Default Windows Processes Quick Reference

Process	Default Folder on Disk	Notes
System	N/A	Special process for running kernel threads, ntoskrnl.exe, and drivers.
Idle	N/A	Special process for idle threads
smss.exe	%SystemRoot%\System32\	Session Manager Subsystem. 1 persistent master instance, child instances spawn and exit per session.
csrss.exe	%SystemRoot%\System32\	Client/Server Runtime Subsystem. 2 or more instances are normal (two near boot time and others as new users log on).
wininit.exe	%SystemRoot%\System32\	Windows initialization process for Session 0 (Services). One instance will be present.
lsass.exe	%SystemRoot%\System32\	One instance will be present (if Credential Guard is enabled, lsaiso.exe will also be created)
services.exe	%SystemRoot%\System32\	Service Control Manager. One instance will be present.
svchost.exe	%SystemRoot%\System32\	A service host process to host services implemented in DLLs. Multiple instances are normal. Note that the service being hosted can still be malicious even if the svchost.exe process itself is legitimate.
taskhost.exe, taskhostex.exe or taskhostw.exe	%SystemRoot%\System32\	Called taskhost.exe in Windows 7, taskhostex.exe in Windows 8 and taskhostw.exe in Windows 10. One or more instances is normal, but only with the name appropriate to your Windows version.
winlogon.exe	%SystemRoot%\System32\	One or more instances are normal depending on number of interactive users (Session 1 and above).
explorer.exe	%SystemRoot%\	One per interactive logon
Registry	N/A	New to Windows 10. Special process to store registry hives in memory.
Memory Compression (MemCompression)	N/A	Part of the Windows memory compression feature.
RuntimeBroker.exe	%SystemRoot%\System32\	One or more instances are normal depending on number of Universal Windows Platform apps open. Windows 8 and later.
dwm.exe	%SystemRoot%\System32\	Desktop Windows Manager, one instance per interactive user logged on.
dllhost.exe	%SystemRoot%\System32\	A COM surrogate process. May appear in zero to multiple instances to host COM objects implemented as DLLs.