Hiding in plain sight | Malwarebytes Labs

By Pieter Arntz

Published: 2013-10-17 · Archived: 2026-04-05 14:29:12 UTC

A lot of programs we install on our computer are automatically run when Windows starts and loads.

While this is not always necessary, there usually is not much harm in this.

But this behavior is also copied by malware writers to pass security checks. Their malicious program try to mimic legitimate programs that you might expect in your Windows startup programs.

Why hide when you can pretend to be something useful?

Copying the art of camouflage from the animal world, malware writers have been trying several methods over the years to hide their registry entries in the open. Sometimes by using (pseudo-)random names and sometimes by using locations that are relatively unknown to the general public. But also by pretending to be, or belong to, legitimate programs.

Arguably there are some 57 ways to make a file get loaded automatically.

The majority of them are found in the registry. Not all of them apply when Windows loads, some get triggered by other events.

Running Internet Explorer for example loads the Browser Helper Objects.

Some of the most well-known and most used startup locations are the Run keys:

HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun

or HKEY_LOCAL_MACHINE SOFTWAREWow6432NodeMicrosoftWindowsCurrentVersionRun

HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun

Together with entries from the Windows startup folder and other possible registry entries these are listed in the Startup database by research engineer Paul Collins aka Pacman.

This database gives you information about the Name of the startup key, the name of the file that gets started, whether the startup is needed, not necessary or even downright malicious. It also has a column where you can find extra information about the files. This can include a link to the site of the manufacturer or a link to a description of the malware.

As you can tell from the screenshot (or if you do a search on the site for yourself) there are a few filenames that are very popular to disguise malware. These are typically entries that are very popular (like skype.exe) or entries that look very much like a legitimate windows filename (i.e., svchost.exe).

If you check your own registry or make a log file with the startup information, a file like skype.exe may jump out at you if you have never installed the program. But if you showed that log to someone else, they might not know if you use the program. That is why experienced and trained log readers pay attention to the folder the file is found in.

Default for the legitimate skype.exe is %ProgramFiles%SkypePhone where %ProgramFiles% is an environmental variable that points to the Program Files directory, usually C:Program Files or C:Program Files (x86).

Any skype.exe located in another folder should be looked at closer. Another important point is the name of the startup. For the legitimate skype.exe (and many fake ones) the name is “Skype”, but there are others, like the malware shown in the example that uses “Skype Update”. That may have been an attempt to make it look less conspicuous if the real Skype is present as well.

If you need to know more about Windows startup programs and especially how to identify them then we recommend you visit Pacman’s Portal – which is powered by Malwarebytes.

Thank you, Paul Collins, for your input.

About the author

Was a Microsoft MVP in consumer security for 12 years running. Can speak four languages. Smells of rich mahogany and leather-bound books.
