice and early in the boot process. If you find a suspicious entry it would be advisable to look for support.

What are these results? "Image Hijacks"



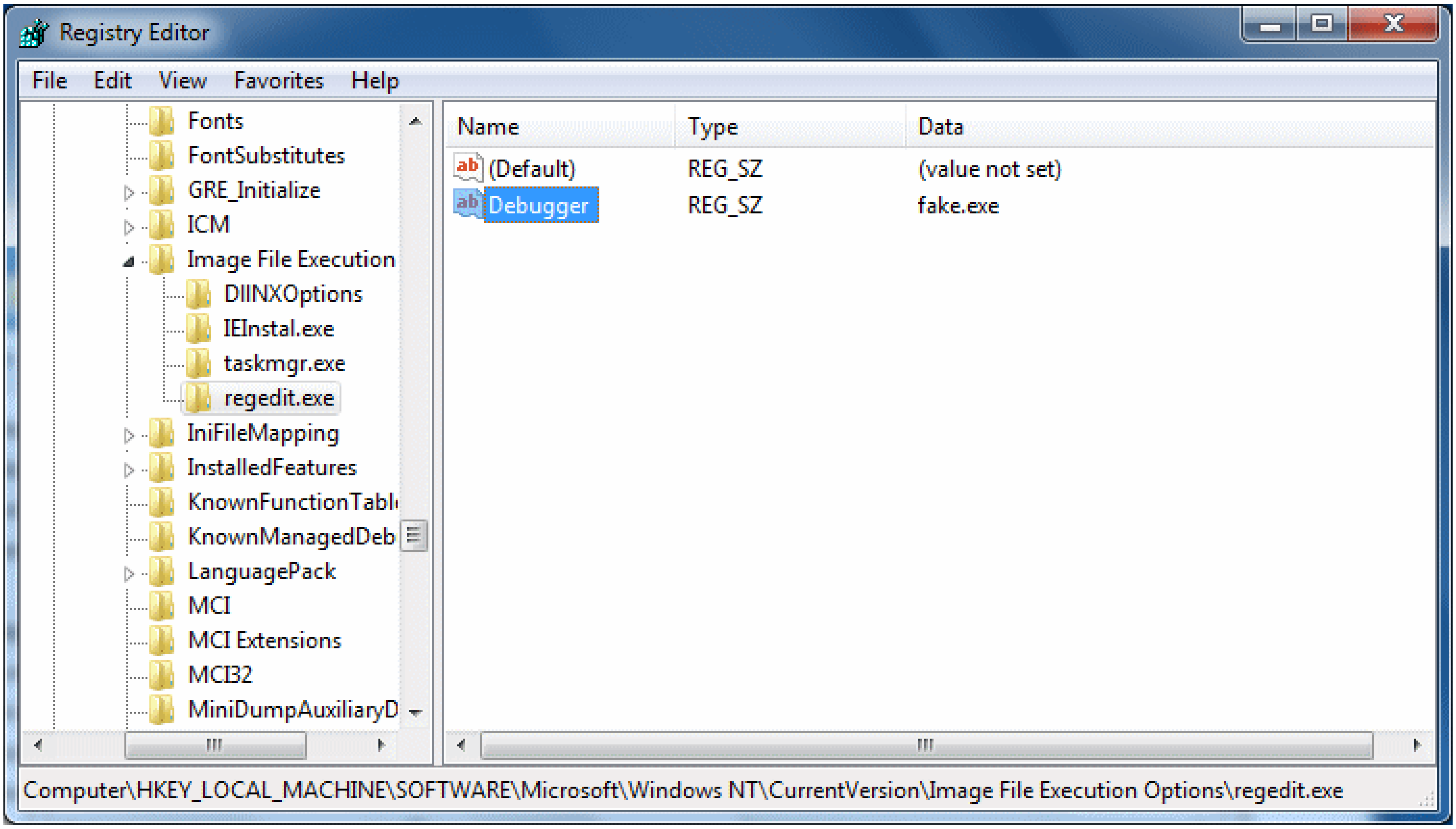
Autorun Entry	Description	Publisher	Image Path
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options			
☑ taskmgr.exe	Sysinternals Process Explorer	Sysinternals - www.sysinter...	c:\windows\procex

procexp.exe	Size:	4,079 K
Sysinternals Process Explorer	Time:	22/11/2010
Sysinternals -	Version:	14.1.0.0
"C:\WINDOWS\PROCEXP.EXE"		

The term "Image Hijack" describes how a malicious program can use techniques to block the running of a certain application or can instead run something completely different. The most common way to do this for malicious software is by exploiting the HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options registry key.

