Table of Contents

Watch the Windows XP SVCHOST companion video here!
Watch the Windows Vista and Windows 7 SVCHOST companion video here!

Introduction

A very common question we see here at Bleeping Computer involves people concerned that there are too many SVCHOST.EXE processes running on their computer. The confusion typically stems from a lack of knowledge about SVCHOST.EXE, its purpose, and Windows services in general. This tutorial will clear up this confusion and provide information as to what these processes are and how to find out more information about them. Before we continue learning about SVCHOST, lets get a small primer on Windows services.

Services are Windows programs that start when Windows loads and that continue to run in the background without interaction from the user. For those familiar with Unix/Linux operating systems, Windows services are similar to *nix daemons. For the most part Windows services are executable (.EXE) files, but some services are DLL files as well. As Windows has no direct way of executing a DLL file it needs a program that can act as a launcher for these types of programs. In this situation, the launcher for DLL services is SVCHOST.EXE, otherwise known as the **Generic Host Process for Win32 Services**. Each time you see a SVCHOST process, it is actually a process that is managing one or more distinct Windows DLL services.

Outlined below are three methods, depending on your Windows version, to see what services a SVCHOST.EXE process is controlling on your computer as well as some advanced technical knowledge about svchost for those who are interested.

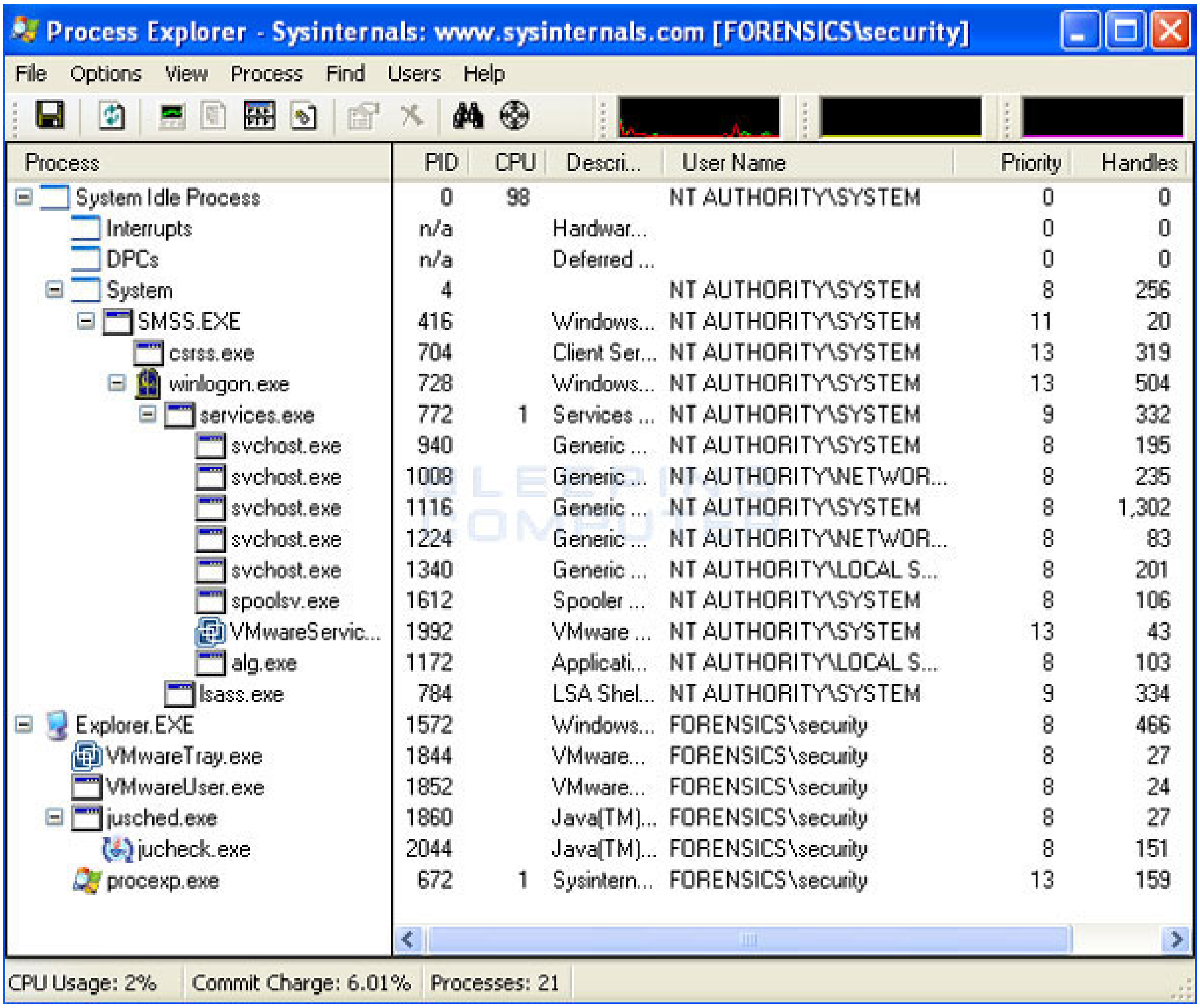
Determining the services running under a SVCHOST.EXE process using Process Explorer

Process Explorer, from Sysinternals, is a process management program that allows you to see the running processes on your computer and a great deal of information about each process. One of the nice features of Process Explorer is that it also gives you the ability to see what services a particular SVCHOST.EXE process is controlling.

First you need to download Process Explorer from the following site:

Process Explorer

Download the file and save it to your hard drive. When it has finished downloading, extract the file into its own folder and double-click on the **procexp.exe** to start the program. If this is your first time running the program, it will display a license agreement. Agree to the license agreement and the program will continue. When it is finished loading you will be presented with a screen containing all the running processes on your computer as shown in the figure below. Remember that the processes you see in this image will not be the same as what is running on your computer.

