E03. Editor-extension package analysis

Ilja Krasnjanski
24 October 2026 · Edited evidence report
Historical evidence through 24 July 2026; later engineering checks identified separately.

This report synthesizes the cited case records. Exhibits distinguish retained artifact excerpts from secondary analytical records and claims whose original inputs are unavailable. Excerpts may be redacted or reformatted; extraction methods and limitations are stated locally. Fingerprints identify inputs, not the truth of their claims. Bracketed S labels identify the analysis records listed at the end.

Package identity

The recorded VSIX was collected on 22 July 2026 and inspected without installation. Its size is 17,647,582 bytes and SHA-256 is `52886aab179f26421678ff23af1b0fabf0a17ffbb534369cdbbac8008cbed8e7`. The manifest names `google-update-support`, publisher `google-dev-tools`, version `1.0.0`, and activation event `onStartupFinished`. The installed identifier is `google-dev-tools.google-update-support`. These are package claims, not evidence of affiliation with Google. [S1]

Activation and configuration

The startup activation event can permit extension activity after the initial lure workspace is removed, provided the extension remains installed and enabled. Repository cleanup therefore does not establish removal of the installed component. The source record describes cleanup of workspace task and staging files after installation. Neither the manifest nor cleanup code establishes that a particular user permitted installation. [S1]

Workspace configuration supplies the server URL, client identifier and agent token through the `googleUpdateSupport` namespace. Other keys select the agent archive and Windows activation mode. Empty defaults in the manifest show why the extension alone may be insufficient to reconstruct a deployment's destination. No token values are reproduced.

Bundled native agents

The nested archive contains three recorded Go agents. Their SHA-256 values are:

- macOS arm64: `339907b44f161f57ff30819f422c552382ff437b3ae437463b4222cfe86bd943`.
- macOS amd64: `bb10adac5b0124efedfe71102c1d5638135ec9e1cde8c8cb3353c5ed91bb9f81`.
- Linux amd64: `a2b9a769df84d9d3a4694bb0252a2c6a5e5f5d1a85a04565362737092bbb3a86`.

The case record reports matches with previously published indicators. The match establishes byte identity for those samples, not execution or ownership. A separate Windows JavaScript pipeline is covered in E04. [S1]

Build interpretation

The May agents and a July implant expose different VCS revisions. The macOS arm64 agent records cgo enabled; other examined builds differ. These are build attributes, not a unique identification of a physical machine. VCS timestamps should not be relabeled as certified compilation times. No editor execution, persistence test or fresh external hash lookup was performed. [S1, S2]

Exhibits

Exhibit E03-1. VSIX package manifest — impersonation fields

Artifact: extension/package.json (from google-update-support.vsix) · 3328 bytes · SHA-256
`ac856c6d118f81b730544dcf7c59e98bd8a8272f98a915fe9ce31617316da893`
Location: archive member `extension/package.json`, lines 1-13
Extraction: `unzip -p google-update-support.vsix extension/package.json`
Supports: manifest names, publisher, version, activation event, installed id, `main`, displayName, description

```
{
  "name": "google-update-support",
  "displayName": "Google Update Support",
  "description": "Keeps your development environment secure and up to date by managing \
essential Google platform services in the background.",
  "version": "1.0.0",
  "publisher": "google-dev-tools",
  "engines": {
    "vscode": "^1.80.0"
  },
  "categories": [
    "Other"
  ],
  "activationEvents": [
    "onStartupFinished"
  ],
  "main": "./extension.js",
```

The installed identifier `publisher.name` is `google-dev-tools.google-update-support`. The description text ("Keeps your development environment secure and up to date …") is reproduced verbatim; it was hard-wrapped with a trailing `\` for width. No redaction.

Exhibit E03-2. The seven googleUpdateSupport configuration keys

Artifact: extension/package.json · 3328 bytes · SHA-256
`ac856c6d118f81b730544dcf7c59e98bd8a8272f98a915fe9ce31617316da893`
Location: archive member `extension/package.json`, `contributes.configuration.properties`
Extraction: `unzip -p google-update-support.vsix extension/package.json`
Supports: "configuration supplies the server URL, client identifier and agent token"; empty defaults

```
googleUpdateSupport.enabled                  type boolean  default true
googleUpdateSupport.agentZipRelativePath     type string   default ""
googleUpdateSupport.windowsActivationMode    type string   default "extensionJs"  \
                                             enum[nativeAgent,extensionJs]
googleUpdateSupport.showPipelineUiMessages   type boolean  default false
googleUpdateSupport.companyWalletServerUrl   type string   default ""
googleUpdateSupport.companyWalletClientId    type string   default ""
googleUpdateSupport.companyWalletAgentToken  type string   default ""
```

The property keys and their declared `type`/`default`/`enum` values are byte-for-byte from the manifest; the layout above is a condensation of the JSON property blocks (key names, type and default tokens unchanged). The three company-wallet keys all default to empty, so the package alone carries no C2. No token values exist in the manifest to redact.

Exhibit E03-3. Bundled native Go agents (nested archive)

Artifact: three Go binaries inside extension/google-update-support-agent.zip · agent zip 17,283,435 bytes · SHA-256
`e1bf1b29e6fa3525d7f32f429290a88d6ea2890e61c06574b8ff6372aa5d0667`
Location: VSIX member `extension/google-update-support-agent.zip`, extracted members
Extraction: `sha256sum extracted/agents/google-update-support-*`
Supports: the three published-IOC sample hashes

```
339907b44f161f57ff30819f422c552382ff437b3ae437463b4222cfe86bd943  darwin-arm64
bb10adac5b0124efedfe71102c1d5638135ec9e1cde8c8cb3353c5ed91bb9f81  darwin-amd64
a2b9a769df84d9d3a4694bb0252a2c6a5e5f5d1a85a04565362737092bbb3a86  linux-amd64
```

These three SHA-256 values are the hashes the report ties to the previously published indicator set. No redaction.

