Behavior-chain detection strategy for T1127.003 Trusted Developer Utilities Proxy Execution: JamPlus (Windows), Detection Strategy DET0585

Archived: 2026-04-05 16:07:55 UTC

Analytics

- Windows

AN1610

Abuse of JamPlus.exe to launch malicious payloads via crafted .jam files, resulting in abnormal process creation, command execution, or artifact generation outside of standard development workflows.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation time window (e.g., 0–30 minutes) for JamPlus.exe execution, child processes, and file/network events.
AllowedBuildHosts	Known developer systems where JamPlus.exe usage is expected; alerts are raised if executed elsewhere.
SuspiciousChildList	Child processes considered anomalous (e.g., PowerShell, cmd, wscript) when spawned by JamPlus.exe.
RarePathRegex	Regex patterns for non-standard or user-writable paths where JamPlus.exe drops artifacts.