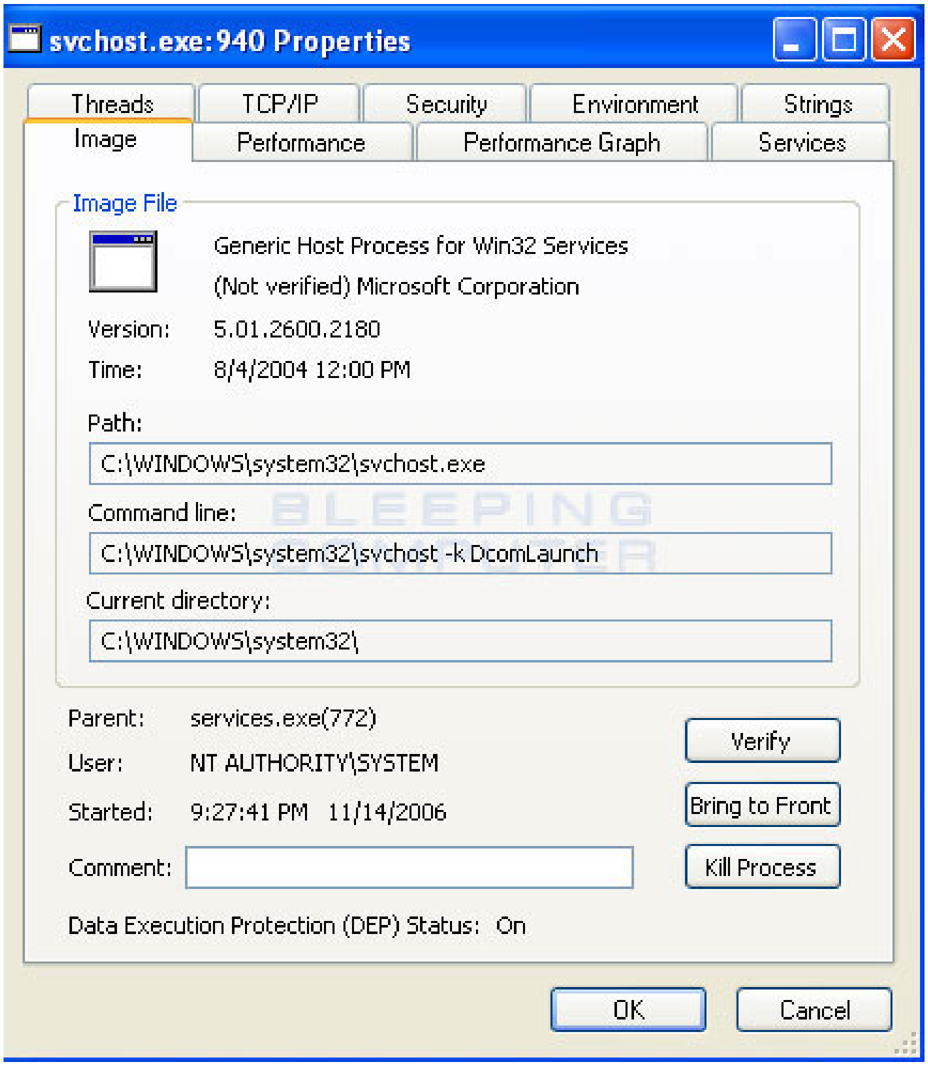

Process Explorer - Sysinternals: www.sysinternals.com [FORENSICS\security]
File
Options
View
Process
Find
Users
Help

Process	PID	CPU	Descri...	User Name	Priority	Handles
System Idle Process	0	98		NT AUTHORITY\SYSTEM	0	0
Interrupts	n/a		Hardwar...		0	0
DPCs	n/a		Deferred ...		0	0
System	4			NT AUTHORITY\SYSTEM	8	256
SMSS.EXE	416		Windows...	NT AUTHORITY\SYSTEM	11	20
csrss.exe	704		Client Ser...	NT AUTHORITY\SYSTEM	13	319
winlogon.exe	728		Windows...	NT AUTHORITY\SYSTEM	13	504
services.exe	772	1	Services ...	NT AUTHORITY\SYSTEM	9	332
svchost.exe	940		Generic ...	NT AUTHORITY\SYSTEM	8	195
svchost.exe	1008		Generic ...	NT AUTHORITY\NETWOR...	8	235
svchost.exe	1116		Generic ...	NT AUTHORITY\SYSTEM	8	1,302
svchost.exe	1224		Generic ...	NT AUTHORITY\NETWOR...	8	83
svchost.exe	1340		Generic ...	NT AUTHORITY\LOCAL S...	8	201
spoolsv.exe	1612		Spooler ...	NT AUTHORITY\SYSTEM	8	106
VMwareServic...	1992		VMware ...	NT AUTHORITY\SYSTEM	13	43
alg.exe	1172		Applicati...	NT AUTHORITY\LOCAL S...	8	103
lsass.exe	784		LSA Shel...	NT AUTHORITY\SYSTEM	9	334
Explorer.EXE	1572		Windows...	FORENSICS\security	8	466
VMwareTray.exe	1844		VMware...	FORENSICS\security	8	27
VMwareUser.exe	1852		VMware...	FORENSICS\security	8	24
jusched.exe	1860		Java(TM)...	FORENSICS\security	8	27
jucheck.exe	2044		Java(TM)...	FORENSICS\security	8	151
procexp.exe	672	1	Sysintern...	FORENSICS\security	13	159

CPU Usage: 2% Commit Charge: 6.01% Processes: 21

Process Explorer Screen

Scroll through the list of processes until you see the SVCHOST.EXE process(es). To find out which services are running within a particular SVCHOST.EXE process we need to examine the properties for the process. To do this double-click SVCHOST.EXE entry in Process Explorer and you will see the properties screen for the process like in the image below.



Generic Host Process for Win32 Services

(Not verified) Microsoft Corporation

Version: 5.01.2600.2180

Time: 8/4/2004 12:00 PM

Path: C:\WINDOWS\system32\svchost.exe

Command line: C:\WINDOWS\system32\svchost -k DcomLaunch

Current directory: C:\WINDOWS\system32\

Parent: services.exe(772)

