E16. Retraction of an earlier campaign attribution

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.

Withdrawn claim

A July analysis associated a domain family, mostly registered in September 2025, with the recruitment campaign based on hosting overlap, closely spaced registrations and persona-like subdomains. A subsequent review withdrew that earlier-phase attribution. The preprint does not extend the campaign timeline to September 2025 on this evidence. [S1]

Reassessment evidence

The record identifies a domain family with Portuguese-language consumer names, beauty-related naming and numbered mail-sender subdomains. Historical resolutions also connected the family to demonstrably shared hosting. Its observed activity preceded the July recruitment infrastructure by months. Batch registration and persona-style subdomains are not sufficiently distinctive to overcome those differences. [S1]

Counts of domains returned by a passive-DNS service reflect that service's coverage, not a complete tenant inventory. The earlier assertion that an address was dedicated because few domains appeared in one search was therefore unsupported. Shared provider space and later reuse of an address permit unrelated tenants and successive occupants.

Uncertainty in the alternative explanation

The retraction describes the family as consistent with affiliate or consumer spam. However, the source explicitly states that substantive page content was not recovered: one retained capture was empty and another was a connection-timeout page. The alternative business interpretation rests on naming, subdomains, mail patterns and hosting behavior. It should not be reported as direct observation of functioning affiliate pages. [S1]

Consequence

Positive evidence was insufficient to sustain the original campaign attribution, even without proving the exact alternative operation. The family and other weak co-residence leads should not be treated as campaign indicators on that basis. This withdrawal does not negate independently supported July payload, resolver or administration observations.

Limits

This report documents a correction to the analytical record. It does not prove that every third-party site in the hosting neighborhood was benign, and it makes no current infrastructure-status claim. Unrelated domains and personal-looking subdomain labels are omitted to avoid carrying the withdrawn attribution into a new indicator list.

Exhibits

No raw third-party query output for the withdrawn domain family is retained in the workspace. That means no VirusTotal, urlscan, Shodan, OTX or CertSpotter JSON, no WHOIS records and no page captures; a full-workspace search for the family's names finds them only in analysis notes. The exhibits below therefore come from the case repository itself: the git history that dates the attribution and its withdrawal, the attribution text as committed, and the retraction record as committed. They show *why* the claim was withdrawn as recorded at the time, not the underlying service responses. Redaction policy, following E16's own rule: domains of the unrelated family, persona-style subdomain labels, impersonated recruiter identities and other third-party sites are replaced with `[REDACTED: …]`. Operator-infrastructure IPs are defanged.

Exhibit E16-1. Commit timeline: attribution and withdrawal on the same morning

Artifact: case repository history (git) · commits `88dfe8fccc57d1c732e8fe6623aa8ee8cabd3e01`, `c6097e1497ee61a826273c348185f6cdd75467a3`, `f259302ee8f6e20a3f147e49b96a10ba8fa59066`
Location: commit metadata (author dates, subjects)
Extraction: `git log -n1 --format='%h %ad %s' --date=iso 88dfe8f; git log --format='%h %ad %s' --date=iso -- <retraction note> <persona-cluster scrub>`
Supports: "A July analysis associated a September 2025 domain family ... A subsequent review withdrew that earlier-phase attribution"

```
88dfe8f 2026-07-24 06:52:45 +0200 CORRECTION: origin co-residents are PROBABLE operator \
(earlier Sept-2025 NameSilo phase), not unrelated
f259302 2026-07-24 08:05:52 +0200 Sept-2025 NameSilo lead: characterised, attribution \
RETRACTED (unrelated Brazilian spam op)
c6097e1 2026-07-24 06:55:32 +0200 Record earlier-phase (Sept-2025 NameSilo) probable-operator \
IOCs in the cluster-scrub tiering
6078e61 2026-07-24 04:10:45 +0200 Persona-cluster scrub: tier confirmed-operator vs \
adjacent/innocent (pre-filing hygiene)
```

The attribution was committed at 06:52 and copied into the indicator tiering at 06:55. It was withdrawn at 08:05, 73 minutes later. The retraction note in the working tree is byte-identical to the copy in commit `f259302` (`git diff --quiet f259302 -- <note>` returns 0). Lines are hard-wrapped with `\`.