This key, used correctly, can attach a debugger to a process as soon as it starts running. There are legitimate reasons why this would be available. However, it presents a problem as it makes it possible for malicious entries to block access to possibly vital tools.

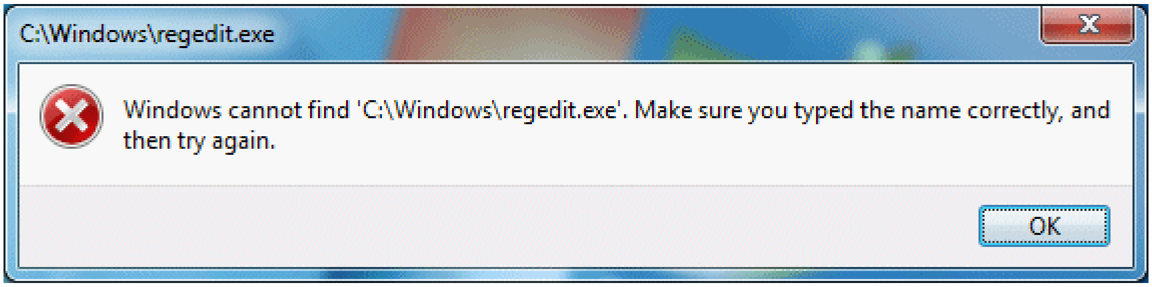
Here is an example. Let's say I want to make it difficult to open regedit in Windows 7. I could use the group policy editor of course, or a number of other options, but I will try something that Autoruns is going to find. I open regedit and navigate to HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Debugger	REG_SZ	fake.exe

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\regedit.exe

I then create a new Key and call it regedit.exe (shown on the left in the image above). Now I create a new String Value under the regedit.exe key. I name the value "Debugger" and for a value I simply put "fake.exe". Now that I have done that, I go to the Start Menu and type regedit into the search box. Immediately I see a result for regedit. So now I click on it like I would have done any time before and...



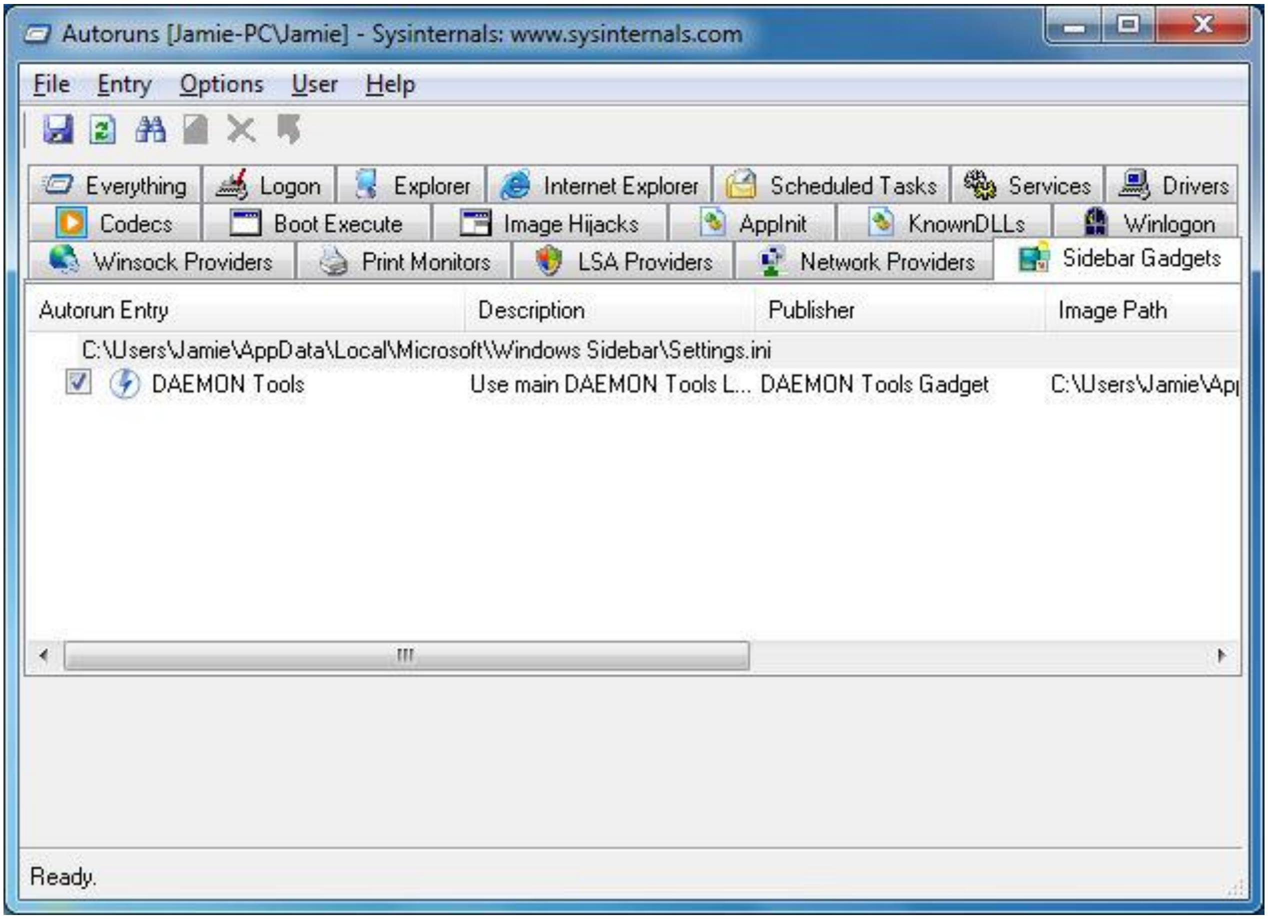
Windows cannot find 'C:\Windows\regedit.exe'. Make sure you typed the name correctly, and then try again.