User: NT AUTHORITY\SYSTEM

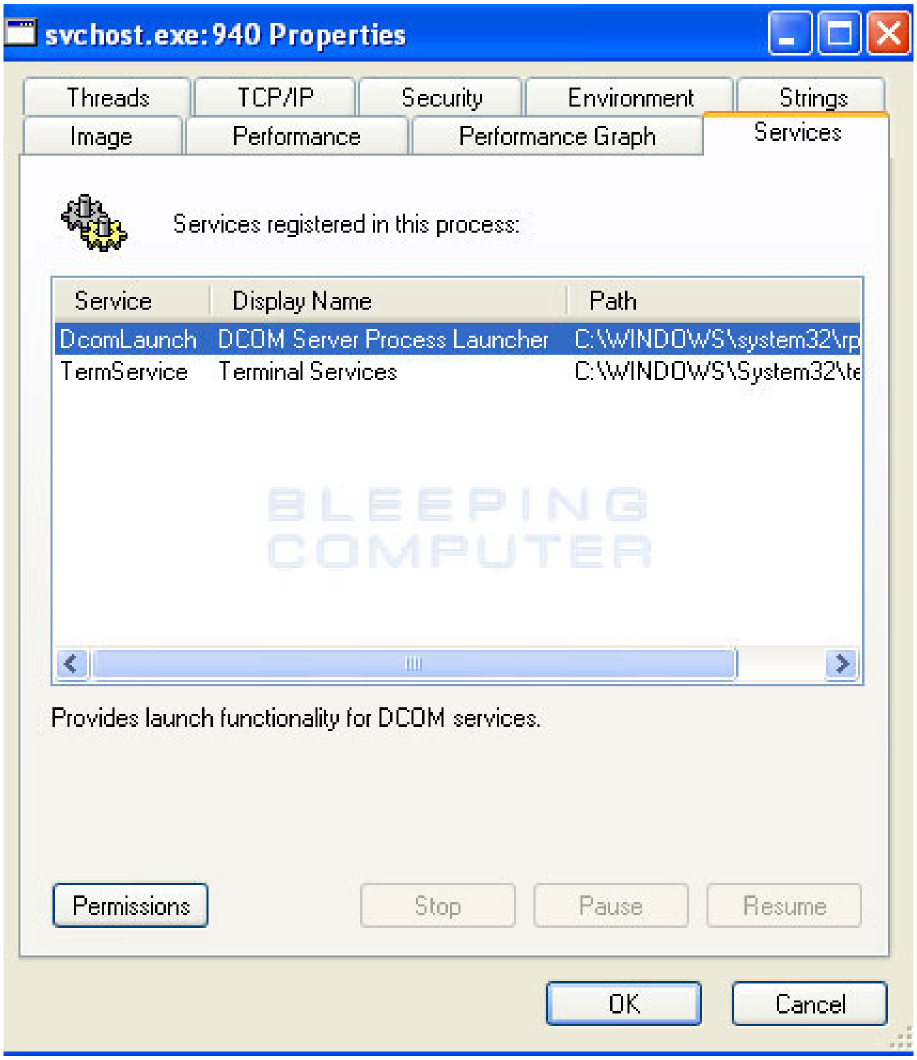
Started: 9:27:41 PM 11/14/2006

Comment:

Data Execution Protection (DEP) Status: On

SVCHOST.EXE Properties

Finally, to view the services running in this process, click on the **Services** tab. You will now see a screen similar to the one below.



Services registered in this process:

Service	Display Name	Path
DcomLaunch	DCOM Server Process Launcher	C:\WINDOWS\system32\rp
TermService	Terminal Services	C:\WINDOWS\System32\te

Provides launch functionality for DCOM services.

Services Tab

This window displays the services that are being managed by this particular SVCHOST.EXE process. As you can see the SVCHOST.EXE that we are currently looking at in this tutorial is managing the DCOM Server Process Launcher and Terminal Services.

Using this method you can determine what services a SVCHOST.EXE process is controlling on your computer.

Determining the services running under a SVCHOST.EXE process using Task List

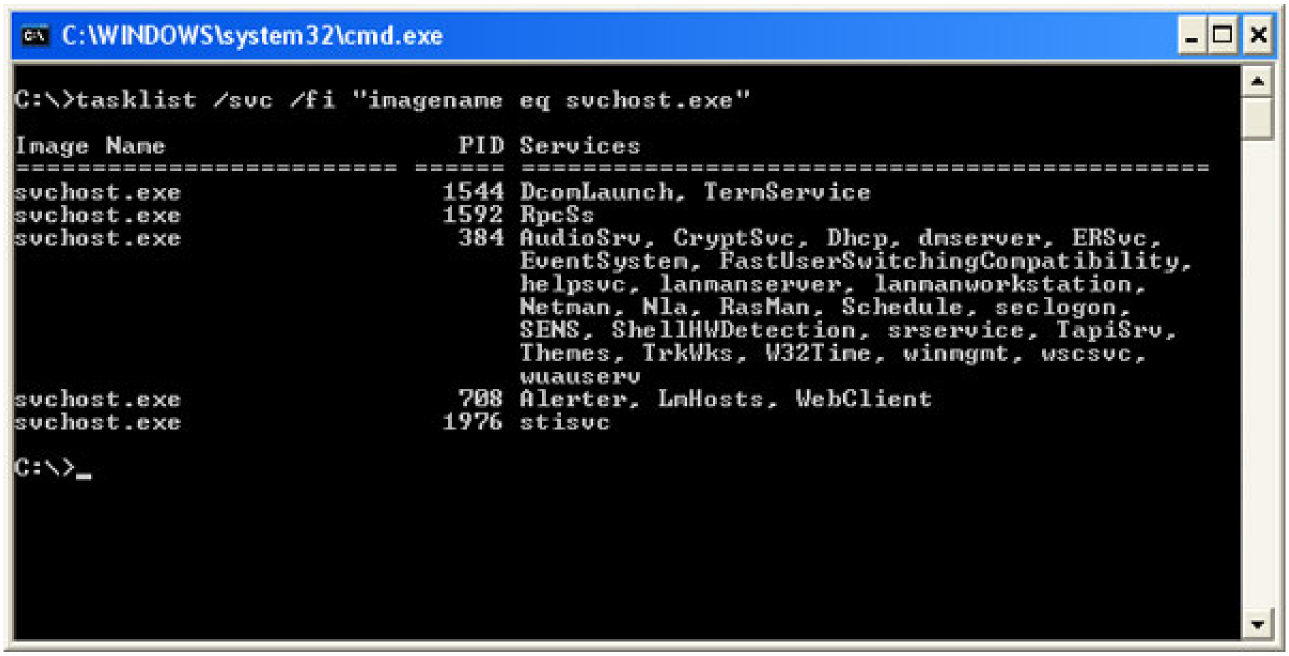
For those who like to tinker around in a Windows command prompt/console window, and have Windows XP Pro or Windows 2003, there is a Windows program called tasklist.exe that can be used to list the running processes, and services, on your computer. To use task list to see the services that a particular SVCHOST.EXE process is loading, just follow these steps:

1. Click on the **Start** button and then click on the **Run** menu command.

2. In the Open: field type **cmd** and press **enter**.

3. You will now be presented with a console window. At the command prompt type **tasklist /svc /fi "imagename eq svchost.exe"** and press the **enter** key. You will see a list of the processes on your

computer as well as the services that a SVCHOST.EXE process is managing. This can be seen in the image below.



```
C:\>tasklist /svc /fi "imagename eq svchost.exe"

Image Name                   PID Services
========================= ====== =============================================
svchost.exe                 1544 DcomLaunch, TermService
svchost.exe                 1592 RpcSs
svchost.exe                  384 AudioSrv, CryptSvc, Dhcp, dmserver, ERSvc,
                                 EventSystem, FastUserSwitchingCompatibility,
                                 helpsvc, lanmanserver, lanmanworkstation,
                                 Netman, Nla, RasMan, Schedule, seclogon,
                                 SENS, ShellHWDetection, srservice, TapiSrv,
                                 Themes, TrkWks, W32Time, winmgmt, wscsvc,
                                 wuauserv
svchost.exe                  708 Alerter, LmHosts, WebClient
svchost.exe                 1976 stisvc

C:\>_
```

TaskList /svc output

When you are done examining the output, you can type **exit** and press the **enter** key to close the console window.

