Compromised software/update chain (installer/write → first-run/child → egress/signature anomaly), Detection Strategy DET0309

Archived: 2026-04-05 15:03:50 UTC

AN0862

Adversary ships a tampered application or update: an updater/installer (msiexec/setup/update.exe/vendor service) writes or replaces binaries; on first run it spawns scripts/shells or unsigned DLLs and beacons to non-approved update CDNs/hosts. Detection correlates: (1) process creation of installer/updater → (2) file metadata changes in program paths → (3) first-run children and module/signature anomalies → (4) outbound connections to unexpected hosts within a short window.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlate write→first-run→egress (default 90 minutes).
ApprovedUpdateHosts	Allow-list of vendor update endpoints, enterprise proxy/cache.
ApprovedSigners	Code-signing publishers allowed for programs/services.
ProgramPaths	Monitored install locations (e.g., C:\Program Files, C:\ProgramData, %LOCALAPPDATA%).

AN0863

A compromised package/update (deb/rpm/tarball/AppImage/vendor updater) is installed, writing/overwriting files in /usr/local/bin, /usr/bin, /opt, or ~/.local; first run executes unexpected shells/curl/wget and connects to unapproved hosts. Correlate package/updater execution → file writes/replace → first-run child processes → egress.

Log Sources

Mutable Elements

Field	Description
PathScope	Monitored install paths (/usr/local, /usr/bin, /opt/*, ~/.local/bin, /var/lib/systemd).
ApprovedRepos	Allow-listed APT/YUM repos and GPG keys for vendor updates.
TimeWindow	Default 90 minutes.

AN0864

A tampered app/pkg/notarized update is installed via installer, softwareupdated, Homebrew, or vendor updater; new Mach-O or bundle contents appear in /Applications, /Library, /usr/local or /opt/homebrew; first run spawns sh/zsh/osascript/curl and makes egress to unfamiliar domains; AMFI/Gatekeeper may log signature/notarization problems.

Log Sources

Mutable Elements

Field	Description
AllowedTeamIDs	Apple Developer Team IDs allowed for enterprise.
BrewTapsAllowList	Trusted Homebrew taps.
TimeWindow	Default 90 minutes.