So even though it found the file when you searched for it, you get a prompt telling you that the file cannot be found. Even if you go to the Windows folder and manually double-click on the regedit.exe file, you will get the exact same message.

So why would Windows allow for such a thing? Well as mentioned before there are legitimate reasons to being able to specify a debugger for troubleshooting application crashes. Also, it's not always used for bad purposes. For example, the developer of Autoruns (Sysinternals) has another popular free tool called Process Explorer, and it has an option to "Replace Task Manager" when you hit CTRL, ALT and DEL.

It achieves this by specifying the Process Explorer executable as the debugger value under a taskman.exe key, and is very useful for people (like me) who would not use Task Manager when a much better alternative is available. The picture that I showed of Autoruns displaying the Image Hijack results clearly shows the Process Explorer entry as mined from the registry. Image Hijack results can be disabled or deleted as easily as anything else.

What are these results? "Sidebar Gadgets"



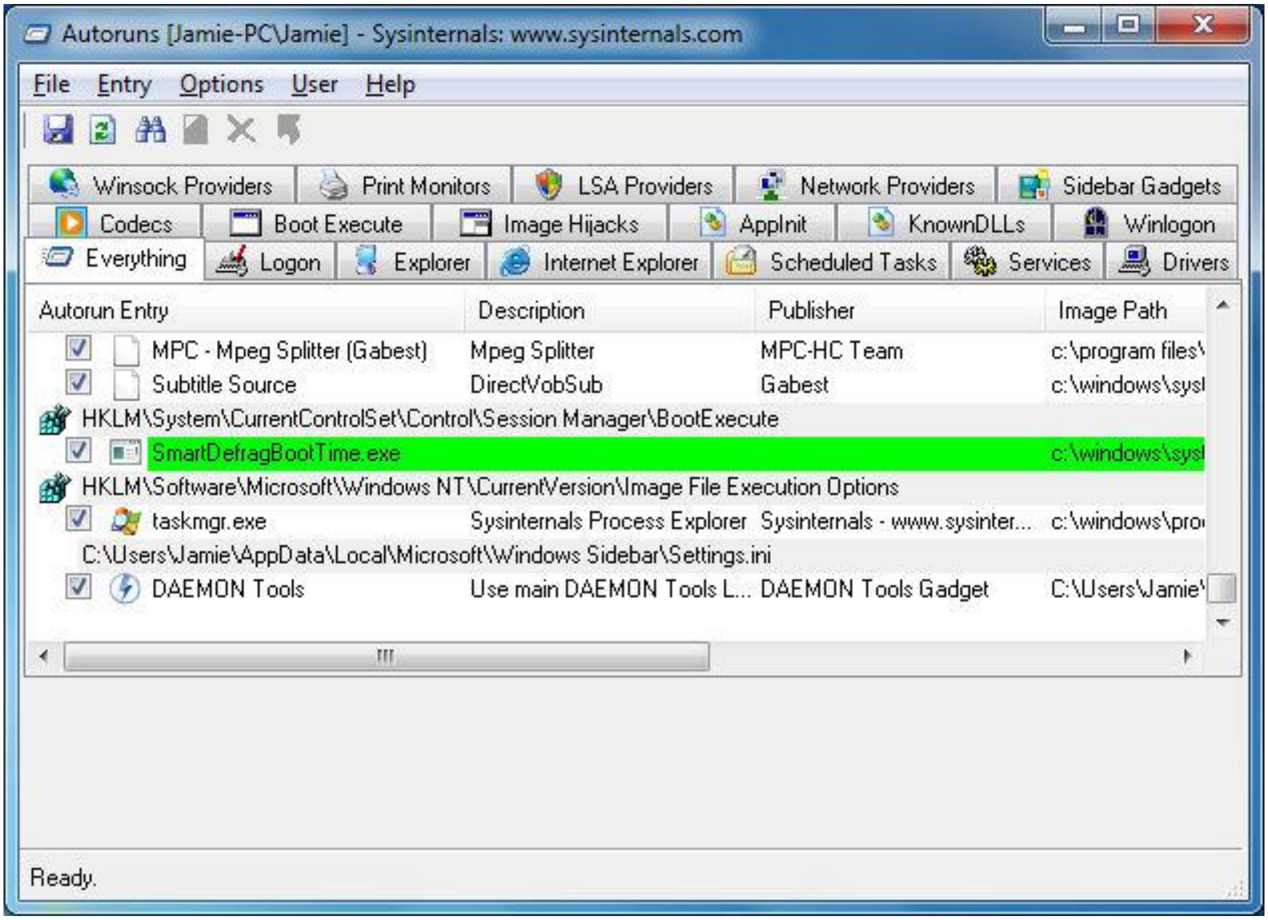
Autorun Entry	Description	Publisher	Image Path
C:\Users\Jamie\AppData\Local\Microsoft\Windows Sidebar\Settings.ini			
☑ DAEMON Tools	Use main DAEMON Tools L...	DAEMON Tools Gadget	C:\Users\Jamie\Ap

In Windows Vista and in Windows 7, the sidebar is playing a more prominent role for users than it ever has before. A lot of software comes with its own Sidebar gadget, giving an option to include it as part of the general installation.

