Detect malicious IDE extension install/usage and IDE tunneling, Detection Strategy DET0561

Archived: 2026-04-05 14:53:23 UTC

AN1548

Adversary installs or side-loads an IDE extension (VS Code, IntelliJ/JetBrains, Eclipse) or enables IDE tunneling. Chain: (1) IDE binary starts on a non-developer endpoint or server, often with install/force/tunnel flags → (2) extension files/registrations appear under user profile → (3) browser/IDE initiates outbound connections to extension marketplaces, update endpoints, or IDE remote/tunnel services → (4) optional child tools (ssh, node, powershell) execute under the IDE context.

Log Sources

Mutable Elements

Field	Description
IDEList	Executable names/paths (e.g., code.exe, idea64.exe, eclipse.exe, jetbrains-gateway.exe) vary by version and packaging.
SuspiciousCLI	Flags such as --install-extension, --force, --disable-extensions, --user-data-dir, --uninstall-extension, tunnel/remote flags are tunable.
ServerZones	List of hosts where IDEs should never run (prod servers, DCs).
AllowedHosts	Approved extension marketplaces/ide services; use to suppress benign traffic.
TimeWindow	Correlation horizon (e.g., 15–30m) between process start, file writes, and outbound IDE/tunnel connections.

AN1549

Adversary installs or abuses IDE extensions via CLI or direct write to profile directories and then communicates with marketplaces or remote tunnel services. Chain: auditd execve (code/idea/eclipse) with install/update flags or writes under ~/.vscode/extensions, ~/.config/JetBrains → outbound flows to *.visualstudio.com, marketplace.visualstudio.com,* .jetbrains.com, githubusercontent.com, or SSH/WebSocket tunnel endpoints → optional ssh/node processes spawned by IDE.

Log Sources

Mutable Elements

Field	Description
IDEPaths	Per-distro/profile extension directories differ; tune for Chromium/JetBrains snap/flatpak paths.
DomainAllowlist	Enterprise-approved repos and proxies to reduce FPs.
UserRoleScope	Limit to non-developer users or production servers.
TimeWindow	Join horizon across file, process, and network telemetry.

AN1550

Adversary adds IDE extensions or plugins (VS Code, JetBrains Toolbox/EAP, Eclipse) via GUI or CLI, possibly via managed profiles. Chain: process start with install/update flags → plist/extension folder changes under ~/Library/Application Support/Code or ~/Library/Application Support/JetBrains → outbound connections to marketplaces/tunnel services → optional helper (ssh/node) spawned.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Execution of Code.app, idea, JetBrainsToolbox, eclipse with install/extension flags
File Creation (DC0039)	macos:unifiedlog	Writes under ~/Library/Application Support/Code*/extensions or JetBrains plugins
Network Traffic Flow (DC0078)	macos:unifiedlog	Outbound connections from IDE processes to marketplace/tunnel domains

Mutable Elements

Field	Description
PlistLocations	Per-app preference domains and plugin directories vary by version.
MDMProfiles	If MDM installs extensions, allowlist those events to avoid FPs.
TimeWindow	Correlation range between install and first beacon.
