E21. Build and hosting chronology

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.

Timestamp sources

The build-artifact record aligns mail-header times, domain-registration times, configuration commits, ZIP-entry timestamps and Go VCS metadata. These fields describe different events and have different precision and trust properties. The chronology is useful only when those distinctions are retained. [S1]

Recorded sequence

On 13 July 2026 the record places new domain registrations and a C2 configuration change. The retained Windows agent ZIP has three members dated 13 July and two package-lock members dated 20 July; its full member-date range is 18 June–20 July (Exhibit E21-3). These stored archive timestamps corroborate the note’s archive-date observations, but do not certify build times or prove one operator or one continuous session. [S1]

A phishing message is recorded at 01:08:32 UTC on 21 July. The Go binary records `vcs.time` as 01:14:06 UTC, five minutes and thirty-four seconds later. The latter is version-control metadata, not certified compiler output time. The original statement that compilation happened five minutes after mailing is therefore not supported by that field alone.

Archive interpretation

ZIP local timestamps must be distinguished from UTC extended fields and from the analyst's display timezone. Even a consistently recovered offset describes archive metadata, not physical location. Repackaging and deliberately set clocks remain alternatives. The Go trimpath setting removes path information but does not identify a build host or prove malicious anti-analysis intent by itself. [S1]

Hosting changes

An early infrastructure note centers on `23.137.105[.]75`, then adds `170.205.30[.]227` through overlapping historical domain observations. Later analysis identifies `207.241.172[.]222` for C2/administration and `170.205.31[.]182` for lure hosting. These notes must be read as successive observations, not simultaneous or exhaustive topology. The earlier single-host and dismantled-fleet descriptions are not evidence that all later activity ended. [S2, S3]

Assessment

A defensible chronology preserves the raw field, timezone semantics, source and event type. Resolution, registration, content retrieval and service disappearance are separate events. This report establishes recorded temporal associations, not an operator's location, certified build times, present availability or measured disruption.

Exhibits

Exhibit E21-1. Timestamps in the D2S AI Trade phishing message

Artifact: Phishing message as received (.eml) · 9,176 bytes · SHA-256
`3efb15d6cc89e3690bd1e19fbc96034110f55066d69ef25dc2d30ca057d2ee21`
Location: header lines 2–3, 59 and 63
Extraction: `sed -n '2,3p;59p;63p' message.eml`
Supports: a phishing message recorded at 01:08:32 UTC on 21 July

```
Received: by 2002:a05:7300:dc10:b0:30f:283c:acee with SMTP id ot16csp1833335dyc;
        Mon, 20 Jul 2026 18:08:36 -0700 (PDT)
Date: Tue, 21 Jul 2026 01:08:32 +0000
Subject: Engineering role at D2S AI Trade (remote)
```

Verbatim header lines; no address appears in them, and the other headers (including all addresses) are omitted. The sender's `Date` is 01:08:32 +0000; the first receiving hop logged 18:08:36 PDT, which is 01:08:36 UTC. Both are claimed times, not independently certified.

Exhibit E21-2. The Go implant's version-control time

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 | grep 'vcs\.'`
Supports: vcs.time 01:14:06 UTC, five minutes and thirty-four seconds after E21-1's Date header

```
▫build▫vcs.revision=056221e342357056c8539585806f76632660e414
▫build▫vcs.time=2026-07-21T01:14:06Z
▫build▫vcs.modified=false
```

Verbatim tool output (full output in E18-1). `vcs.time` is the commit time of the checked-out revision recorded by the Go toolchain; it is not a signed compile time, so it shows when the source revision was committed, not when the binary was built.

Exhibit E21-3. Windows agent ZIP member timestamps

Artifact: Windows agent bundle · 603,347 bytes · SHA-256
`be5859f23f0781242d854dc24c102c694dabfc14a159b56429e313f0521141b6`
Extraction: Python `zipfile.ZipFile(...).infolist()`; count `date_time[:3]` and inspect package-lock entries. No archive member was executed.
Supports: the archive-date observations, with no claim that these are certified creation or build times.

```
Member dates (stored local ZIP dates):
2026-06-18: 142
2026-06-21:   4
2026-06-24:   6
2026-06-26:  26
2026-06-29:   6
2026-06-30:   1
2026-07-02:   2
2026-07-13:   3
2026-07-20:   2
node_modules/.package-lock.json: 2026-07-20 21:15:32
package-lock.json:               2026-07-20 21:15:32
```

This corrects the previous exhibit’s incomplete 18–29 June range. The full listing includes July entries and supports the reported 20 July dependency-lock timestamp.

Claims without a retained primary artifact

- The 13 July domain registrations rest on the analysis note; the registry responses were not retained.
- The hosting sequence rests on passive-DNS and scan-service observations that were not exported. E20 contains retained panel files fetched from a domain, not a retained direct-IP scan response.

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.

Phishing message as received (.eml) · 9,176 bytes

`SHA-256 3efb15d6cc89e3690bd1e19fbc96034110f55066d69ef25dc2d30ca057d2ee21`

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

`SHA-256 ef183bbb40f4c7c3f4b52994cdba3295f3eab2604fdad99eefa3b67b8d966e8d`

Windows agent bundle (ZIP) · 603,347 bytes

`SHA-256 be5859f23f0781242d854dc24c102c694dabfc14a159b56429e313f0521141b6`

Source records and fingerprints

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

[S1] Build-artifact analysis, 22 July 2026 · 11,326 bytes

`SHA-256 b9bcb011e8e78bdf876fd2225956b27d263a86d3afd7c9f147619727a8e4b0ca`

[S2] Historical shared-host observations, 23 July 2026 · 5,533 bytes

`SHA-256 687bcb25909e7ee65b762110636f672e7039f3c83078f441343b297d98d3eac6`

[S3] Historical origin-server analysis, 23–24 July 2026 · 7,668 bytes

`SHA-256 234b2b355bb32644bf73d572d4850a45560e15006d0119d72ce317a248b7d48f`