E01. Master investigation report

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.

Scope and material

The investigation began with three phishing messages received on 22 June and 21–22 July 2026. The corpus includes lures, delivery repositories, payloads, administration source and targeting databases. The evidence cutoff is 24 July 2026. This is an edited synthesis of the master record. [S1]

Delivery and collection

Two documented delivery mechanisms are a recruitment-page clipboard substitution and a repository-triggered editor-extension pipeline. These replace verification text with an installation command or deploy a VSIX masquerading as Google Update Support. Execution depends on permissions and platform conditions. A third, archive-based ECHOES strand retains staging and configuration history but lacks its final payload. [S1]

Recovered collection components reference browser databases, wallet material, developer credentials and a broader filename-based secret search. Windows source includes an elevation attempt and browser-decryption logic; capture-related artifacts support a screen-streaming capability assessment. None of these static observations establishes successful collection from a particular endpoint. E02–E05 and E17–E19 document these mechanisms.

Infrastructure, administration and targeting

A GitLab-hosted JSON resource provides C2 configuration separately from the deployed payload. Recorded history includes a July destination change. Historical observations associate distinct addresses with lure hosting, C2 and administration; these are dated service relationships rather than proof of exclusive ownership. Recovered frontend source contains mail metrics, delivery-repository status views and wallet-claim interfaces. Backend code and transaction evidence were not recovered with that frontend. [S1]

The two targeting pools contain 79,698 and 62,667 rows. Read-only verification recorded in the preprint gives 142,365 distinct stored address strings, no exact address overlap, and 27,698 distinct repository values. These are targeting-data measures, not counts of people, delivered messages, infections or financial losses. E08 specifies the aggregate queries and their limitations. [S2]

Corrections and evidentiary limits

The preprint qualifies several stronger statements in the master record. A resolver does not guarantee that every client follows every update. Capture symbols do not establish a recorded screen session. A frontend privilege check does not establish server-side authorization. Shared hosting does not establish a common operator, and build metadata does not locate a person. Equivalence with G1052 and real-world operator identity are not established. [S2]

The record distinguishes filed preservation requests from drafts. No new outreach, payload execution or infrastructure checks were performed to prepare this report. Withheld raw inputs limit independent replication.

Exhibits

E01 synthesizes the master record. Its mechanisms are exhibited in E02–E21, so this file adds a single artifact register: the key primary artifacts of the case, fingerprinted on 24 October 2026. Every artifact was hashed and sized only. Nothing was opened beyond `file`/`unzip -l`/`git bundle list-heads` type checks, and nothing was executed. Local paths are listed only in `E01.artifacts.json`.

Exhibit E01-1. Register of key primary artifacts

Artifact: 14 primary artifacts, listed in the block below (each line pair gives name, kind, bytes and SHA-256)
Location: whole files
Extraction: `sha256sum <artifact>; stat -c %s <artifact>` for each register entry, formatted by a helper that substitutes the descriptive name for the local path

Supports: "The corpus includes lures, delivery repositories, payloads, administration source and targeting databases"; "three phishing messages"

```
01 Lure email: Nodit recruitment message (rcvd 22 Jun 2026) · email · 7185 bytes
   6c1835159c8da69aaf0743fce634c3345e6b4f16eb4a492cfda5cf893b98eb5b
02 Lure email: D2S AI Trade recruitment message (rcvd 21 Jul 2026 UTC) · email · 9176 bytes
   3efb15d6cc89e3690bd1e19fbc96034110f55066d69ef25dc2d30ca057d2ee21
03 Lure email: Category Labs recruitment message (rcvd 22 Jul 2026 UTC) · email · 9462 bytes
   924db78f6fe47e7696c42d77d42d8f030c80e4a04965f7529731bfab4353d6ec
04 ClickFix lure-page JavaScript bundle · sample · 73545 bytes
   5ee915bb8d0363bd92176cc595d7425fd7e7830508d8824d90b5285a3d2b11bd
05 Stage-three JavaScript collection payload · sample · 1140214 bytes
   694626bed2df1f0d0026a3f7ead7692b44c7e73041cdd799b79a025335533cdc
06 Overlord Go implant, Linux x86-64 ELF · binary · 15790242 bytes
   ef183bbb40f4c7c3f4b52994cdba3295f3eab2604fdad99eefa3b67b8d966e8d
07 Windows Node agent archive (192 members) · sample · 603347 bytes
   be5859f23f0781242d854dc24c102c694dabfc14a159b56429e313f0521141b6
08 VSIX extension "Google Update Support" · sample · 17647582 bytes
   52886aab179f26421678ff23af1b0fabf0a17ffbb534369cdbbac8008cbed8e7
09 ECHOES archive (RAR v5) · sample · 2294526 bytes
   7db6789c09e29305c728bf3d7b94c5ef1c3e13eef1b321ee52d3ae3997731f56
10 ECHOES poster Post.png (C2PA) · image · 3698494 bytes
   d213b4184b93ccf59449237b071ac2e41ff71b83213b2e338917b26696a7b520
11 GitLab dead-drop configuration repository (git bundle) · repository · 4900 bytes
   804df377a0425d0aa7433ec2402d55ce8c913e1e4063d32565ddfda8ae807245
12 Administration frontend source, wallet-balances page · source · 109637 bytes
   f9b1b0c3e259d90ca35e827dc84cb137335b0a79420c532d4ffa0988bd994954
13 Targeting database, safe pool (SQLite) · database · 6922240 bytes
   a84cee4ce20e0d40177b750a2692acd37ae6cd30a4e303790c6eb1ecf6348187
14 Targeting database, antispam pool (SQLite) · database · 5496832 bytes
   7eff7dac7119b6b4462e685855a3e81269ecf9ecb1f392fa4e51282825d4429c
```

