/in/halilbaris/

Originating processes on EDRs

Originating Process	Description	Security Implications
explorer.exe	File manager process in Windows, often initiates user-launched applications.	If it launches executables from suspicious directories (like `Temp` or `AppData`), it may indicate malware attempting to masquerade as a legitimate user action.
powershell.exe	Command-line shell and scripting language, used for automation.	Frequently used in phishing and ransomware attacks. Look for obfuscation, encoded commands, or unusual PowerShell usage.
cmd.exe	Windows Command Prompt for executing commands.	Abnormal commands, scripts, or executions in unusual locations can signal malware, lateral movement, or privilege escalation attempts.
wmiprvse.exe	Windows Management Instrumentation (WMI) provider, used for system management.	WMI commands from unauthorized users or systems may indicate lateral movement or remote execution attempts by attackers.
services.exe	Manages system services on Windows.	If it spawns unexpected processes, it may signal privilege escalation or persistence mechanisms by malware.
svchost.exe	Generic host process for running Windows services.	Extra or suspicious instances, especially from non-standard directories, could indicate process injection or backdoor activity.
lsass.exe	Local Security Authority Subsystem, handles system security policies and user sessions.	Access to this process or memory dumps may suggest credential harvesting by attackers.

winword.exe / excel.exe	Microsoft Office applications, used in document handling.	Macros spawning other processes like `cmd.exe` or `powershell.exe` can indicate a phishing or malware infection.
rundll32.exe	Executes functions from DLL files.	Loading unexpected DLLs, especially from unknown directories, often suggests malicious activity.
mshta.exe	Microsoft HTML Application Host, used to run HTML applications.	Commonly exploited in phishing to execute scripts or payloads, especially if connecting to external URLs.
schtasks.exe	Command-line tool for creating scheduled tasks.	New or unusual tasks may indicate persistence tactics by attackers. Review the scheduling time and task actions.
taskeng.exe	Task Scheduler engine for managing scheduled tasks.	Sudden or unknown task creation could be linked to persistence mechanisms or unauthorized access.
regsvr32.exe	Registers and unregisters DLL files.	Attackers often use it to bypass defenses and execute malicious DLLs. Watch for unregistered DLL paths.
msiexec.exe	Microsoft installer for handling `.msi` files.	Unrecognized installations may indicate attempts to install unauthorized or malicious software.
conhost.exe	Console Window Host, used to manage console processes in the background.	Unusual instances could indicate attempts to mask malicious command-line activity.
chrome.exe / firefox.exe / iexplore.exe / msedge.exe	Web browser processes.	Browser activity that spawns unexpected processes may suggest drive-by downloads or web-based exploitation.

java.exe / javaw.exe	Executes Java applications.	Java is often targeted for exploitation. Unexpected Java executions may indicate malware or vulnerability exploitation.
mstsc.exe	Microsoft Remote Desktop Client, used for remote access.	Repeated or unusual usage can signal lateral movement or unauthorized access to remote machines.
anydesk.exe / teamviewer.exe	Third-party remote desktop tools for remote management.	Unauthorized installation or usage could indicate unauthorized remote access by an attacker.
psexec.exe	Tool for remote command execution on Windows, often used in IT administration.	If used unexpectedly, it may indicate lateral movement by an attacker aiming for remote control of systems.
putty.exe	SSH client for remote access to servers.	Unexpected use suggests unauthorized access attempts or lateral movement, especially in environments where it's not standard.
acrobat.exe	Adobe Acrobat for handling PDFs.	Embedded scripts or executables from PDFs may signal malware infections through document exploitation.
python.exe	Python interpreter, used for running Python scripts.	If Python isn't normally used on a system, unexpected executions could signal the presence of custom malware or attacker tools.