Determining the services running under a SVCHOST.EXE process in Windows Vista and Windows 7

Windows Vista and Windows 7 have enhanced their Windows Task Manager and one of its features allows us to easily see what services are being controlled by a particular SVCHOST.EXE process. To start, simply start the task manager by right clicking on the task bar and then selecting Task Manager. When Task Manager opens click on the **Processes** tab. You will now be presented with a list of processes that your user account has started as shown in the image below.

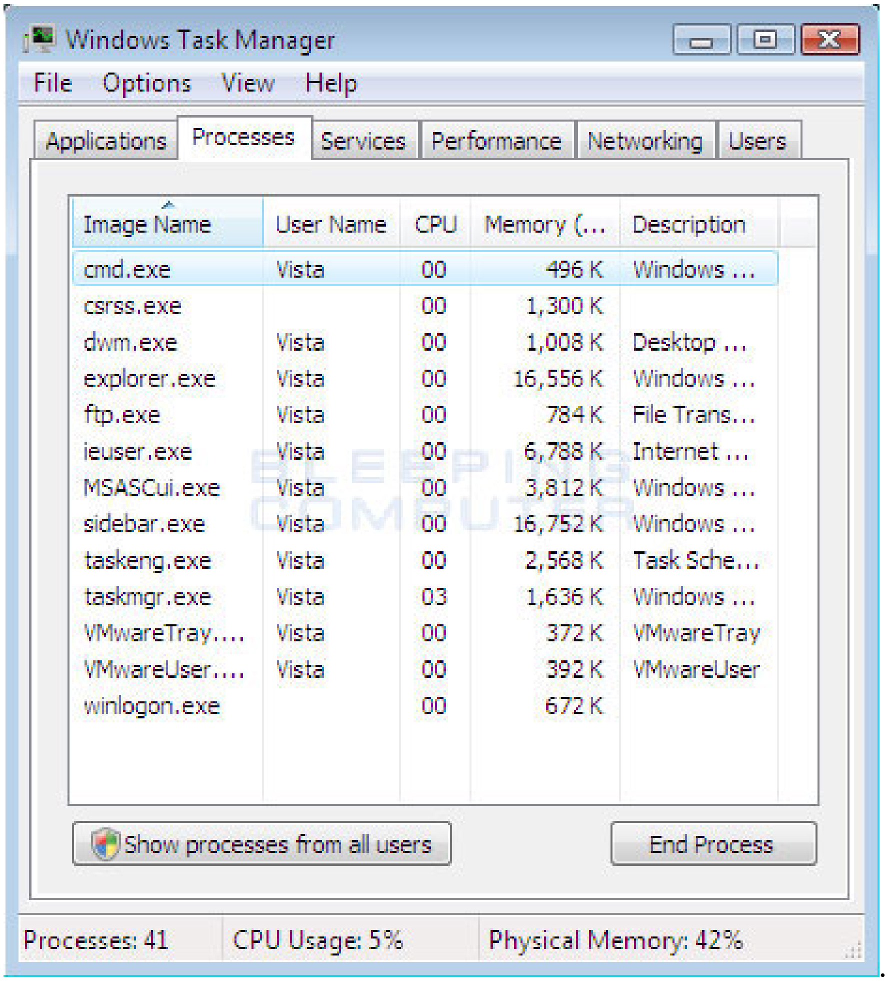
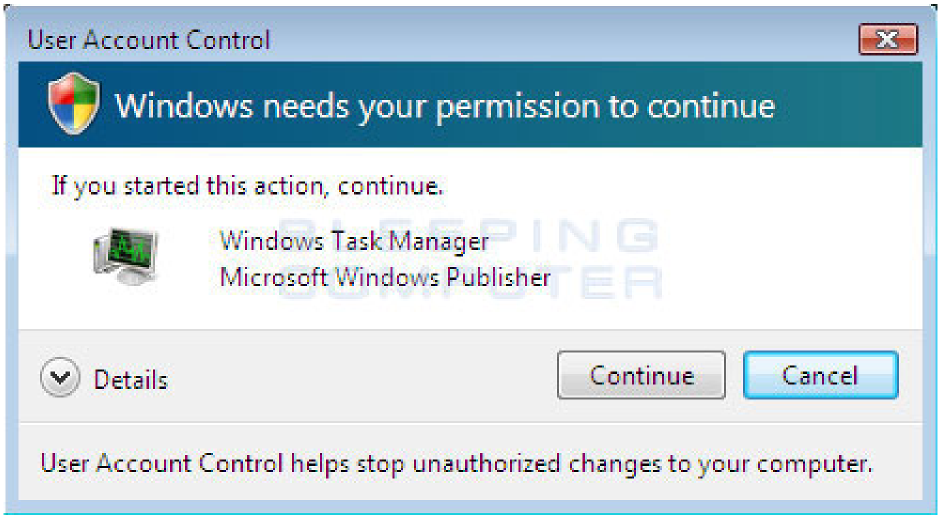


Image Name	User Name	CPU	Memory (...	Description
cmd.exe	Vista	00	496 K	Windows ...
csrss.exe		00	1,300 K	
dwm.exe	Vista	00	1,008 K	Desktop ...
explorer.exe	Vista	00	16,556 K	Windows ...
ftp.exe	Vista	00	784 K	File Trans...
ieuser.exe	Vista	00	6,788 K	Internet ...
MSASCui.exe	Vista	00	3,812 K	Windows ...
sidebar.exe	Vista	00	16,752 K	Windows ...
taskeng.exe	Vista	00	2,568 K	Task Sche...
taskmgr.exe	Vista	03	1,636 K	Windows ...
VMwareTray....	Vista	00	372 K	VMwareTray
VMwareUser....	Vista	00	392 K	VMwareUser
winlogon.exe		00	672 K	

Processes: 41 CPU Usage: 5% Physical Memory: 42%

Windows 7's Current User Processes

We, though, need to see **all** of the processes running on the computer. To do this click on the button labeled **Show All Processes**. When you do this, Windows may prompt you to allow authorization to see all the processes as shown below.



