SYSTEM.EXE

The System process is responsible for most kernel-mode threads. Modules run under System are primarily drivers (.sys files), but also include several important DLLs as well as the kernel executable, ntoskrnl.exe.

Image Path:	N/A for system.exe – Not generated from an executable image
Parent Process:	None
Number of Instances:	One
User Account:	Local System
Start Time:	At boot time

SMSS.EXE

The Session Manager process is responsible for creating new sessions. The first instance creates a child instance for each new session. Once the child instance initializes the new session by starting the Windows subsystem (csrss.exe) and wininit.exe for Session 0 or winlogon.exe for Session 1 and higher, the child instance exits.

Image Path:	%SystemRoot%\System32\smss.exe
Parent Process:	System
Number of Instances:	One master instance and another child instance per session. Children exit after creating their session.
User Account:	Local System
Start Time:	Within seconds of boot time for the master instance

WININIT.EXE

Wininit.exe starts key background processes within Session 0. It starts the Service Control Manager (services.exe), the Local Security Authority process (lsass.exe), and lsaiso.exe for systems with Credential Guard enabled. Note that prior to Windows 10, the Local Session Manager process (lsm.exe) was also started by wininit.exe. As of Windows 10, that functionality has moved to a service DLL (lsm.dll) hosted by svchost.exe.

Image Path:	%SystemRoot%\System32\wininit.exe
Parent Process:	Created by an instance of smss.exe that exits, so tools usually do not provide the parent process name.
Number of Instances:	One
User Account:	Local System
Start Time:	Within seconds of boot time

TASKHOSTW.EXE

The generic host process for Windows Tasks. Upon initialization, taskhostw.exe runs a continuous loop listening for trigger events.

Image Path:	%SystemRoot%\System32\taskhostw.exe
Parent Process:	svchost.exe
Number of Instances:	One or more
User Account:	Multiple taskhostw.exe processes are normal. One or more may be owned by logged-on users and/or by local service accounts.
Start Time:	Start times vary greatly

WINLOGON.EXE

Winlogon handles interactive user logons and logoffs. It launches LogonUI.exe, which uses a credential provider to gather credentials from the user, and then passes the credentials to lsass.exe for validation. Once the user is authenticated, Winlogon loads the user's NTUSER.DAT into HKCU and starts the user's shell (usually explorer.exe) via userinit.exe.

Image Path:	%SystemRoot%\System32\winlogon.exe
Parent Process:	Created by an instance of smss.exe that exits, so analysis tools usually do not provide the parent process name.
Number of Instances:	One or more
User Account:	Local System
Start Time:	Within seconds of boot time for the first instance (for Session 1).

CSRSS.EXE

The Client/Server Run-Time Subsystem is the user-mode process for the Windows subsystem. Its duties include managing processes and threads, importing many of the DLLs that provide the Windows API, and facilitating shutdown of the GUI during system shutdown.

Image Path:	%SystemRoot%\System32\csrss.exe
Parent Process:	Created by an instance of smss.exe that exits.
Number of Instances:	Two or more
User Account:	Local System
Start Time:	Within seconds of boot time for the first two instances (for Session 0 and 1).

SERVICES.EXE

Implements the Unified Background Process Manager (UBPM), which is responsible for background activities such as services and scheduled tasks. Services.exe also implements the Service Control Manager (SCM), which specifically handles the loading of services and device drivers marked for auto-start.

Image Path:	%SystemRoot%\System32\services.exe
Parent Process:	wininit.exe
Number of Instances:	One
User Account:	Local System
Start Time:	Within seconds of boot time

SVCHOST.EXE

Generic host process for Windows services. It is used for running service DLLs. Windows will run multiple instances of svchost.exe, each using a unique "-k" parameter for grouping similar services. Typical "-k" parameters include DcomLaunch, RPCSS, LocalServiceNetworkRestricted, LocalServiceNoNetwork, LocalServiceAndNoImpersonation, netsvcs, NetworkService, and more.

Image Path:	%SystemRoot%\system32\svchost.exe
Parent Process:	services.exe (most often)
Number of Instances:	Many (generally at least 10)
User Account:	Varies depending on svchost instance

Start Time:	Typically, within seconds of boot time. However, services can be started after boot (e.g., at logon)

LSASS.EXE

The Local Security Authentication Subsystem Service process is responsible for authenticating users by calling an appropriate authentication package specified in HKLM\SYSTEM\CurrentControlSet\Control\Lsa.. lsass.exe is also responsible for implementing the local security policy (such as password policies and audit policies) and for writing events to the security event log.

Image Path:	%SystemRoot%\System32\lsass.exe
Parent Process:	wininit.exe
Number of Instances:	One
User Account:	Local System
Start Time:	Within seconds of boot time

EXPLORER.EXE

At its core, Explorer provides users access to files. Functionally, though, it is both a file browser via Windows Explorer (though still explorer.exe) and a user interface providing features such as the user's Desktop, the Start Menu, the Taskbar, the Control Panel, and application launching via file extension associations and shortcut files.

Image Path:	%SystemRoot%\explorer.exe
Parent Process:	Created by an instance of userinit.exe that exits
Number of Instances:	One or more per interactively logged-on user
User Account:	<logged-on user(s)>
Start Time:	First instance starts when the owner's interactive logon begins

REFERENCE: https://www.sans.org/posters/hunt-evil/