Exhibit E03-4. Go build metadata — VCS revision and the cgo difference

Artifact: google-update-support-linux-amd64 / -darwin-arm64 (embedded build info) · SHA-256 `a2b9a769…3a86` (linux), `339907b4…d943` (darwin-arm64)

Location: embedded Go buildinfo in each agent

Extraction: `go version -m extracted/agents/google-update-support-linux-amd64` (static; binary not executed)

Supports: shared VCS revision; cgo enabled on darwin/arm64 and not on the others

```
google-update-support-linux-amd64: go1.26.2
▫build▫-trimpath=true
▫build▫CGO_ENABLED=0
▫build▫GOARCH=amd64   GOOS=linux
▫build▫vcs.revision=85669fbcaa34ba565229b491db96ece6722cc346
▫build▫vcs.time=2026-05-13T05:09:31Z    vcs.modified=false

google-update-support-darwin-arm64: go1.26.2
▫build▫-trimpath=true
▫build▫CGO_ENABLED=1
▫build▫GOARCH=arm64   GOOS=darwin
▫build▫vcs.revision=85669fbcaa34ba565229b491db96ece6722cc346
▫build▫vcs.time=2026-05-13T05:09:31Z    vcs.modified=false
```

The bundled agents are the May build (`vcs.revision=85669fb…`, `vcs.time=2026-05-13`). The darwin/arm64 agent records `CGO_ENABLED=1` while the linux/amd64 agent records `CGO_ENABLED=0`, the build-attribute difference the report cites. No redaction.

Exhibit E03-5. extension.js is obfuscated — rotated string array, zero config matches

Artifact: extension/extension.js · 606,460 bytes · SHA-256 `d5e9288693aa745dc89368deac677e7ea1ec81e663283af30838cdae189b7a7e`

Location: byte offset ~1900 (string-array rotation IIFE); whole-file grep

Extraction: `grep -c googleUpdateSupport extracted/extension/extension.js` and a byte-offset read of the rotation call

Supports: "obfuscated … searching for googleUpdateSupport … returns zero matches"; rotation of the 3,899-entry array

```
}(_0x3205,0x7a73a*0x1+0x10*0x35f1+0xff95*-0x3));\
const vscode=require(_0x3ef45d(0x87b,0xdf3,'3975',0xb1a)+'e'),
```

`grep -c googleUpdateSupport` returns `0` on this file, versus the plaintext manifest. The string array `_0x3205` holds 3,899 entries and is rotated inside a self-shifting IIFE (the numeric expression resolves to the rotation count); module names such as `require('vscod'+'e')` are rebuilt from decoder calls. No redaction.

Claims without a retained primary artifact

- "Matches with previously published indicators" / "Proofpoint's published set": the three agent SHA-256 values are re-derivable from the retained binaries (E03-3), but the external published IOC list they are matched against is not in the workspace, so the equality is an analytical cross-reference rather than something re-derivable from a local artifact.
- "A separate Windows JavaScript pipeline is covered in E04": the May bundled agents (E03-4) and the July implant (`vcs.revision=056221e34235…`, `vcs.time=2026-07-21`) are both retained — the July implant is in `overlord_go_implant_linux-amd64.elf`, a different incident folder — so the two-commit development-timeline claim is backed, just not from a single artifact.

Exhibit inputs

Retained inputs identified by size and SHA-256. These include artifacts and analytical records; each exhibit identifies its evidence type and extraction limitations. The files themselves are not distributed.

google-update-support.vsix (editor extension package) · 17,647,582 bytes

`SHA-256 52886aab179f26421678ff23af1b0fabf0a17ffbb534369cdbbac8008cbed8e7`

extension/package.json (VSIX manifest) · 3,328 bytes

`SHA-256 ac856c6d118f81b730544dcf7c59e98bd8a8272f98a915fe9ce31617316da893`

extension/extension.js (obfuscated loader) · 606,460 bytes

`SHA-256 d5e9288693aa745dc89368deac677e7ea1ec81e663283af30838cdae189b7a7e`

extension/google-update-support-agent.zip (nested agent archive) · 17,283,435 bytes

`SHA-256 e1bf1b29e6fa3525d7f32f429290a88d6ea2890e61c06574b8ff6372aa5d0667`

google-update-support-darwin-arm64 (Go agent) · 13,304,624 bytes

`SHA-256 339907b44f161f57ff30819f422c552382ff437b3ae437463b4222cfe86bd943`

google-update-support-darwin-amd64 (Go agent) · 14,495,504 bytes

`SHA-256 bb10adac5b0124efedfe71102c1d5638135ec9e1cde8c8cb3353c5ed91bb9f81`

google-update-support-linux-amd64 (Go agent) · 14,655,650 bytes

`SHA-256 a2b9a769df84d9d3a4694bb0252a2c6a5e5f5d1a85a04565362737092bbb3a86`

Source records and fingerprints

SHA-256 identifies the reviewed source bytes, not acquisition time or every artifact described. Restricted originals are not reproduced.

[S1] VSIX static analysis, 22 July 2026 · 18,399 bytes

`SHA-256 2d21fee6780bbc217490d80daa5de424cbb154dee0034b5fd53ef30af46563b2`

[S2] Edited preprint manuscript · 54,752 bytes

`SHA-256 dc5d8abe46fcd33e9a28ccc859778e22ced661beff2d559a072bfb04f9d131dc`