



Automatic Startup in Microsoft Windows

infectionvectors.com

April 2004

The phrase “Corresponding Registry entries” appears throughout reports on infectionvectors.com. The following is a brief discussion of what this means, how the entries are used, and a general guide to identifying a virus infection by inspecting the Windows Registry.

When used in reference to automatic startup of a virus, “corresponding Registry entries” refers to the keys and values a virus will set in an effort to ensure that it is started each time the Windows machine is rebooted, a user logs in, etc. The reason that these keys exist is to allow system utilities (such as anti virus software) and services to start up with the operating system, not requiring manual user intervention for every restart. They also allow “setup” routines to add a value indicating that a program needs to be run after a reboot of the computer. Within the Registry Hives are multiple locations where a virus could plant such keys and values, although virus writers use some much more than others. Understanding these keys and how they are used is important in analyzing how viruses work. A knowledgeable user can also scan the keys when investigating suspicious activity on a PC. New and/or unrecognizable entries may be a viral or spyware application’s startup hook.

RunServicesOnce

These keys house the Services that are to load on the next boot. It exists in both HKEY_LOCAL_MACHINE and HKEY_LOCAL_USER for this purpose.

`\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`

RunServices

This key houses the Services that are to load on each boot. It exists in both HKEY_LOCAL_MACHINE and HKEY_LOCAL_USER for this purpose.

`\Software\Microsoft\Windows\CurrentVersion\RunServices`

RunOnce

These keys are designed to load applications on only the next restart/login. Once a program is run the entry is deleted (unless it has an exclamation point “!” in front of the entry, in which case it is deleted after the program finishes). Primarily, this is used by setup routines that require a reboot before finishing installations. The keys in HKEY_LOCAL_MACHINE:

\Software\Microsoft\Windows\CurrentVersion\RunOnce
\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

The key in HKEY_CURRENT_USER:

\Software\Microsoft\Windows\CurrentVersion\RunOnce

Run (Explorer)

This key contains a list of applications to start with Windows. It exists in both HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER.

\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

<http://support.microsoft.com/default.aspx?scid=kb;en-us;270035>

UserInit

This list indicates which programs should be run once a user logs into Windows. It exists in HKEY_LOCAL_MACHINE:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

An additional entry here adds itself to the auto-start list by appending a path/program to the value. This is the normal entry: C:\windows\system32\userinit.exe. Something like this is a suspicious entry: C:\Windows\SYSTEM32\userinit.exe,C:\UR_0\(\n3)\.exe. Note, there are legitimate applications that may be appended to the “userinit.exe” entry.

Load

This key still exists in the Registry, however, it is rarely used (the last legitimate application I remember using this was SMS). The majority of viruses also bypass this key (probably because it is not especially well-known).

SMS reference (an fix bulletin for a piece of SMS that used the key):

<http://www.microsoft.com/smsserver/downloads/20/servicepacks/sms20sp2/operation.asp>

Last virus I know of that used the key:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.kullan.html>

The Startup Folder

Of course, Registry entries are not required. Anything that is placed in the Windows Startup folder will be executed. There is one for the “All Users” group in Windows NT/2000/XP and one for the specific user in all versions of Windows.

Any entry (application, shortcut, document, etc.) found in the “Start Menu\Programs\Startup\” directory (for NT/2000/XP this is in the “Document and Settings” folder) will be executed. Worms, as in the case of Nebiwo/Deborm, use this frequently to ensure automatic startup. However, this is the most visible means of achieving this, as the shortcut/application will appear in the user’s Start menu.

Alternatively, anything that is written to the WIN.INI file will be started. This also goes for the AUTOEXEC.BAT file for older versions of Windows.

Changes to Default Shells/Handlers

It is also possible to change a user’s default shell by “adjusting” the Registry entries associated with CMD, EXE, BAT, etc. files. This is almost an infinite regression of entries, as it is, of course, possible to change any entry and have it hook the virus/Trojan. This is very rare, as most viruses want to aim at the lowest common denominator, increasing the number of infections. Some keys that are more likely candidates than others however:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon

HKEY_CLASSES_ROOT\exefile\shell\open\command

HKEY_CLASSES_ROOT\batfile\shell\open\command

Viral Infections

Of course, if a virus has infected any EXE, the virus will run once the infected file is executed.

The primary focus of this brief has been on the standard locations for hooking a piece of malware with the autostart entries in the Registry, so additional mechanisms of autostarting applications will not be explored. With the near limitless changes a virus can make to the Registry (sometimes for functional purposes, sometimes, destructive, sometimes just to tag a machine), it is advised that all critical systems have some time of monitoring tool running to identify unauthorized changes. This could be something like antivirus software, Tripwire, or even a manually run tool like RegShot.

Copyright © 2004 infectionvectors.com. All rights reserved.
For reprint rights contact@infectionvectors.com