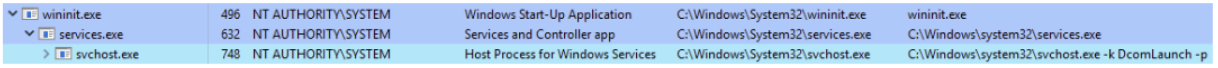
6 - wininit.exe > services.exe > svchost.exe

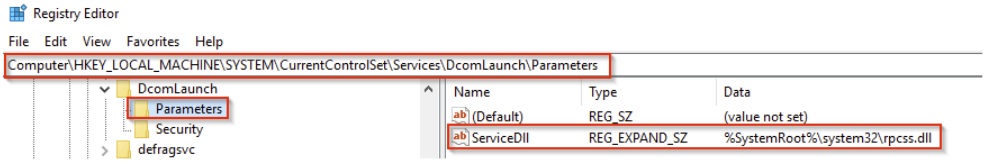
Task 8 wininit.exe > services.exe > svchost.exe

The **Service Host** (Host Process for Windows Services), or **svchost.exe**, is responsible for hosting and managing Windows services.

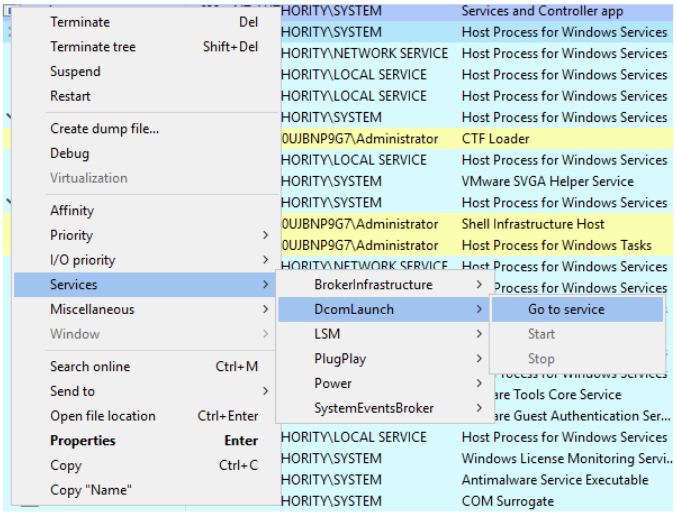


The services running in this process are implemented as DLLs. The DLL to implement is stored in the registry for the service under the `Parameters` subkey in `ServiceDLL`. The full path is `HKLM\SYSTEM\CurrentControlSet\Services\SERVICE NAME\Parameters`.

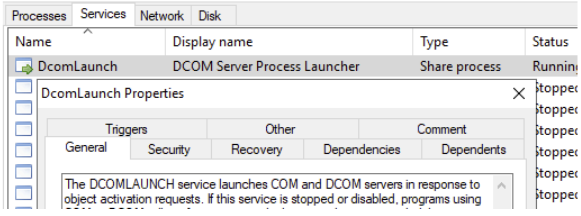
The example below is the ServiceDLL value for the Dcomlaunch service.

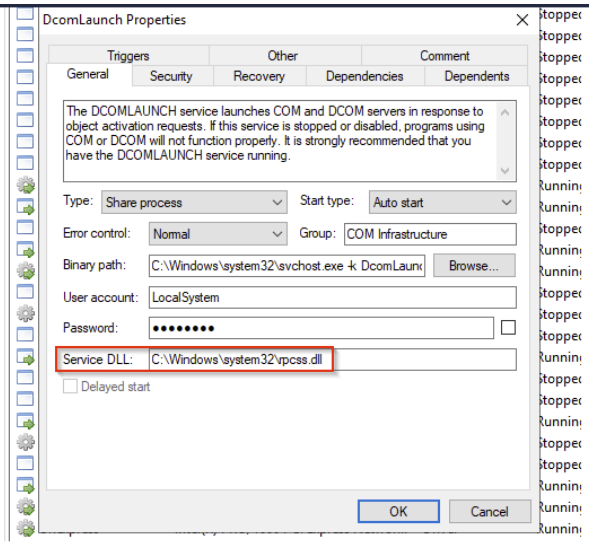


To view this information from within Process Hacker, right-click the svchost.exe process. In this case, it will be PID 748.



Right-click the service and select Properties. Look at Service DLL.



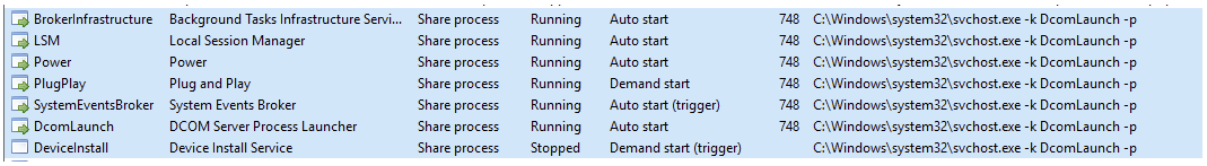


From the above screenshot, the Binary Path is listed.