The digests are verbatim `sha256sum` output. The path column was replaced by a descriptive label; the "rcvd" dates come from each message's own `Date:` header (UTC). Other checks agree with this register:

- Entries 04–06 match the held-file hashes in the companion validation record (see E15).
- Entries 13–14 match the restricted packaging manifest of 22 October 2026.
- Entry 11 is a single-branch bundle (`refs/heads/main` at `c3c71d6…`).
- Entry 08 contains `extension/google-update-support-agent.zip` (17,283,435 bytes). The register is a fingerprint list, not a chain-of-custody attestation; acquisition times are not attested here.

Claims without a retained primary artifact

- The "July destination change" in the C2 configuration and the historical address/service relationships. These are covered by E07, E11 and E21. The dead-drop repository (entry 11) is retained; passive-DNS and hosting observations exist only as notes.
- "Filed preservation requests" versus drafts. The workspace holds drafts and dispatch notes, but no provider acknowledgement artifact was identified in this pass.
- Row and distinct-value counts for the targeting pools are not re-derived here. E08 owns those queries.

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.

Lure email: Nodit recruitment message (rcvd 22 Jun 2026) · 7,185 bytes

`SHA-256 6c1835159c8da69aaf0743fce634c3345e6b4f16eb4a492cfda5cf893b98eb5b`

Lure email: D2S AI Trade recruitment message (rcvd 21 Jul 2026 UTC) · 9,176 bytes

`SHA-256 3efb15d6cc89e3690bd1e19fbc96034110f55066d69ef25dc2d30ca057d2ee21`

Lure email: Category Labs recruitment message (rcvd 22 Jul 2026 UTC) · 9,462 bytes

`SHA-256 924db78f6fe47e7696c42d77d42d8f030c80e4a04965f7529731bfab4353d6ec`

ClickFix lure-page JavaScript bundle · 73,545 bytes

`SHA-256 5ee915bb8d0363bd92176cc595d7425fd7e7830508d8824d90b5285a3d2b11bd`

Stage-three JavaScript collection payload · 1,140,214 bytes

`SHA-256 694626bed2df1f0d0026a3f7ead7692b44c7e73041cdd799b79a025335533cdc`

Overlord Go implant, Linux x86-64 ELF · 15,790,242 bytes

`SHA-256 ef183bbb40f4c7c3f4b52994cdba3295f3eab2604fdad99eefa3b67b8d966e8d`

Windows Node agent archive (192 members) · 603,347 bytes

`SHA-256 be5859f23f0781242d854dc24c102c694dabfc14a159b56429e313f0521141b6`

VSIX extension "Google Update Support" · 17,647,582 bytes

`SHA-256 52886aab179f26421678ff23af1b0fabf0a17ffbb534369cdbbac8008cbed8e7`

ECHOES archive (RAR v5) · 2,294,526 bytes

`SHA-256 7db6789c09e29305c728bf3d7b94c5ef1c3e13eef1b321ee52d3ae3997731f56`

ECHOES poster Post.png (C2PA) · 3,698,494 bytes

`SHA-256 d213b4184b93ccf59449237b071ac2e41ff71b83213b2e338917b26696a7b520`

GitLab dead-drop configuration repository (git bundle) · 4,900 bytes

`SHA-256 804df377a0425d0aa7433ec2402d55ce8c913e1e4063d32565ddfda8ae807245`

Administration frontend source, wallet-balances page · 109,637 bytes

`SHA-256 f9b1b0c3e259d90ca35e827dc84cb137335b0a79420c532d4ffa0988bd994954`

Targeting database, safe pool (SQLite) · 6,922,240 bytes

`SHA-256 a84cee4ce20e0d40177b750a2692acd37ae6cd30a4e303790c6eb1ecf6348187`

Targeting database, antispam pool (SQLite) · 5,496,832 bytes

`SHA-256 7eff7dac7119b6b4462e685855a3e81269ecf9ecb1f392fa4e51282825d4429c`

Source records and fingerprints

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

[S1] Master investigation record · 65,312 bytes

`SHA-256 9f3736d9c68564553945d8427d0ba6d5b7cf12a92f559bc0d615ef2fd0e26bed`

[S2] Edited preprint manuscript · 54,752 bytes

`SHA-256 dc5d8abe46fcd33e9a28ccc859778e22ced661beff2d559a072bfb04f9d131dc`