E18. Framework and sample comparison

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.

Comparison scope

The July analysis compares recovered Go build information with selected files from the public Overlord project, including its module dependencies and configuration examples. The comparison is bounded to the material examined at that time. It is not a comprehensive audit of all historical versions, forks or plugins. No upstream resource was fetched again for this document. [S1]

Shared framework components

The module path, WebAssembly runtime, remote-control functions and transport configuration appear in the framework comparison. Those features identify software lineage rather than this campaign's operator. The framework's authors and other users cannot be attributed to the campaign merely because the samples derive from its code. [S1]

A recorded build revision was not found in the public repository examined. That result is compatible with a private clone, unpublished work, removed history or other metadata explanations. It does not by itself prove a particular private fork or who maintained it.

Sample-specific findings

The comparison identifies SQLite-related dependencies and wallet/browser-collection markers absent from the selected upstream files. It also distinguishes GUS-prefixed configuration and deployment logic from the generic framework surface. This supports sample-specific extensions relative to the comparison baseline. It does not establish that every similarly named function was authored by the same operator or absent from every other framework version. [S1]

Capture discrepancy

The original dependency review inferred that the Linux sample lacked screen capture because selected upstream capture dependencies were absent. The later capability review reports capture-related symbols and frame-difference routines in the held binary. Dependency lists and binary symbols answer different questions. The earlier categorical capture-free conclusion is therefore not retained. Build-specific reachability and functioning capture require further analysis or controlled runtime evidence. [S1, S2]

Assessment

Detection should distinguish framework markers from the narrower combination of collection, configuration and delivery indicators. A generic Overlord hit is not campaign attribution. The strongest supported conclusion is a framework-derived agent with additional collection-related components in the examined material. E05 details the capture observations, and E15 documents the companion's deliberately combined selectors.

Exhibits

Exhibit E18-1. Embedded Go build information

Artifact: Go implant (linux-amd64) · 15,790,242 bytes · SHA-256
`ef183bbb40f4c7c3f4b52994cdba3295f3eab2604fdad99eefa3b67b8d966e8d`
Location: Go build-info section
Extraction: `go version -m overlord_go_implant_linux-amd64.elf`
Supports: the overlord-client module path, the wazero WebAssembly runtime, the SQLite dependencies (modernc.org/sqlite, libc, memory, mathutil), the build revision and vcs.time

```
overlord_go_implant_linux-amd64.elf: go1.26.2
▫path▫overlord-client/cmd/agent
▫mod▫overlord-client▫(devel)▫
▫dep▫github.com/creack/pty▫v1.1.21▫h1:1/QdRyBaHHJP61QkWMXlOIBfsgdDeeKfK8SYVUWJKf0=
▫dep▫github.com/dustin/go-humanize▫v1.0.1▫h1:GzkhY7T5VNhEkwH0PVJgjz+fX1rhBrR7pRT3mDkpeCY=
▫dep▫github.com/google/uuid▫v1.6.0▫h1:NIvaJDMOsjHA8n1jAhLSgzrAzy1Hgr+hNrb57e+94F0=
▫dep▫github.com/remyoudompheng/bigfft▫v0.0.0-20230129092748-24d4a6f8daec▫h1:W09IVJc94icq4NjY3\
clb7Lk8O1qJ8BdBEF8z0ibU0rE=
▫dep▫github.com/tetratelabs/wazero▫v1.7.0▫h1:jg5qPydno59wqjpGrHph81lbtHzTrWzwwtD4cD88+hQ=
▫dep▫github.com/vmihailenco/msgpack/v5▫v5.4.1▫h1:cQriyiUvjTwOHg8QZaPihLWeRAAVoCpE00IUPn0Bjt8=
▫dep▫github.com/vmihailenco/tagparser/v2▫v2.0.0▫h1:y09buUbR+b5aycVFQs/g70pqKVZNBmxwAhO7/IwNM9\
g=
▫dep▫golang.org/x/crypto▫v0.47.0▫h1:V6e3FRj+n4dbpw86FJ8Fv7XVOql7TEwpHapKoMJ/GO8=
▫dep▫golang.org/x/sys▫v0.43.0▫h1:Rlag2XtaFTxp19wS8MXlJwTvoh8ArU6ezoyFsMyCTNI=
▫dep▫modernc.org/libc▫v1.55.3▫h1:AzcW1mhlPNrRtjS5sS+eW2ISCgSOLLNyFzRh/V3Qj/U=
▫dep▫modernc.org/mathutil▫v1.6.0▫h1:fRe9+AmYlaej+64JsEEhoWuAYBkOtQiMEU7n/XgfYi4=
▫dep▫modernc.org/memory▫v1.8.0▫h1:IqGTL6eFMaDZZhEWwcREgeMXYwmW83LYW8cROZYkg+E=
▫dep▫modernc.org/sqlite▫v1.34.5▫h1:Bb6SR13/fjp15jt70CL4f18JIN7p7dnMExd+UFnF15g=
▫dep▫nhooyr.io/websocket▫v1.8.10▫h1:mv4p+MnGrLDcPlBoWsvPP7XCzTYMXP9F9eIGoKbgx7Q=
▫build▫-buildmode=exe
▫build▫-compiler=gc
▫build▫-trimpath=true
▫build▫DefaultGODEBUG=cryptocustomrand=1,tlssecpmlkem=0,urlstrictcolons=0
▫build▫CGO_ENABLED=0
▫build▫GOARCH=amd64
▫build▫GOOS=linux
▫build▫GOAMD64=v1
▫build▫vcs=git
▫build▫vcs.revision=056221e342357056c8539585806f76632660e414
▫build▫vcs.time=2026-07-21T01:14:06Z
▫build▫vcs.modified=false
```

