Find and remove Malware with Sysinternals Tools - Part 2: Autoruns

In the second part of this series, I will show you how to use the Autoruns tool to find malware that starts during the startup phase.

In the second part of this series, I will show you how to use the Autoruns tool to find malware that starts during the startup phase.

In Part 1 of this series, we learned how to use Process Explorer to find suspicious processes that are active malware in the system. In this section, we will show you how to use the Autoruns tool to find malware that starts during the startup phase.

Overview of Autoruns

The next tool we will look at is Autoruns, which will show you what programs are set up to run during system boot and login process. The configuration for this tool is very flexible, allowing you to not only display programs in the startup, registry, Run and RunOnce folders, but also many other programs, such as Winlogon directives, objects. browser, toolbar, autostart service, etc. And it will display them in the order processed by Windows. You can disable startup programs directly from within Autoruns. The current version of this tool is 10.07 and it can run on Windows XP / Server 2003 as well as newer versions. You can download the tool here.

The command line version is autorunsc also available in this download. Both are downloaded as executable files in a compressed file, along with a help file (autoruns.chm). As you can see in Figure 1, this tool is much more comprehensive than the Windows tool called MSConfig.

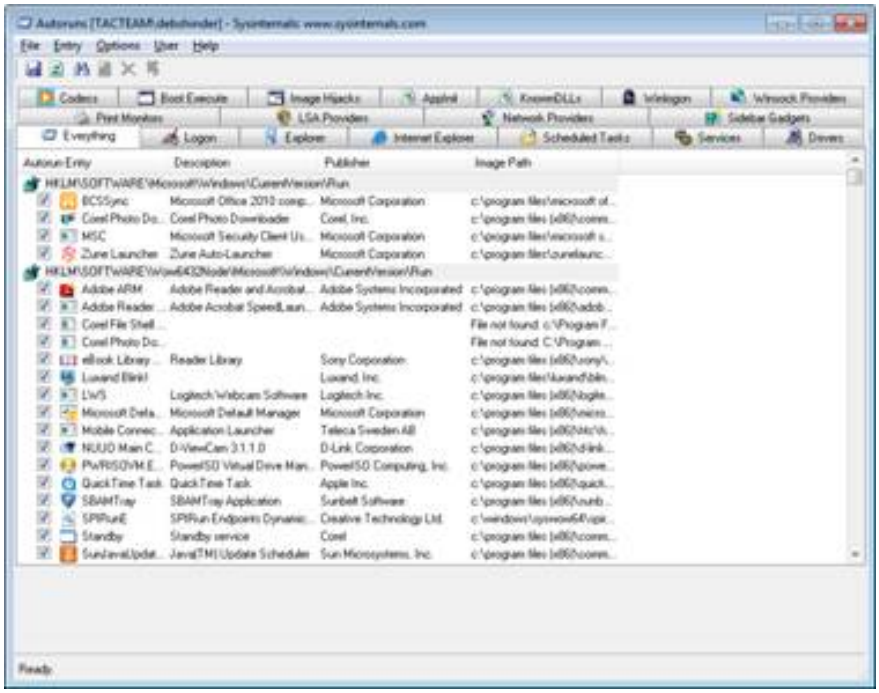

Figure 1

At first glance, you can see the interface has 18 different tabs above. The first tab labeled 'Everything' will show you all the types of programs and services configured to run at startup. Surely you will be surprised with the amount you see here. Unlike MSConfig, Autoruns does not require administrator rights.

Other tabs allow you to see information categorized by category, including:

- Logon
- Explorer (context menus, expand, .)
- Internet Explorer (toolbar, browser object)
- Scheduled Tasks (the process of running in the background through activating events)
- Services (default Windows items are hidden)
- Drivers
- Print Monitors
- LSA Providers
- Network Providers
- Sidebar Gadgets
- Codecs
- Boot Execute
- Image Hijacks
- AppInit
- KnownDLLs
- Winlogon
- Winsock Providers

Most of the above items are quite familiar to us, but you will probably feel strange for AppInit. The value of AppInit_DLLs is used when certain programs load the DLL window manager (User32.dll). Since all programs that use the graphical interface (not the command line) in Windows load the DLL listed in this value,

AppInit_DLLs are often the target of malware attacks.

Another tab you might encounter is Image Hijacks. This tab involves using Image File Execution options in the Windows registry to redirect the loading process by mapping the executable name and then loading a completely different process.

