How Malware hides and is installed as a Service

By Lawrence Abrams

Archived: 2026-04-05 21:52:38 UTC

Table of Contents

Introduction

A common misconception when working on removing malware from a computer is that the only place an infection will start from is in one of the entries enumerated by HijackThis. For the most part these entries are the most common, but it is not always the case. Lately there are more infections installing a part of themselves as a service. Some examples are Ssearch.biz and Home Search Assistant.

When cleaning a computer the standard approach is to clean up the Run entries and the other more common startup entries first. For the most part, that will be enough to remove the infection. The problem arises when the log looks clean and yet there are still problems. One place to continue looking for the infection is in the operating system's services to see if there is a service that does not belong there and could possibly be loading the infection. A service is a program that is automatically started by Windows NT/XP/2000/2003 on startup or through some other means and is generally used for programs that run in the background.

Please note, in order to properly use the instructions below you must either run the programs with Administrator privileges.

Service Configuration

A service is loaded on startup by either using svchost.exe or by windows directly launching the application. If a service is loaded directly by windows, the associated file name that launches the service can be found in the ImagePath value under the following registry entry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*servicename*

When the service is being launched by svchost.exe, it will be placed in a particular service group, which is then launched by svchost.exe. A listing of these groups and the services that are launched under them can be found here:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost

Under this key you will find various groups (netsvcs, LocalServices, etc) in which each contain multiple services that will be launched when the group is loaded by svchost.exe. These groups are loaded by the following command:

svchost.exe -k netsvcs

It will load all the services found under the netsvcs group in the above key and appear as one process under the process list. So each time a new group is loaded by svchost.exe, you will find a new svchost.exe process listed in memory. It is for this reason why there are multiple svchost.exe processes listed on a machine. If you are using Windows XP, as this command is not available on Windows 2000, you can see what services each svchost.exe process is controlling by running the following command from a command prompt: **tasklist /SVC**

When a service is launched in this way, the actual filename for the service can be found here:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*servicename*\Parameters\\ServiceDll

The value of ServiceDLL is the actual service file that we want to be concerned with.

Listing and Analyzing the services

To get a report of configured services on your computer, I put together a simple batch file that uses Bobbi Flekman's swsc program program to get a list of the services and open a notepad. Nothing fancy, but saves time when diagnosing.

This file can be found here: Getservices.zip

To use the script, you simply unzip the file to your C: drive and you will now find a directory called c:\getservice. Inside that directory is a batch file called getservice.bat and the psservice.exe file. Simply double-click on the getservice.bat file and it will create a notepad containing a list of services installed on the computer you are running it on. **Note: You must be running as a user with Administrator privileges or this script will either not work or not give enough information.**

The output of the script will contain information about each service installed on your computer. The important information to look at in the service entries are::

SERVICE_NAME	This is the name the service goes by and is what it is stored in the registry under.
BINARY_PATH_NAME	This is the actual file that is being used to launch the service.
DISPLAY_NAME	This is the name the service appears under in the services.msc in the control panel.

START_TYPE	This tells you if the service is disabled, manually started, or automatically started.

Below are examples of how an entry would look for two different types of infections explanations of how to interpret the information given:

```
SERVICE_NAME: O?'Å½rtñåÈ²$Ó
(null)
TYPE : 20 WIN32_SHARE_PROCESS
START_TYPE : 2 AUTO_START
ERROR_CONTROL : 0 IGNORE
BINARY_PATH_NAME : C:\WINDOWS\system32\d3xi.exe /s
LOAD_ORDER_GROUP :
TAG : 0
DISPLAY_NAME : Remote Procedure Call (RPC) Helper
DEPENDENCIES :
SERVICE_START_NAME: LocalSystem
```

Home Search Assistant Example

The Home Search Assistant uses a service, among standard Run entries, as part of its infection. The important attributes we can gather from the above information are as follow:

1. It's display name in the Services control panel is Remote Procedure Call (RPC) Helper
2. It has a service name of O?'Å½rtñåÈ²$i in the registry.
3. It is started automatically on boot up
4. The file that starts this service is C:\WINDOWS\system32\d3xi.exe

Armed with this information we now know what registry entries the service is stored in and the file that is being used as part of the Home Search Assistant infection.

