

## Autostart Locations where Malware can Hide by Bleepingcomputer.com

**Windows Boot Device Drivers** - These drivers are loaded first as they are required for the proper operation of hardware such as storage devices. Boot device drivers will be located under the following key and have a Start value equal to 0.

RegistryKeys:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services

### **Windows will now perform various tasks and then start the Winlogon process.**

Winlogon eventually starts the service control manager that loads services and drivers that are set for auto-start.

Windows Auto-start Services & Drivers - The Service Control Manager (SCM) process (\Windows\System32\services.exe), will now launch any services or drivers that are marked with a Start value of 2.

RegistryKeys:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services

### **RunServicesOnce**

This key is designed to start services when a computer boots up. These entries can also continue running even after you log on, but must be completed before the HKEY\_LOCAL\_MACHINE\...\RunOnce registry can start loading its programs.

RegistryKeys:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce

### **RunServices**

This key is designed to start services as well. These entries can also continue running even after you log on, but must be completed before the HKEY\_LOCAL\_MACHINE\...\RunOnce registry can start loading its programs.

RegistryKeys:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

### **The Windows logon prompt is shown on the screen. After a user logs in the rest of the keys continue.**

Notify - This key is used to add a program that will run when a particular event occurs. Events include logon, logoff, startup, shutdown, start screensaver, and stop screensaver. When Winlogon.exe generates an event such as the ones listed, Windows will look in the Notify registry key for a DLL that will handle this event. Malware has been known to use this method to load itself when a user logs on to their computer. Loading in such a way allows the malware program to load in such a way that it is not easy to stop.

RegistryKey:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify

### **UserInit Key**

This key specifies what program should be launched right after a user logs into Windows. The default program for this key is C:\windows\system32\userinit.exe. Userinit.exe is a program that restores your profile, fonts, colors, etc for your user name. It is possible to add further programs that will launch from this key by separating the programs with a comma.

For example:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit=C:\windows\system32\userinit.exe,

c:\windows\badprogram.exe.

This will make both programs launch when you log in and is a common place for trojans, hijackers, and spyware to launch from.

RegistryKey:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit

### **Shell Value**

This value contains a list of comma separated values that Userinit.exe will launch. The default shell for Windows is explorer.exe, though there are legitimate replacements that have been made. When userinit.exe starts the shell, it will first launch the Shell value found in HKEY\_CURRENT\_USER. If this value is not present, it will then launch the value found in HKEY\_LOCAL\_MACHINE.

RegistryKey:

HKEY\_CURRENT\_USER\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell

HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell

**The rest of the Autostart locations will now be processed.**

### **RunOnce Local Machine Key**

These keys are designed to be used primarily by Setup programs. Entries in these keys are started once and then are deleted from the key. If there is an exclamation point preceding the value of the key, the entry will not be deleted until after the program completes, otherwise it will be deleted before the program runs. This is important, because if the exclamation point is not used, and the program referenced in this key fails to complete, it will not run again as it will have already been deleted. All entries in this key are started synchronously in an undefined order. Due to this, all programs in this key must be finished before any entries in

HKEY\_LOCAL\_MACHINE\...\Run,

HKEY\_CURRENT\_USER\...\Run,

HKEY\_CURRENT\_USER\...\RunOnce, and

Startup Folders can be loaded.

The RunOnce keys are ignored under Windows 2000 and Windows XP in Safe Mode. The RunOnce keys are not supported by Windows

NT 3.51.

Registry Keys:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

**Run** - These are the most common startup locations for programs to install auto start from. By default these keys are not executed in Safe mode. If you prefix the value of these keys with an asterisk, \*, it will run in Safe Mode.

Registry Keys:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

### **All Users Startup Folder**

For Windows XP, 2000, and NT, this folder is used for programs that should be auto started for all users who will login to this computer. It is generally found at:

**Windows XP**

C:\Documents and Settings\All Users\Start Menu\Programs\Startup

**Windows NT**

C:\wont\Profiles\All Users\Start Menu\Programs\Startup

**Windows 2000**

C:\Documents and Settings\All Users\Start Menu\Programs\Startup

### **User Profile Startup Folder**

This folder will be executed for the particular user who logs in. This folder is usually found in:

**Win 9X, ME**

c:\windows\start menu\programs\startup

**Windows XP**

C:\Documents and Settings\LoginName\Start Menu\Programs\Startup

### **RunOnce Current User Key**

These keys are designed to be used primarily by Setup programs. Entries in these keys are started once and then are deleted from the key. If there is an exclamation point preceding the value of the key, the entry will not be deleted until after the program completes, otherwise it will be deleted before the program runs. This is important, because if the exclamation point is not used, and the program referenced in this key fails to complete, it will not run again as it will have already been deleted. The RunOnce keys are ignored under Windows 2000 and Windows XP in Safe Mode. The RunOnce keys are not supported by Windows NT 3.51.

Registry Key:

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

### **Explorer Run**

These keys are generally used to load programs as part of a policy set in place on the computer or user.

Registry Keys:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

### Load Key

This key is not commonly used anymore, but can be used to auto start programs.

RegistryKey:

HKEY\_CURRENT\_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows\load

### AppInit DLLs

This value corresponds to files being loaded through the AppInit\_DLLs registry value. The AppInit\_DLLs registry value contains a list of DLLs that will be loaded when user32.dll is loaded. As most Windows executables use the user32.dll, that means that any DLL that is listed in the AppInit\_DLLs registry key will be loaded also. This makes it very difficult to remove the DLL as it will be loaded

within multiple processes, some of which can not be stopped without causing system instability. The user32.dll file is also used by processes that are automatically started by the system when you log on. This means that the files loaded in the AppInit\_DLLs value will be loaded very early in the Windows startup routine allowing the DLL to hide itself or protect itself before we have access to the system.

RegistryKey:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Windows

### ShellServiceObjectDelayLoad

This Registry value contains values in a similar way as the Run key does. The difference is that instead of pointing to the file itself, it points to the CLSID's InProcServer, which contains the information about the particular DLL file that is being used.

The files under this key are loaded automatically by Explorer.exe when your computer starts. Because Explorer.exe is the shell for your computer, it will always start, thus always loading the files under this key. These files are therefore loaded early in the startup process before any human intervention occurs.

RegistryKey:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

### SharedTaskScheduler

This section corresponds to files being loaded through the SharedTaskScheduler registry value for XP, NT, 2000 machines. The entries in this registry value run automatically when you start windows.

RegistryKey:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler

### The following are files that programs can autostart from on bootup:

1. c:\autoexec.bat
2. c:\config.sys
3. windir\wininit.ini - Usually used by setup programs to have a file run once and then get deleted.
4. windir\winstart.bat
5. windir\win.ini - [windows] "load"
6. windir\win.ini - [windows] "run"
7. windir\system.ini - [boot] "shell"
8. windir\system.ini - [boot] "scrnsave.exe"
9. windir\dosstart.bat - Used in Win95 or 98 when you select the "Restart in MS-DOS mode" in the shutdown menu.
10. windir\system\autoexec.nt
11. windir\system\config.nt

Though it is good to know these details, if you just need a program to quickly scan these keys and produce a list for you, you can use Sysinternals Autoruns program. While you are at that site, you should browse some of the other excellent utilities.