Windows needs your permission to continue

If you started this action, continue.

Windows Task Manager
Microsoft Windows Publisher

User Account Control helps stop unauthorized changes to your computer.

Show all Processes Confirmation

Press the **Continue** button and the Task Manager will reload, but this time showing all the processes running in the operating system. Scroll down through the list of processes until you see the SVCHOST processes as shown in the image below.

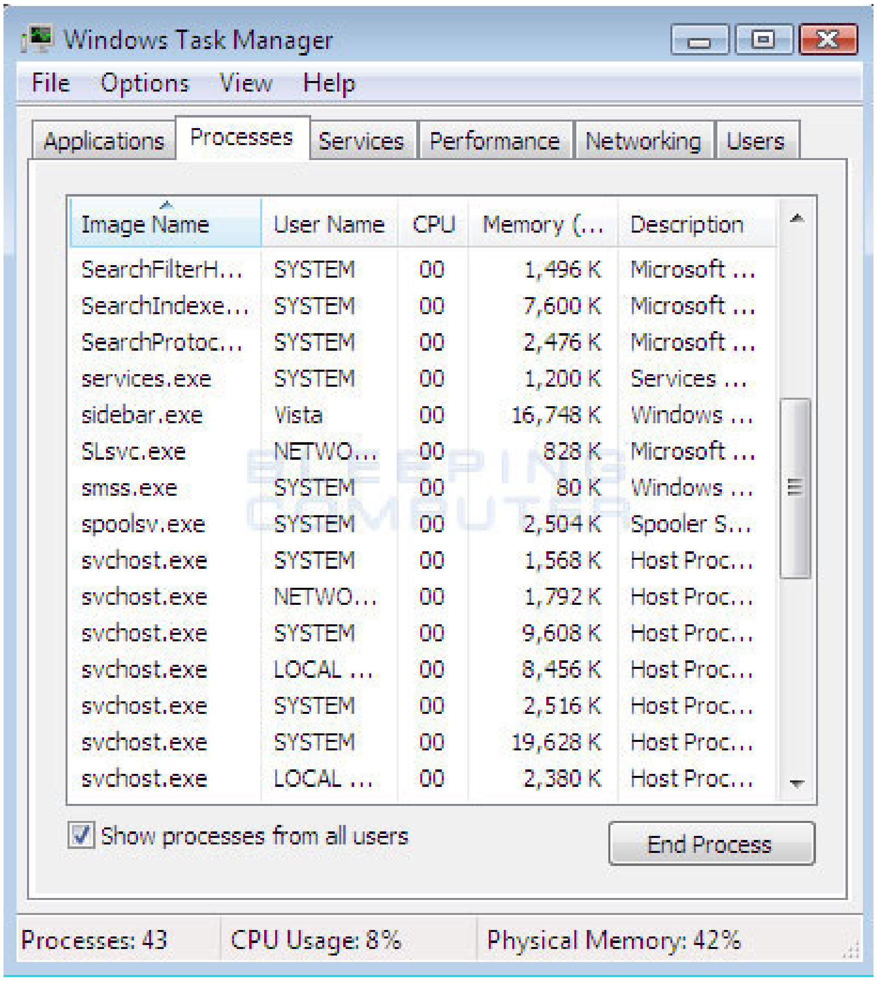

Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
End Process

Image Name	User Name	CPU	Memory (...	Description
SearchFilterH...	SYSTEM	00	1,496 K	Microsoft ...
SearchIndexe...	SYSTEM	00	7,600 K	Microsoft ...
SearchProtoc...	SYSTEM	00	2,476 K	Microsoft ...
services.exe	SYSTEM	00	1,200 K	Services ...
sidebar.exe	Vista	00	16,748 K	Windows ...
SLsvc.exe	NETWO...	00	828 K	Microsoft ...
smss.exe	SYSTEM	00	80 K	Windows ...
spoolsv.exe	SYSTEM	00	2,504 K	Spooler S...
svchost.exe	SYSTEM	00	1,568 K	Host Proc...
svchost.exe	NETWO...	00	1,792 K	Host Proc...
svchost.exe	SYSTEM	00	9,608 K	Host Proc...
svchost.exe	LOCAL ...	00	8,456 K	Host Proc...
svchost.exe	SYSTEM	00	2,516 K	Host Proc...
svchost.exe	SYSTEM	00	19,628 K	Host Proc...
svchost.exe	LOCAL ...	00	2,380 K	Host Proc...

☑ Show processes from all users

Processes: 43 CPU Usage: 8% Physical Memory: 42%

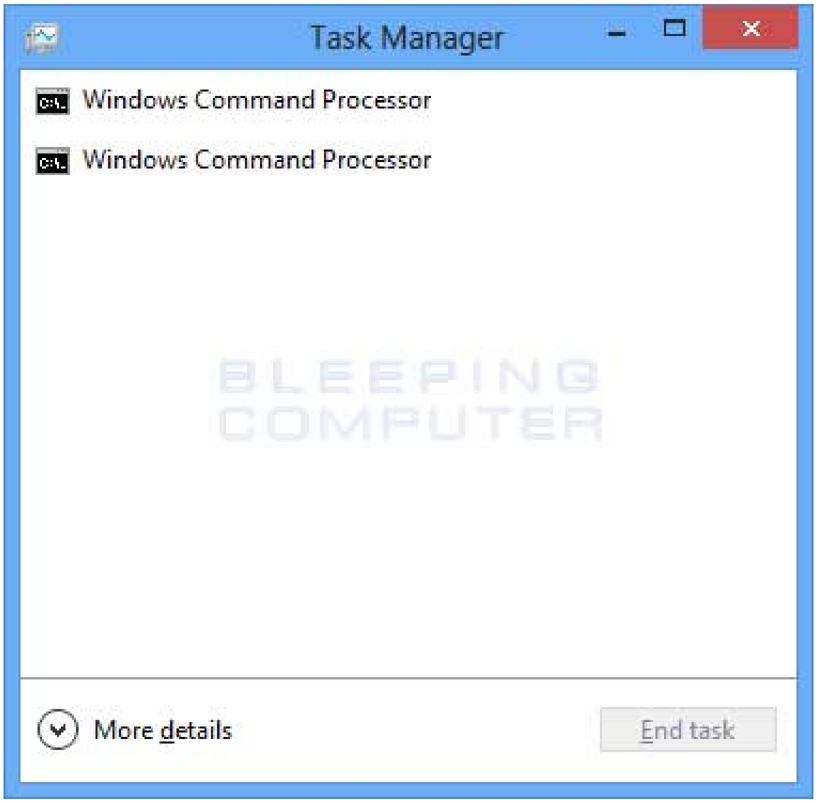
All Windows 7 Processes

Right-click on a SVCHOST process and select the **Go to Service(s)** menu option. You will now see a list of services on your computer with the services that are running under this particular SVCHOST process highlighted. Now you can easily determine what services a particular SVCHOST process is running in Windows Vista or Windows 7.