Verbatim tool output; only the leading file path was shortened to the file name. `go version -m` reads metadata and does not execute the binary. The upstream `go.mod` used for the comparison was not retained in the workspace; it is in the public Overlord repository (hxxps://github[.]com/vxaboveground/Overlord), where readers can compare `Overlord-Client/go.mod` and look for revision `056221e3`.

Exhibit E18-2. Wallet and browser-store markers in the implant

Artifact: Go implant (linux-amd64) · 15,790,242 bytes · SHA-256
`ef183bbb40f4c7c3f4b52994cdba3295f3eab2604fdad99eefa3b67b8d966e8d`
Location: whole-file string counts
Extraction: `for p in …; do grep -a -o -i -F "$p" overlord_go_implant_linux-amd64.elf | wc -l; done`
Supports: wallet and browser-collection markers that the comparison found absent from the selected upstream files

```
nkbihfbeogaeaoehlefnkodbefgpgknn   1
bfnaelmomeimhlpmgjnjophhpkkoljpa   1
metamask                           3
phantom                            3
exodus                             5
electrum                           4
Login Data                         7
Local State                        6
logins.json                        5
key4.db                            9
```

Counts of case-insensitive fixed-string matches. The first two values are the Chrome Web Store IDs of the MetaMask and Phantom wallet extensions. The upstream side of this comparison rests on the public repository, not on a retained copy.

Claims without a retained primary artifact

- The upstream Overlord files used in the July comparison (`Overlord-Client/go.mod`, configuration examples) were not saved; they are public, so the comparison can be repeated against the repository named in E18-1.

• That build revision `056221e3…` is absent from the public repository is a recorded July result; it depends on the repository's state at that time.

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.

Go implant (linux-amd64) · 15,790,242 bytes

`SHA-256 ef183bbb40f4c7c3f4b52994cdba3295f3eab2604fdad99eefa3b67b8d966e8d`

Source records and fingerprints

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

[S1] Framework comparison, 22 July 2026 · 10,772 bytes

`SHA-256 1f0d02347ae2bc952b31779cb0c5e946b0305daf6bd75f5b795000e2690e21f7`

[S2] Static capability re-examination, 24 July 2026 · 9,290 bytes

`SHA-256 75b0ac85d0d6dd6d7b68588a0618252369a5431c268e8f4b04f24a2f4d9f3117`