The next example is for the Ssearch.biz hijacker, but it is loaded in a slightly different way, causing us to work a little more in finding out what the infection file is.

```
SERVICE_NAME: pnpsvc
Provides plug and play svc devices support
TYPE : 120 WIN32_SHARE_PROCESS INTERACTIVE_PROCESS
START_TYPE : 2 AUTO_START
ERROR_CONTROL : 1 NORMAL
BINARY_PATH_NAME : C:\WINNT\system32\svchost.exe -k netsvcs
LOAD_ORDER_GROUP :
TAG : 0
DISPLAY_NAME : Plug and Play svc service
```

DEPENDENCIES : SERVICE_START_NAME: LocalSystem
SSearch.biz Example

The SSearch.biz hijacker uses a service as part of its infection as well. The important attributes we can gather from the above information are as follow:

1. It's display name in the Services control panel is Plug and Play svc service
2. It has a service name of pnpsvc in the registry
3. It is started automatically on boot up
4. The file that starts this service is C:\WINNT\system32\svchost.exe -k netsvcs

Now this information, though helpful, is somewhat useless without digging around further in the registry. We know that the file that starts the service is svchost.exe, but that is a legitimate program, so we do not want to delete it. How then can we find the appropriate file to remove? Remember what we discussed above about how svchost.exe works?

From the BINARY_PATH_NAME we know that the file is part of the netsvcs group. That means that when svchost loads that group, which may contain many services, it will also load the file associated with this service. To find the actual file name for this particular service, we need to check the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pnpsvc\Parameters\\ServiceDll

The value of the ServiceDLL key is the actual file that we want to get rid of.

In the next section we will discuss how to remove the service via deleting entries in the registry.

Removing a service

Removing a service manually requires removing entries from the registry. This can be a dangerous task for the health of your computer. If you do not feel comfortable doing this, then please ask someone else to help with this step of the cleanup procedure as making a mistake can cause the computer you are working on to not work properly.

Service entries are stored in the registry under a section called ControlSet. A ControlSet are located under the following key:

HKEY_LOCAL_MACHINE\SYSTEM

A ControlSet is a complete copy of the configuration that is used to successfully launch services and other critical files & drivers for Windows. When you look under the above key there will always be at least two ControlSets and one CurrentControlSet. For the sake of this tutorial I will use what I have on my machine, which is ControlSet1 and ControlSet2 (there may be more up to a maximum of 4). One of these numbered control sets refers to the default configuration that is used when the computers normally boots. The other numbered control set

refers to the one used when you choose to boot up using the Last Known Good Configuration. The last one, CurrentControlSet, is an exact mirror of the ControlSet we had used to boot into Windows, so that if you make a change CurrentControlSet it will automatically appear in the ControlSet it is mirroring and vice-versa.

If you wanted to know for sure which ControlSet the CurrentControlSet is pointing to you can examine the following key:

HKEY_LOCAL_MACHINE\SYSTEM\Select

This key gives us important information as to which ControlSet was used on the last boot, which is used by default, and which is designated for LastKnownGoodConfiguration. This key contains the following values:

Current	This will contain the number of the ControlSet that we are currently using and which CurrentControlSet points to.
Default	This will contain the number of the ControlSet that Windows uses by default when booting.
Failed	This will indicate with ControlSet was the one that failed on last boot. If it is 0, then there was no failures.
LastKnownGood	This will contain the number of the ControlSet that Windows uses when we choose the Last Known Good Configuration

If we wanted to manually remove a service from the registry we would only need to remove it from the numbered ControlSets (remember CurrentControlSet is a mirror of one of the numbered ones). For example, to remove the service for a SSearch.biz hijacker on my computer, we would simply delete from the registry the following entries:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\pnpsvc
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\pnpsvc

Once we reboot, these services will no longer be listed in the Services control panel.

At times though, the malware will also install itself under these keys:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Enum\Root

as subkeys called **LEGACY_*svcname.*** These **LEGACY_*svcname*** entries should be deleted as well, but will usually require you to change the permissions on them in order to delete them. Simply change the security permissions on these keys to Everyone (Full) and then delete them.

Conclusion

Knowing how to diagnose a service running as a malware is an important part of fighting spyware. As more and more spyware and viruses use this technique , the understanding of how services work and are configured in the Registry will make the difference between fixing a computer and not fixing it.

As always if you have any comments, questions or suggestions about this tutorial please do not hesitate to tell us in the forums.

For expert malware removal assistance, you can ask for help at our Virus, Trojan, Spyware, and Malware Removal Logs.

--

Lawrence Abrams
Bleeping Computer Advanced Spyware Removal Tutorial
BleepingComputer.com: Computer Support & Tutorials for the beginning computer user.