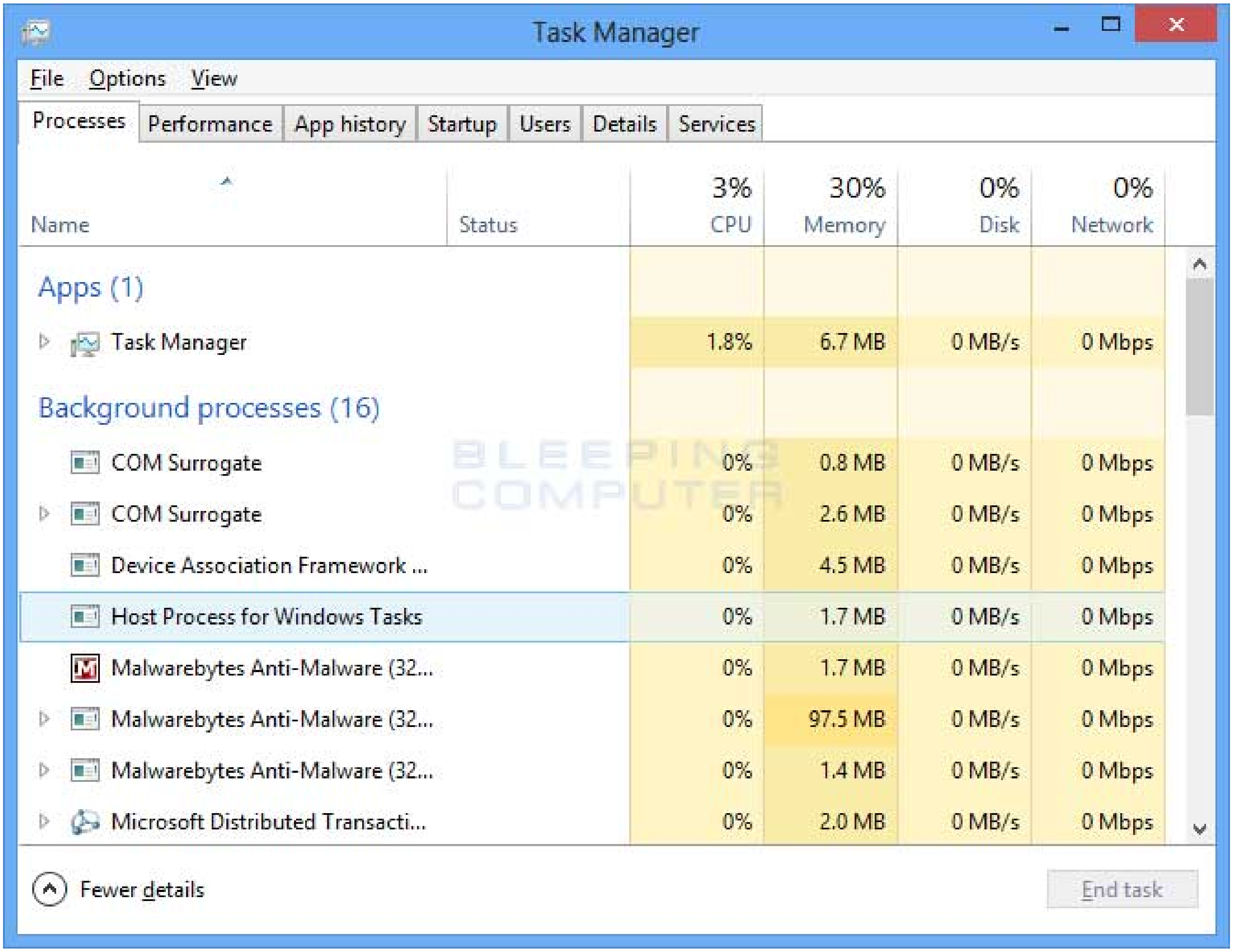
Determining the services running under a SVCHOST.EXE process in Windows 8

The Windows 8 Task Manager makes it much easier to find what services are running under a particular SVCHOST.exe instance. To access the Task Manager, type **Task Manager** from the Windows 8 Start Screen and then click on the **Task Manager** option when it appears in the search results. This will open the basic Task Manager as shown in the screenshot below.

Tip: You can also use the **Ctrl**+**Shift**+**Esc** keyboard combination to automatically open the Task Manager from any screen in Windows.