Also, notice how it is structured. There is a key identifier in the binary path, and that identifier is `-k` . This is how a legitimate svchost.exe process is called.

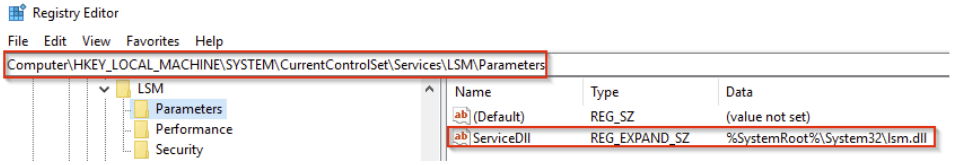
The -k parameter is for grouping similar services to share the same process. This concept was based on the OS design and implemented to reduce resource consumption. Starting from **Windows 10 Version 1703,** services grouped into host processes changed. On machines running more than 3.5 GB of memory, each service will run its own process. You can read more about this process here.

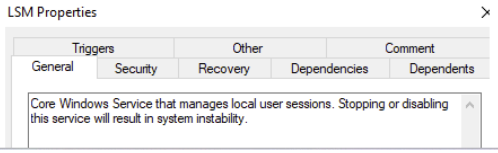
Back to the key identifier (-k) from the binary path, in the above screen, the -k value is **Dcomlaunch**. Other services are running with the same binary path in the virtual machine attached to this room.

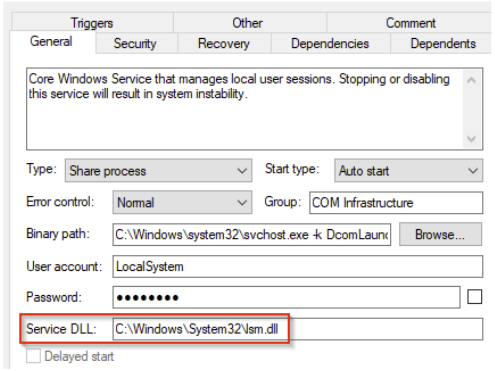


BrokerInfrastructure	Background Tasks Infrastructure Servi...	Share process	Running	Auto start	748	C:\Windows\system32\svchost.exe -k DcomLaunch -p
LSM	Local Session Manager	Share process	Running	Auto start	748	C:\Windows\system32\svchost.exe -k DcomLaunch -p
Power	Power	Share process	Running	Auto start	748	C:\Windows\system32\svchost.exe -k DcomLaunch -p
PlugPlay	Plug and Play	Share process	Running	Demand start	748	C:\Windows\system32\svchost.exe -k DcomLaunch -p
SystemEventsBroker	System Events Broker	Share process	Running	Auto start (trigger)	748	C:\Windows\system32\svchost.exe -k DcomLaunch -p
DcomLaunch	DCOM Server Process Launcher	Share process	Running	Auto start	748	C:\Windows\system32\svchost.exe -k DcomLaunch -p
DeviceInstall	Device Install Service	Share process	Stopped	Demand start (trigger)		C:\Windows\system32\svchost.exe -k DcomLaunch -p

Each will have a different value for ServiceDLL. Let's take LSM as an example and inspect the value for ServiceDLL.







Since svchost.exe will always have multiple running processes on any Windows system, this process has been a target for malicious use. Adversaries create malware to masquerade as this process and try to hide amongst the legitimate svchost.exe processes. They can name the malware svchost.exe or misspell it slightly, such as scvhost.exe. By doing so, the intention is to go under the radar. Another tactic is to install/call a malicious service (DLL).

Extra reading - Hexacorn Blog

What is normal?

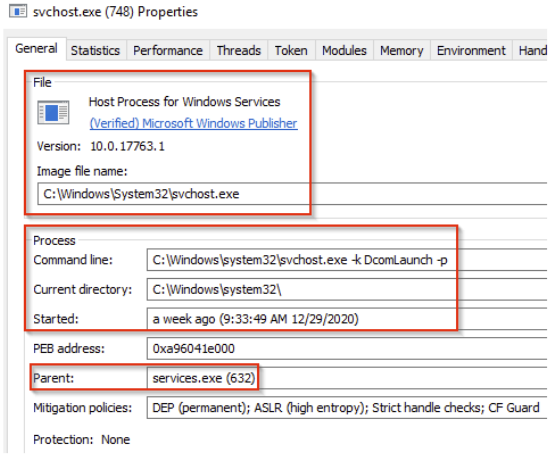


Image Path: %SystemRoot%\System32\svchost.exe
Parent Process: services.exe
Number of Instances: Many
User Account: Varies (SYSTEM, Network Service, Local Service) depending on the svchost.exe instance. In Windows 10, some instances run as the logged-in user.
Start Time: Typically within seconds of boot time. Other instances of svchost.exe can be started after boot.

What is unusual?

- A parent process other than services.exe
- Image file path other than C:\Windows\System32
- Subtle misspellings to hide rogue processes in plain sight
- The absence of the -k parameter