Exhibit E16-2. The withdrawn attribution as committed (three arguments)

Artifact: investigation log blob at commit `88dfe8f` · 127990 bytes · SHA-256 `8a8c7891b260b5f8b54710149f4a30fbe12e26a5e4214c4414cb62644c0650ff`
Location: lines 814–831 of `git show 88dfe8f:<investigation log>`
Extraction: `git show 88dfe8f:<investigation log> | sed -n 814,831p`
Supports: "associated ... based on hosting overlap, closely spaced registrations and persona-like subdomains"

```
### 2026-07-24 — Origin `170.205.31[.]182` sweep → EARLIER campaign phase found (corrected \
same day)
VT passive DNS (13 resolutions) on the lure-fleet origin. **Current (2026-07-23) set = \
exactly the known
…
**▫ CORRECTION (same day):** my first pass dismissed the 6 historical co-residents as \
"probably unrelated"
on **registrar grounds (NameSilo/Cloudflare ≠ Namecheap)** — that was **wrong** (the \
operator can use any
registrar). Re-checked: **(1)** the origin is essentially **dedicated** (only **13 domains \
ever** — a
shared box has hundreds); **(2)** the NameSilo set was **batch-registered** — \
`[REDACTED: unrelated domain]` & `[REDACTED: unrelated domain]`
created **1 second apart** (2025-09-22 20:31:47/:48), `[REDACTED: unrelated domain]` \
2025-09-29 — the operator's signature
batch-reg MO; **(3)** the subdomains are **fake-persona-at-fake-company** \
(`[REDACTED: personal-looking subdomain]`,
`[REDACTED: 3 personal-looking subdomains]`) — matching the
operator's recruiter-persona MO ([REDACTED: impersonated recruiter identities]). **So these are
PROBABLE operator infrastructure from an EARLIER campaign phase (Sept 2025, on NameSilo)** — \
extending the
campaign timeline back ~10 months. Confidence: **high** for the NameSilo batch set \
(dedicated origin +
batch-reg + persona pattern; content unconfirmed — dead, no Wayback), **moderate** \
`[REDACTED: unrelated domain]`
…
```

Lines 816–817 and 829–831 are elided with …. They list current campaign domain stems and the lower-confidence third-party domains. Note the three pillars: "dedicated" origin, batch registration, and persona-style subdomains. The hedge "content unconfirmed — dead, no Wayback" was present from the start.

Exhibit E16-3. Registration dates and naming of the withdrawn family

Artifact: retraction record (commit `f259302`) · 9494 bytes · SHA-256 `75d9ea47cfe375a03598f29892e184229bbc2ac0417bd19ec420d036399cc10d`
Location: lines 18–27 and 37–39
Extraction: `sed -n '18,27p;37,39p' <retraction note>`
Supports: "Portuguese-language consumer names, beauty-related naming and numbered mail-sender subdomains"

```
| domain | created | theme | persona subdomains |
|---|---|---|---|
```

```
| `[REDACTED: domain 1].autos` | 2025-09-22 | *[REDACTED: PT phrase and English gloss]* (PT) \
| 3 |
| `[REDACTED: domain 2].hair` | 2025-09-22 | hair | 6 |
| **`[REDACTED: domain 3].makeup`** ← new | 2025-09-22 | *[REDACTED: PT phrase]* (PT) | 11 |
| `[REDACTED: domain 4].cfd` | 2025-09-29 | — | 7 |
| **`[REDACTED: domain 5].skin`** ← new | 2025-09-29 | skin | 5 |
| `[REDACTED: domain 6].lease` | **2025-03-20** | *[REDACTED: PT phrase]* (PT) | 8 + 4 mail |

**40 fake-persona subdomains**, every one a Brazilian/Portuguese consumer name:
**The decisive tell:** `[REDACTED: domain 6].lease` also carries
**`sswmail51`, `sswmail66`, `sswmail172`, `sswmail5251`** — numbered bulk-mail-sender
subdomains. Combined with **beauty/cosmetics TLDs** (`.hair`, `.makeup`, `.skin`), **one
```

Second-level labels and the Portuguese theme glosses are redacted because they spell the domain names. TLDs, dates and counts are kept. Lines 28–35 (the 40 personal-looking labels) are omitted entirely. Note that one family member was registered on 2025-03-20, not in September 2025.