Since gadgets in the sidebar are technically things that load automatically on start-up, they deserve to be listed by Autoruns the same as anything else. In the example picture, there is only one gadget listed, and that is the Daemon Tools gadget.

I do have more gadgets on my sidebar however, and they are viewable by removing the filter on Windows and Microsoft entries in the Options menu. Sidebar gadgets can be disabled or deleted just as easily as anything else in Autoruns.

Saving Autoruns Log and comparing it later



Autorun Entry	Description	Publisher	Image Path
☑ MPC - Mpeg Splitter (Gabest)	Mpeg Splitter	MPC-HC Team	c:\program files\
☑ Subtitle Source	DirectVobSub	Gabest	c:\windows\syst
HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute			
☑ SmartDefragBootTime.exe			c:\windows\syst
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options			
☑ taskmgr.exe	Sysinternals Process Explorer	Sysinternals - www.sysinter...	c:\windows\pro
C:\Users\Jamie\AppData\Local\Microsoft\Windows Sidebar\Settings.ini			
☑ DAEMON Tools	Use main DAEMON Tools L...	DAEMON Tools Gadget	C:\Users\Jamie\

Autoruns cannot tell you the state of your system in the past, of course, but it can compare a log of an Autoruns output that you saved in the past to the current system state. As shown in the picture above, it also helpfully displays "new" Autoruns in green. This can be very helpful to find out what is a causing a new problem on a system, and it can be an interesting way for you to find out how a program sets itself to start on your computer.

To save an Autoruns log, simply go to File - Save. It can be output in plain text if you would like. Now if you want to compare it later to your system, you can go to File - Compare and simply open the log that you saved before.