E10. Repository-ownership reassessment

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.

Initial classification

An earlier analysis described `lautaro19/rekt-db` as victim-owned because it used a personal namespace and was an independent copy rather than a platform fork. The later record withdraws that classification. Namespace style and fork metadata cannot determine whether a repository belongs to a candidate or an operator. [S1]

Revised observations

The analysis note reports platform timestamps placing creation of that repository at 04:03:05 on 25 May 2026 and creation of a related `forge-4626-invariants` repository at 04:03:40, thirty-five seconds later. The record reports matching payload structure and a common cache-marker set, including `cleanup-paths`, `one-shot`, `use-extension-pipeline`, `vsix-rel` and `ws-hops`. Another related repository was created later that morning. [S1]

Timing proximity and matching artifacts make coordinated staging a plausible explanation. They do not make an independent clone impossible. The correct result is an ownership hypothesis requiring provider-side registration and access records, rather than an unconditional reversal from confirmed victim to confirmed operator.

Published-indicator comparison

Review of the complete published indicator table supplied repository paths and brand-domain mappings missing from an earlier summary. The record distinguishes exact task/settings hashes from structural selectors: a byte hash covers identical files only, while renamed or modified deployments require broader comparison. These are recorded comparison results; no public source or repository status was rechecked for this document. [S1]

Limits

The original repository snapshots and platform API responses supporting the ownership comparison are not retained with these exhibits. The quoted correspondence and analytical records document the reassessment, rather than independently reproducing its underlying observations.

Payload-bearing forks on established accounts remain exposure leads, but even a fork followed by later commits does not establish task execution, extension installation or compromise. Current availability cannot be inferred from July responses. The correction concerns attribution of repository ownership and the precision of incident communication, not a new count of infected developers.

Personal account details and the full historical sender roster are excluded. The retained repository identifiers are limited to explaining the specific reassessment cited by the preprint.

Exhibits

No primary artifact for this report is retained in the case workspace.

Claims without a retained primary artifact

- The repository creation times (04:03:05 and 04:03:40 UTC on 25 May 2026) came from GitLab API responses that were viewed but not saved. The only retained record of them is the author's own abuse report to GitLab of 22 July 2026, which is correspondence, not platform data.
- The matching payload structure and the shared cache marker rest on the repository contents as inspected in July; neither repository's files were kept.

- The published-indicator comparison relies on the public Proofpoint report, which readers can consult directly.

Source records and fingerprints

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

[S1] Repository-ownership correction, 22 July 2026 · 10,565 bytes

`SHA-256 9c412a09ff3cfa6d674d5b0bfd0833944949db5e50073b660795f67abe624a1d`