Autoruns

Sysinternals - www.sysinternals.com

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and what extension load into various Windows processes, including Explorer and Internet Explorer. It reports the image timestamp of executables, the last-modified timestamp of other file types, and the last-modified timestamp of the autostart locations. A "Hide Signed Microsoft Entries" option helps you to zoom in on third-party auto-starting images that have been added to your system.

Autoruns works on Windows XP and higher, including 64-bit Windows.

Note: before you send e-mail reporting what you believe to be an auto-start location that's overlooked by Autoruns, please make sure that Autoruns doesn't cover it and verify that the location actually works.

Displayed Locations and Entries

Simply run Autoruns and it shows you the currently configured auto-start applications in the locations that most directly execute applications. Perform a new scan that reflects changes to options by refreshing the display.

- **Logon** This entry results in scans of standard autostart locations such as the Startup folder for the current user and all users, the Run Registry keys, and standard application launch locations.
- **Explorer** Select this entry to see Explorer shell extensions, browser helper objects, explorer toolbars, active setup executions, and shell execute hooks.
- **Internet Explorer** This entry shows Browser Helper Objects (BHO's), Internet Explorer toolbars and extensions.
- **Services** All Windows services configured to start automatically when the system boots.
- **Drivers** This displays all kernel-mode drivers registered on the system except those that are disabled.
- **Scheduled Tasks** Task scheduler tasks configured to start at boot or logon.
- **AppInit DLLs** This has Autoruns shows DLLs registered as application initialization DLLs.
- **Boot Execute** Native images (as opposed to Windows images) that run early during the boot process.
- **Image Hijacks** Image file execution options and command prompt autostarts.
- **Known DLLs** This reports the location of DLLs that Windows loads into applications that reference them.
- **Winlogon Notifications** Shows DLLs that register for Winlogon notification of logon events.
- **Winsock Providers** Shows registered Winsock protocols, including Winsock service providers. Malware often installs itself as a Winsock service provider because there are few tools that can remove them. Autoruns can disable them, but cannot delete them.
- **LSA Providers** Shows registers Local Security Authority (LSA)

authentication, notification and security packages.
- **Printer Monitor Drivers** Displays DLLs that load into the print spooling service. Malware has used this support to autostart itself.
- **Sidebar** Displays Windows Sidebar gadgets.

Unless the **Include Empty Locations** selection in the **Options** menu is checked Autoruns doesn't show locations with no entries.

The **Users** menu is populated with user names. Select one to view the auto-starting images for that account.

Scan Options

Use the scan options dialog to specify what information should be collected in a scan.

The **Verify Signatures** can result in Autoruns querying certificate revocation list (CRL) web sites to determine if image signatures are valid. Autoruns displays the text "(Not verified)" next to the company name of an image that either does not have a signature or has a signature that is not signed by a certificate root authority on the list of root authorities trusted by the system. If you select the **Verify Signatures** option, entries corresponding to unsigned images highlight in light red. If the **Verify Signatures** option is disabled, items that have a missing image or an image with no company name or description highlight in light red.

If you enable the **Check VirusTotal** option, Autoruns will query the free VirusTotal.com service to get the results of the entry's scan with dozens of antimalware engine. The result displayed is either the number of engines that reported the entry as malicious over the total number of engines that have scanned the entry, or 'unknown', which indicates the entry has not been submitted for scanning. You can enable **Submit Unknown Images** to have Autoruns submit an image for scanning and wait for the results, which can take several minutes.

To have Autoruns only scan per-user locations for the current or specified user profile, select the **Scan Only Per-User Locations** option. This can be useful for analyzing only the entries under the influence of unprivileged accounts.

Filters

Use the **Hide Microsoft Entries, Hide Windows Entries**, and **Hide VirusTotal Clean Entries** in the **Options** menu to help you identify software that's been added to a system since installation. Autoruns prefixes the name of an image's publisher with "(Not verified)" if it cannot verify a digital signature for the file that's trusted by the system.

- The **Hide Microsoft Entries** selection omits images that have been signed by Microsoft if **Verify Signatures** is selected and omits images that have Microsoft in their resource's company name field if **Verify Signatures** is not selected.
- The **Hide Windows Entries** omits images signed by Windows if **Verify Signatures** is selected. If **Verify Signatures** is not selected, **Hide Windows Entries** omits images that have Microsoft in their resource's company name field and the image resides beneath the %SystemRoot% directory.
- The Hide VirusTotal Clean Entries omits any entries that have

The toolbar also includes a free-form text entry that dynamically filters the displayed items. To undo a filter, simply clear the filter entry.

Getting More Information about an Entry

There are several ways to get more information about an autorun location or entry. To view a location or entry in **Explorer** or **Regedit** chose Jump To in the **Entry** menu or double-click on the entry or location's line in the display. You can view Explorer's file properties dialog for an entry's image file by choosing **Properties** in the **Entry** menu. You can also have Autoruns automatically execute an Internet search in your browser by selecting **Search Online** in the **Entry** menu.

Disabling and Deleting Entries

If you don't want an entry to activate the next time you boot or login you can either disable or delete it. To disable an entry uncheck it. Autoruns will store the startup information in a backup location so that it can reactivate the entry when you recheck it. For items stored in startup folders Autoruns creates a subfolder named Autorunsdisabled. Check a disabled item to re-enable it.

You should delete items that you do not wish to ever execute. Do so by choosing **Delete** in the **Entry** menu. Only the currently selected item will be deleted.

If you are running Autoruns without administrative privileges on Windows Vista and attempt to change the state of a global entry, you'll be denied access. Autoruns will display a dialog with a button that enables you to re-launch Autoruns with administrative rights. You can also use the -e command-line option to launch initially launch Autoruns with administrative rights.

Saving, Loading and Exporting

You can save the results of a scan with **File->Save** and load a saved scan with **File->Load.** These commands work with native Autoruns file formats, but you can use File->Export to save a text-only version of the scan results. You can also automate the generation of native Autoruns export files with command line options:

usage: autoruns [[-v] -a <output file>]

-v	Verify image digital signatures
-a	Run automatically, export scan results to an autoruns output file, and then exit

Autorunsc, the command-line version of Autoruns, can be scripted and also reports the cryptographic hashes of the images identified in a scan.

Comparing to Saved Results

You can compare the current Autoruns display with previous results that you've saved. Select **File|Compare** and browse to the saved file. Autoruns will display in green any new items, which correspond to entries that are not present in the saved file, and in red any items that have been deleted.

Analyzing Offline Systems

You can use Autoruns to analyze the autostart configuration of offline systems, something that can be useful for malware analysis and cleaning. To analyze an offline system, open the offline-system browse dialog by selecting **File|Analyze Offline System**. Specify the path to the system root (e.g. \Windows) directory of the system you wish to examine. You can also specify the location of an associated off-line user profile to examine by entering the path to the top-level directory of the user profile (e.g. \users\joe).

Note that Autoruns will only show correct file information for autostart paths that are on the same volume as the system volume.

Reporting Bugs and Feedback

If you wish to report a bug, please check the Sysinternals Autoruns forum first to see if it has already been reported or if there's a work-around. When submitting a bug, provide a complete description of your system and describe the behavior you see compared to what you expect to see. Please try to supply enough information so that we can reproduce the problem. Send bug reports to markruss@microsoft.com.