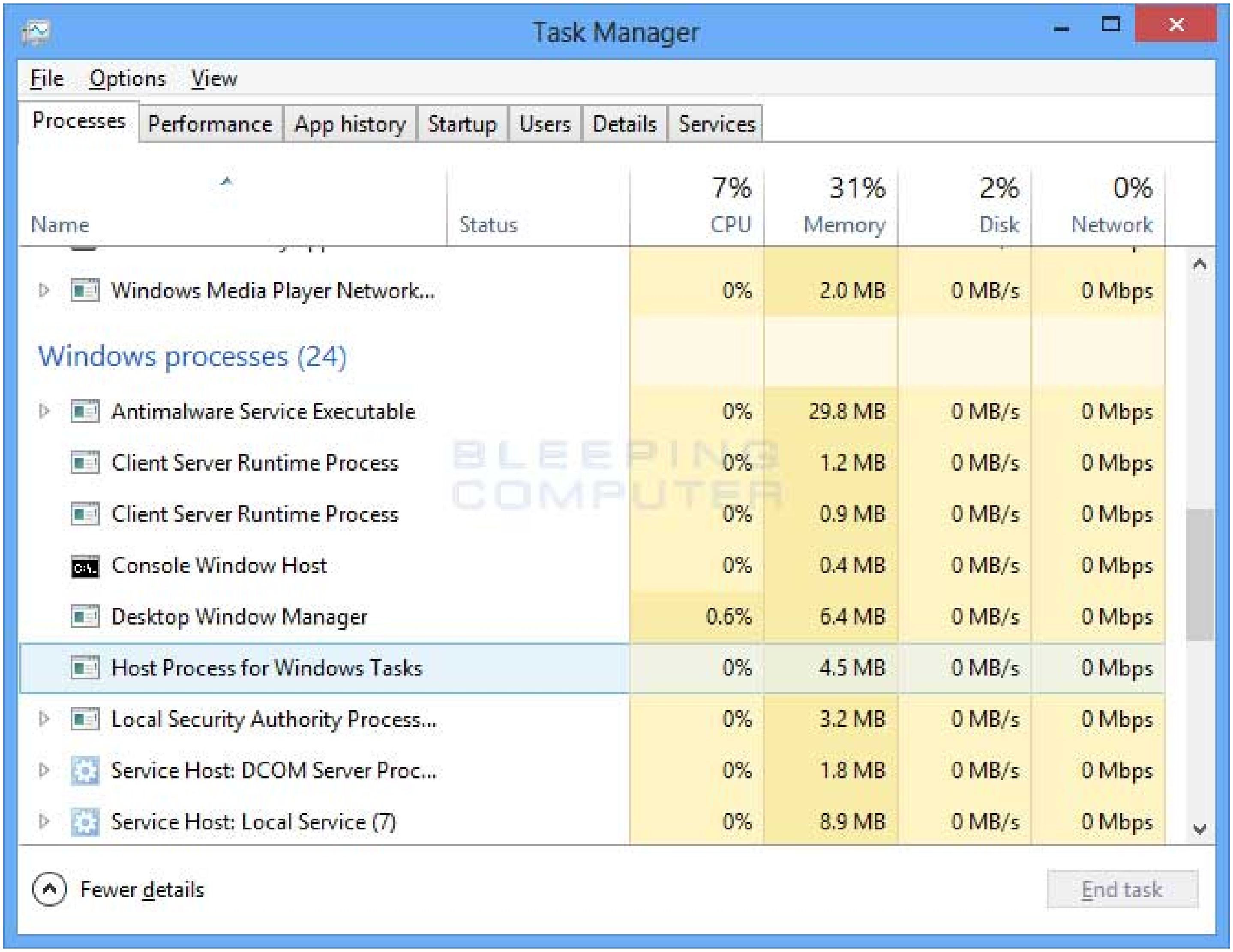


To see the list of processes, click on the **More details** option.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

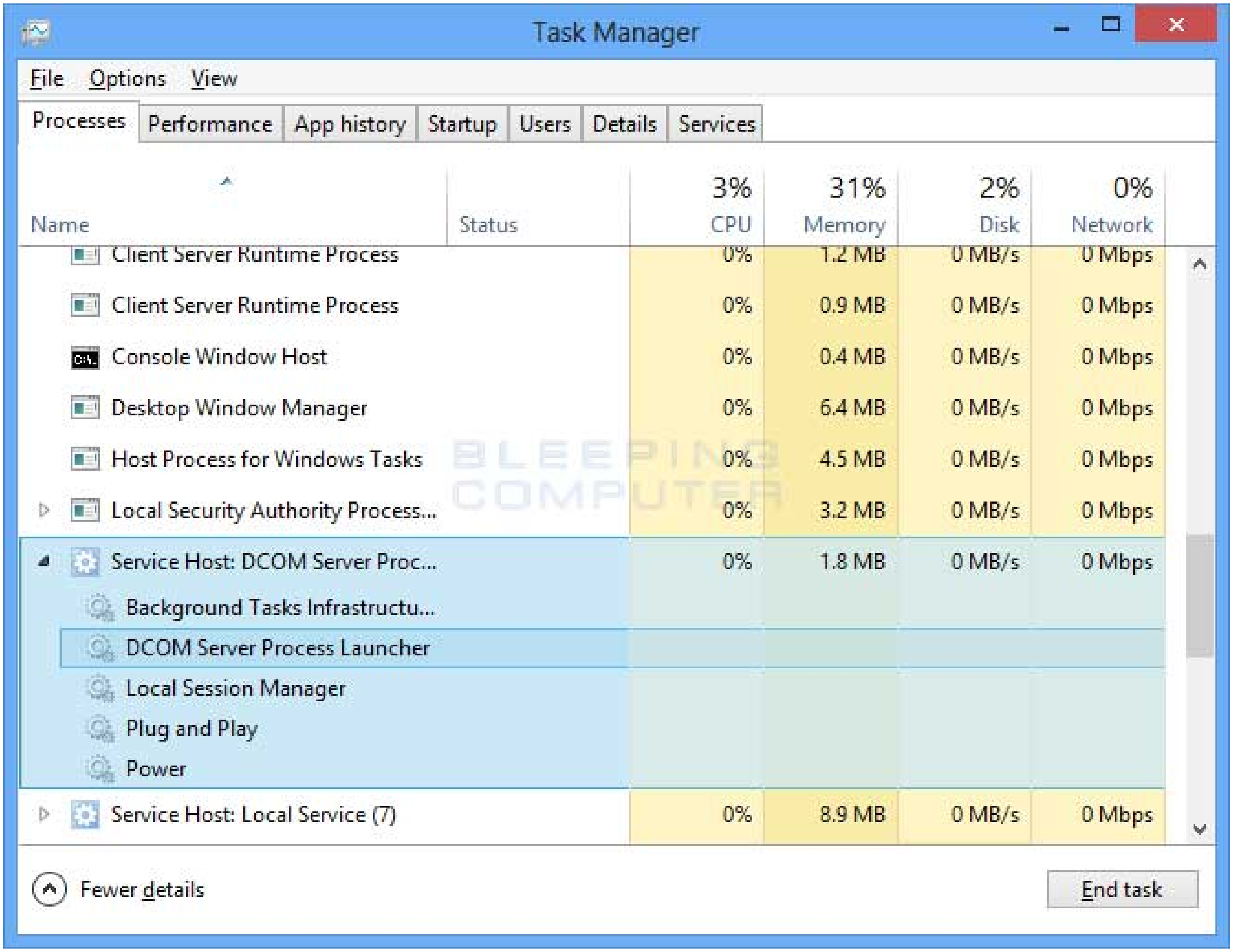
Name	Status	3% CPU	30% Memory	0% Disk	0% Network
Apps (1)					
Task Manager		1.8%	6.7 MB	0 MB/s	0 Mbps
Background processes (16)					
COM Surrogate		0%	0.8 MB	0 MB/s	0 Mbps
COM Surrogate		0%	2.6 MB	0 MB/s	0 Mbps
Device Association Framework ...		0%	4.5 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	1.7 MB	0 MB/s	0 Mbps
Malwarebytes Anti-Malware (32...		0%	1.7 MB	0 MB/s	0 Mbps
Malwarebytes Anti-Malware (32...		0%	97.5 MB	0 MB/s	0 Mbps
Malwarebytes Anti-Malware (32...		0%	1.4 MB	0 MB/s	0 Mbps
Microsoft Distributed Transacti...		0%	2.0 MB	0 MB/s	0 Mbps

Scroll down until you see the Windows Processes category and look for the **Service Host** entries as shown in the image below.



