E20. Historical origin-server observations

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.

Observation sources

The 23 July record combines Censys, Shodan and VirusTotal observations associated with `207.241.172[.]222`. The analyst queried research-service records rather than directly probing that host. The findings below describe the analyst's notes; the raw scan responses and certificate were not retained. The retained panel files were fetched from api.domatisc[.]ink, not the bare IP. They do not independently reproduce the reported direct-IP response or establish present service availability. [S1]

Certificate and content associations

The record reports an HTTPS certificate naming `api.cklomino[.]ink` and a direct-IP response containing a Subtensor sign-in panel. Panel markup and assets were compared with related observations. Other domain associations derive from certificate facets, reverse-DNS fields or passive DNS. Each relationship should retain its evidence type: a presented certificate, an observed resolution and matching content are not interchangeable proofs of control. [S1]

The certificate interval recorded as 13 July to 11 October 2026 dates that certificate's validity, not the campaign or tenancy. A matching interface can support a deployment association but can also be copied.

Service coverage

The saved enumeration lists SSH, HTTP and HTTPS. It cannot prove that no other ports or services existed outside the scan coverage. An empty vulnerability result does not establish a secure host, and a recent-looking software banner does not establish whether the machine was rented or compromised. [S1]

A host-key search reportedly returned only this address in the searched datasets. That is a bounded negative, not proof that no fallback or sibling host exists. Common OpenSSH banners and handshake fingerprints were recognized as weak discriminators because they occur widely.

Assessment

Certificate and panel-content observations strengthen the historical association of this address with the administration/C2 deployment. They do not prove exclusive tenancy, identify the person operating it or guarantee that blocking it would have no collateral effect. The source's descriptions of a sole origin and a decisive takedown point exceed the available evidence and are not adopted here.

No login, direct-origin request, fresh scan or current ownership check was performed for this evidence report. Domain and address values are historical, defanged research indicators.

Exhibits

Exhibit E20-1. Retained copy of the Subtensor operator sign-in panel

Artifact: Subtensor panel page (retained copy) · 3,665 bytes · SHA-256
`ed2ee1e1ba0c38ab0f0568326ef060c9a1543f27d30806c8b7a19a4627953b6d`
Location: lines 6, 24 and 43–50
Extraction: `sed -n '6p;24p;43,50p' subtensor_panel.html`
Supports: the Subtensor sign-in panel content compared with the origin observation

```
    <title>Subtensor — Sign In</title>
    <link rel="stylesheet" href="/assets/theme-bittensor.css" />
      <div class="brand login-brand brand-mark">Subtensor <span class="tau">τ</span></div>
      <h2 class="login-title">Operator Access</h2>
      <p class="muted login-subtitle">
        Decentralized intelligence infrastructure — secure entry for subnet validators and mi\
ners.
      </p>
      <form id="login-form">
        <div class="form-group">
          <label class="label">Operator ID</label>
```

Selected excerpt, with a display line break. This copy was retrieved from the operator host api.domatisc[.]link, not from the bare IP. The observation that `207.241.172[.]222` itself served this panel comes from a third-party scan record that was not exported (see below); exact content equivalence cannot be independently checked without that scan response.

Exhibit E20-2. The panel's sign-in request

Artifact: Panel login script (retained copy) · 6,380 bytes · SHA-256
`5557912dedf7f75666683afbe2632e0b89b8ee23f621432296a9c48eff63e9f4`
Location: lines 200–206
Extraction: `sed -n '200,206p' login.js`
Supports: the panel is an application front end that posts to its own API, giving an application-level association beyond the address

```
  }

  try {
    const res = await fetch("/api/login", {
      method: "POST",
      headers: { "Content-Type": "application/json" },
      body: JSON.stringify({ user: user.value, pass: pass.value }),
```

Verbatim; no credential or address appears in the span. The file's SHA-256 prefix `5557912d` is the one the origin note matches against the scanned panel.

Claims without a retained primary artifact

- The scan of the bare IP returning the panel, the certificate naming `api.cklomino[.]ink`, the certificate facets, passive DNS and reverse-DNS observations, and the SSH host-key and banner searches all come from research-service records (Censys and similar) that were viewed but not exported. Only the analysis note records them.
- The certificate itself was not saved, so its subject, SAN list and validity interval cannot be shown here.

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.

Subtensor panel page (retained copy) · 3,665 bytes

`SHA-256 ed2ee1e1ba0c38ab0f0568326ef060c9a1543f27d30806c8b7a19a4627953b6d`

Panel login script (retained copy) · 6,380 bytes

`SHA-256 5557912dedf7f75666683afbe2632e0b89b8ee23f621432296a9c48eff63e9f4`

Source records and fingerprints

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

[S1] Historical origin-server analysis, 23–24 July 2026 · 7,668 bytes

`SHA-256 234b2b355bb32644bf73d572d4850a45560e15006d0119d72ce317a248b7d48f`