Exhibit E16-4. The contradicting observations: shared hosting and an eight-month gap

Artifact: retraction record (commit `f259302`) · 9494 bytes · SHA-256
`75d9ea47cfe375a03598f29892e184229bbc2ac0417bd19ec420d036399cc10d`
Location: lines 51–61 and 81–88
Extraction: `sed -n '51,61p;81,88p' <retraction note>`
Supports: "Counts ... reflect that service's coverage"; "demonstrably shared hosting"; "activity preceded the July recruitment infrastructure by months"

```
### 1. "The origin is essentially dedicated — only 13 domains ever" ▫ false premise
That "13" is an artifact of **VirusTotal passive-DNS coverage**, not a property of the host.
Two independent checks contradict it:

- The same Brazilian family **also resolved to `170.205.30[.]8`**, which is demonstrably
  **shared hosting**: alongside `[REDACTED: persona subdomain]` and
  `[REDACTED: persona subdomain]` it hosts `[REDACTED: third-party site]` (2023-11),
  [REDACTED: five unrelated third-party sites] — a
  years-long run of unrelated, mostly Chinese-language sites.
- Both surrounding ranges are dense multi-tenant space: Shodan counts **544 services on
  `170.205.31[.]0/24`** and **489 on `170.205.30[.]0/24`**.
- **Timeline.** The Brazilian activity on `170.205.31[.]182` runs **2025-10-30 → 2025-11-05**.
  The operator's lure fleet appears there on **2026-07-23** — an **eight-month gap**, ample
  time for a budget VPS to be re-let.
- **Apexes were parked, not operated.** `[REDACTED: domain 1]`, `[REDACTED: domain 2]` and \
`[REDACTED: domain 4]`
  all resolved to **`91.195.240[.]123`**, a mass **domain-parking** IP currently serving 40+
  unrelated junk domains ([REDACTED: two third-party domains],
  [REDACTED: third-party domain], assorted slot/gambling sites). Only the persona *subdomains*
  ever pointed at Advin. That is a domainer/affiliate pattern, not C2 infrastructure.
```

IPs are defanged. The third-party sites co-hosted on the shared address and the parking IP are redacted, because naming them would create a new unrelated indicator list. Lines 62–80 are not shown, so the two ranges are joined without a separator. One line is hard-wrapped with `\`.

Exhibit E16-5. Recorded limit: page content was never recovered

Artifact: retraction record (commit `f259302`) · 9494 bytes · SHA-256
`75d9ea47cfe375a03598f29892e184229bbc2ac0417bd19ec420d036399cc10d`
Location: lines 143–150
Extraction: `sed -n 143,150p <retraction note>`
Supports: "substantive page content was not recovered: one retained capture was empty and another was a connection-timeout page"; the alternative explanation is inferred

```
**Honest limit: page content was never recovered.** urlscan[.]io holds exactly two captures for
this entire family — `[REDACTED: domain 4]` (2025-10-02, empty) and `[REDACTED: persona \
subdomain]`
(2025-11-05), and the latter is a **1.4 KB Cloudflare 522 "Connection timed out" shell**, not
the site. The domains are dead with no Wayback coverage. So the *specific* affiliate content
is inferred from the domain/TLD/persona/mail-sender/parking pattern rather than observed
directly. That inference is strong enough to withdraw an attribution — which requires
positive evidence to sustain — but it is not the same as having seen the pages, and it should
not be written up as though it were.
```

The service name is defanged and the domains are redacted. The source text says "urlscan holds". The bracketed `[.]` was inserted only to defang a hostname-like token.

Claims without a retained primary artifact

- All passive-DNS, resolution, registration-date, VirusTotal category and Shodan-count observations (Exhibits E16-3 and E16-4). They are recorded in the analysis note only. No service response, WHOIS record or export file is retained, so none of these values can be re-derived from workspace bytes.
- The two urlscan captures (empty page; 1.4 KB Cloudflare 522 shell). They are described but not retained.
- The July 2026 appearance of the operator's lure fleet on the same origin (2026-07-23). That date is again a passive-DNS observation recorded in notes; no resolution data is retained.

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.

Investigation log as committed with the earlier-phase attribution · 127,990 bytes

`SHA-256 8a8c7891b260b5f8b54710149f4a30fbe12e26a5e4214c4414cb62644c0650ff`

Retraction record as committed · 9,494 bytes

`SHA-256 75d9ea47cfe375a03598f29892e184229bbc2ac0417bd19ec420d036399cc10d`

Source records and fingerprints

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

[S1] Earlier-phase retraction, 24 July 2026 · 9,494 bytes

`SHA-256 75d9ea47cfe375a03598f29892e184229bbc2ac0417bd19ec420d036399cc10d`