		7%	31%	2%	0%
Name	Status	CPU	Memory	Disk	Network
Windows Media Player Network...		0%	2.0 MB	0 MB/s	0 Mbps
Windows processes (24)					
Antimalware Service Executable		0%	29.8 MB	0 MB/s	0 Mbps
Client Server Runtime Process		0%	1.2 MB	0 MB/s	0 Mbps
Client Server Runtime Process		0%	0.9 MB	0 MB/s	0 Mbps
Console Window Host		0%	0.4 MB	0 MB/s	0 Mbps
Desktop Window Manager		0.6%	6.4 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	4.5 MB	0 MB/s	0 Mbps
Local Security Authority Process...		0%	3.2 MB	0 MB/s	0 Mbps
Service Host: DCOM Server Proc...		0%	1.8 MB	0 MB/s	0 Mbps
Service Host: Local Service (7)		0%	8.9 MB	0 MB/s	0 Mbps

Next to each Service Host row process will be a little arrow. Click on this arrow to expand that particular Service Host entry to see what services are running under it.



Name	Status	3% CPU	31% Memory	2% Disk	0% Network
Client Server Runtime Process		0%	1.2 MB	0 MB/s	0 Mbps
Client Server Runtime Process		0%	0.9 MB	0 MB/s	0 Mbps
Console Window Host		0%	0.4 MB	0 MB/s	0 Mbps
Desktop Window Manager		0%	6.4 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	4.5 MB	0 MB/s	0 Mbps
Local Security Authority Process...		0%	3.2 MB	0 MB/s	0 Mbps
Service Host: DCOM Server Proc...		0%	1.8 MB	0 MB/s	0 Mbps
Background Tasks Infrastructu...					
DCOM Server Process Launcher					
Local Session Manager					
Plug and Play					
Power					
Service Host: Local Service (7)		0%	8.9 MB	0 MB/s	0 Mbps

Under the expanded Service Host, you will now see the list of services that is running under it. This allows you to easily determine what services a particular SVCHOST process is managing in Windows 8.

Advanced Information about SVCHOST.EXE

Now that we know that a single SVCHOST.EXE process can load and manage multiple services, what determines what services are grouped together under a SVCHOST instance? These groups are determined by the settings in the following Windows Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SVCHOST

Under this key are a set of values that group various services together under one name. Each group is a REG_MULTI_SZ Registry value that contains a list of service names that belong to that group. Below you will see standard groups found in XP Pro.

Group Name	Services in the group
	Alerter, WebClient, LmHosts, RemoteRegistry,

LocalService	upnphost, SSDPSRV
NetworkService	DnsCache
netsvcs	6to4, AppMgmt, AudioSrv, Browser, CryptSvc, DMServer, DHCP, ERSvc, EventSystem, FastUserSwitchingCompatibility, HidServ, Ias, Iprip, Irmon, LanmanServer, LanmanWorkstation, Messenger, Netman, Nla, Ntmssvc, NWCWorkstation, Nwsapagent, Rasauto, Rasman, Remoteaccess, Schedule, Seclogon, SENS, Sharedaccess, SRService, Tapisrv, Themes, TrkWks, W32Time, WZCSVC, Wmi, WmdmPmSp, winmgmt, TermService, wuauserv, BITS, ShellHWDetection, helpsvc, xmlprov, wscsvc, WmdmPmSN
rpcss	RpcSs
imgsvc	StiSvc
termsvcs	TermService
HTTPFilter	HTTPFilter
DcomLaunch	DcomLaunch, TermService

Each of the service names in these groups corresponds to a service entry under the Windows Registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Under each of these service entries there is a **Parameters** subkey that contains a **ServiceDLL** value which corresponds to the DLL that is used to run the service.

When Windows loads it begins to start services that are set to enabled and have an automatic startup. Some services are started using the SVCHOST.exe command. When Windows attempts to start one of these types of services and there is currently not a svchost instance running for that services group, it will create a new SVCHOST instance and then load the DLL associated with the service. If on the other hand, there is already a SVCHOST process running for that group it will just load the new service using that existing process. A service that uses SVCHOST to initialize itself, provides the name of the group as a parameter to svchost.exe command. An example would be:

C:\WINDOWS\system32\svchost.exe -k DcomLaunch

In the above command line, the svchost process will look up the ServiceDLL associated with the service name from the DcomLaunch group and load it.

This can be confusing, so let's use an example. There is a Windows service called **Distributed Link Tracking Client** which has a service name **TrkWks.** If we examine the table above, we can see that the TrkWks service is part of the **netsvcs** group. If we look at the Registry key for this service we see that it's

ServiceDLL is **%SystemRoot%\system32\trkwks.dll**. Therefore, using this information and what we learned above, we know that the executable command for the TrkWks service must be:

C:\WINDOWS\system32\svchost.exe -k netsvcs

When the TrkWks service is started Windows will check to see if there is a SVCHOST process for the netsvcs group already created. If not it will create an instance of one to handle services in the netsvcs group. The SVCHOST process for netsvcs will then start the service by executing the **%SystemRoot%\system32\trkwks.dll**. Once the DLL has been loaded by SVCHOST the service will then be in a started state.

Conclusion

Now that you understand what SVCHOST.EXE is and how it manages certain Windows services, seeing multiple instances in your process list should no longer be a mystery or a concern. It is not uncommon to see numerous SVCHOST entries, sometimes upwards to 8 or 9 entries, running on your computer. If you are concerned with what is running under these processes, simply use the steps described above to examine their services. If you are unsure what a particular service does and need help, feel free to ask any question you may have in of our Windows **forums**.