What can be done with Autoruns

Note that all the entries you see in Autoruns are not necessary programs, but they are programs that are configured to run automatically. To determine if an item is running, you can right-click it and select Process Explorer. Assuming you have Process Explorer installed, open this program so you can see the process properties dialog here. Note that if Process Explorer is running with administrator rights, while you are running Autoruns with standard user rights, this action will fail because Autoruns cannot communicate with Process Explorer.

One of the favorite features here is the 'Jump to' option. If the right click on an entry, you can select 'Jump to' as shown in Figure 2 and the registry editor will display the location of the item.

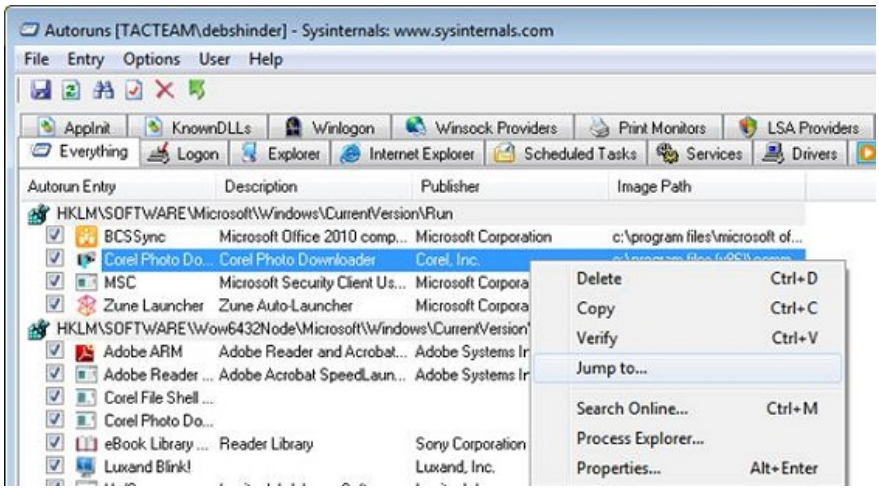

Figure 2

There will definitely be some entries that you do not recognize the name, description, and manufacturer information. You can use the 'Search online' option to perform a search online. This is a way to help you detect whether startup items are related to malicious software.

Another extremely useful feature is found in the File menu. Here you will see an option called 'Compare .'. Using this option requires some caution and you need to use the File | option Save to save an Autoruns file (.ARN extension) before starting to solve the problem. If you do that, you can use the Compare option to mark new entries on the Autoruns list to narrow down the suspicions about malware.

For ease of management, you can select Hide entries that are identified as Microsoft software (the section is in the Options menu). This is not a good idea, though, because malware writers are very easy to label fake software for their software as created by Microsoft. To do so with a specific entry, select Verify from the Entry menu (or press CTRL + V). In addition, you also have the option of Code Signatures Verify in the Options menu.

Another advantage of Autoruns when compared with MSConfig is that it will show you the autostart entries by user. More and more malware is currently exploiting standard user accounts by writing to HKEY_CURRENT_USER. With Autoruns, you can choose the username of the account you want to view from the User menu. This will allow you to find malware in the registry in other user accounts.

Autoruns can even analyze offline systems, support operations for detecting rootkits. You will see this option in the File menu. What you need to do is enter the system root directory which is offline as well as the user profile you want to check. Note that Autorunsc (the command line version of Autoruns) can be used with Sysinternals, psexec tools, to view autostart entries on the remote computer.

Remove Autoruns entries

Another problem is that you need to know some options to remove items found in Autoruns. There are two ways to do that within Autoruns:

- Select the item in the list and click the **Delete** button in the taskbar, or press the **Delete** key on the keyboard. This does not delete the linked files and it does not stop the process if it is running. It only changes the value of the registry, the value that instructs Windows to automatically launch it.
- You can also temporarily remove an item from startup by canceling the check box next to it. When you do this, the program will be removed from the Run key in the registry and stored in the small key 'AutorunsDisabled' so you can reactivate it by checking the checkbox.

Note that in some cases, you may have to restart the process, log out and log back in, or even restart the computer for the changes to take effect.

Conclude

In this second article we will cover only Autoruns, in the next part of this article series, I will show you how to use Process Monitor to track malware actions and how to remove malware from the system. when it is detected as well as what to do if the Sysinternals tool does not help.