Supply-chain tamper in dependencies/dev-tools (manager → write/install → first-run → egress), Detection Strategy DET0009

Archived: 2026-04-05 12:51:46 UTC

AN0021

Adversary manipulates dependencies/dev tools used by developers or CI: a package manager (npm/yarn/pnpm, pip/pipenv, nuget/dotnet, chocolatey/winget, maven/gradle) or a compiler/IDE downloads or restores content; files are written under project paths and execution paths (node_modules, packages, .nuget, .gradle, .m2, %AppData%\npm, %UserProfile%.cargo\bin, temp build dirs). First run of newly written components triggers scripts (preinstall/postinstall), shell/PowerShell spawning, or loader DLLs, followed by network egress to non-approved registries/CDNs.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlate file write by package manager to first execution and egress (default 90 minutes).
ApprovedRegistries	Allow-listed registries (e.g., registry.npmjs.org, pypi.org, nuget.org, maven.apache.org, company proxies/CDNs).
DevHosts	Limit analytics to engineering endpoints/CI agents to reduce noise.
TrustedPublishers	Code-signing publishers acceptable for dev tools.

AN0022

Developer or CI invokes package managers/compilers (apt/yum + build-essential, npm/yarn/pnpm, pip/pip3, gem, cargo, go, maven/gradle). These write executable or script files into PATH or project dirs and immediately execute embedded lifecycle hooks (preinstall/postinstall, setup.py, npm scripts) that spawn shells or curl/wget, followed by egress to unfamiliar registries or domains.

Log Sources

Mutable Elements

Field	Description
ApprovedRepos	Allowed APT/YUM repos and GPG keys for build tools.
PathScope	Monitor /usr/local/bin, /usr/bin, /opt/*/bin, ~/.local/bin, node_modules/.bin, .venv/bin, .cargo/bin, .gradle, .m2.
TimeWindow	Default 90 minutes for write → exec → egress linkage.

AN0023

Developer tools (Homebrew, pip, npm/yarn, Xcode builds) install or update dependencies; new Mach-O or scripts appear under /usr/local, /opt/homebrew, ~/Library/Application Support, project dirs (node_modules/.bin, venv/bin). First run spawns sh/zsh/osascript/curl and new outbound flows; Gatekeeper/AMFI may flag unsigned components.

Log Sources

Mutable Elements

Field	Description
AllowedTeamIDs	Apple Developer Team IDs for approved dev tools (Xcode, JetBrains, etc.).
BrewTapsAllowList	Homebrew taps allowed in your environment.
TimeWindow	Default 90 minutes.
