Behavior-chain, platform-aware detection strategy for T1127 Trusted Developer Utilities Proxy Execution (Windows), Detection Strategy DET0172

Archived: 2026-04-05 14:30:39 UTC

AN0488

A trusted/signed developer utility (parent) is executed in a non-developer context and (a) spawns suspicious children (e.g., powershell.exe, cmd.exe, rundll32.exe, regsvr32.exe, wscript.exe), (b) loads unsigned/user-writable DLLs, (c) writes and then runs a new PE from user-writable paths, and/or (d) immediately makes outbound network connections.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window between developer utility execution, payload write, and network egress (e.g., 0–30 minutes).
AllowedUtilitiesList	Org-specific list of dev utilities legitimately used on build/dev hosts to suppress noise.
DeveloperHosts	List of known developer/build systems where these tools are expected; raise severity off-host.
SuspiciousChildList	Child processes considered high-risk when spawned by dev utilities (powershell.exe, rundll32.exe, regsvr32.exe, cmd.exe, wscript.exe, mshta.exe).
RarePathRegex	Regex of user-writable or atypical paths (e.g., %TEMP%, %APPDATA%, recycle bin, public profile) for payload drops.
UnsignedOrInvalidSignatureOnly	Toggle to alert only when child/payload is unsigned or signature invalid to reduce noise.
ParentProcessAllowList	Known orchestrators (e.g., CI/CD agents) that often run these utilities legitimately.
NetworkReputationThreshold	Heuristic for rare/unknown destination (no DNS reputation, new domain, geo outside region).

Source: https://attack.mitre.org/detectionstrategies/DET0172#AN0488