Behavior-chain detection for T1134.004 Access Token Manipulation: Parent PID Spoofing (Windows), Detection Strategy DET0489

Archived: 2026-04-05 17:07:23 UTC

AN1351

A process explicitly forges its parent using EXTENDED_STARTUPINFO + PROC_THREAD_ATTRIBUTE_PARENT_PROCESS (UpdateProcThreadAttribute → CreateProcess[A/W]/CreateProcessAsUserW) or other Native API paths, resulting in **mismatched/implausible lineage** across ETW EventHeader ProcessId, Security 4688 Creator Process ID/Name, and sysmon ParentProcessGuid. Often paired with privilege escalation when the chosen parent runs as SYSTEM.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	WinEventLog:Security	EventCode=4688
OS API Execution (DC0021)	etw:Microsoft-Windows-Kernel-Process	api_call: UpdateProcThreadAttribute (PROC_THREAD_ATTRIBUTE_PARENT_PROCESS) and CreateProcess* with EXTENDED_STARTUPINFO_PRESENT / StartupInfoEx
Process Metadata (DC0034)	etw:Microsoft-Windows-Kernel-Process	process_start: EventHeader.ProcessId true parent vs reported PPID mismatch

Mutable Elements

Field	Description
TimeWindow	Correlation window between UpdateProcThreadAttribute/CreateProcess* and the resulting process (default 5–10 minutes).
AllowedSpoofers	Legitimate binaries that commonly use StartupInfoEx/PPID assignment (e.g., consent.exe, svchost.exe during UAC).

Field	Description
ParentPrivilegeDeltaThreshold	Minimum privilege/integrity gap between chosen parent and real caller to raise severity.
LineageMismatchTolerance	Number of mismatched sources (0–3) before alerting to reduce noise.
SensitiveParents	List of SYSTEM parents that, if spoofed, auto-escalate severity (e.g., lsass.exe, services.exe, wininit.exe).
