E09. Deployment and mail-guide analysis

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.

Source and acquisition

The 23 July record describes an HTML guide retrieved through the unauthenticated route loaded by the administration frontend. The guide covers server setup, business email configuration, GitHub-user collection and spam-filter troubleshooting. No authenticated mailbox or administration API was queried in that acquisition record. This report relies on the saved analysis. [S1]

Mail-provider evidence

Example DNS configuration refers to Namecheap Private Email. The associated sender tooling uses `mail.privateemail.com`, although some variable names contain ZOHO. A variable label is therefore insufficient to identify the actual provider. The case record links a discussed outbound relay to shared Private Email infrastructure. Other tenants on that relay cannot be attributed to the campaign merely through co-residence. [S1]

Later received-message records contain Mailgun-related evidence. That is compatible with different providers across messages or periods. The guide's deliverability discussion is not proof of why a provider changed, nor of which provider handled every campaign message.

Workflow evidence

The guide describes GitHub API and web-based user collection and includes generic domain, server and email setup instructions. This is consistent with reusable recruitment operations. Sender configuration and the harvester provide more direct evidence of the collection-to-messaging relationship than the guide alone; E08 covers those artifacts.

The record identifies text resembling copied assistant output in the troubleshooting section. Such text supports a limited observation about the document's composition. It does not identify its author, quantify reliance on AI, measure technical skill or establish the number of operators. Second-person instructions can be written for oneself as well as a team.

Assessment

Provider attribution should follow configured endpoints and received headers. Shared relay addresses are contextual infrastructure observations, not campaign-exclusive indicators. The guide describes intended procedures, not verified execution of them. Recovered account values and operational credentials are omitted, and no provider status or network observation was refreshed for this report.

Exhibits

Exhibit E09-1. The guide is loaded by an unauthenticated fetch

Artifact: rms-platform admin client — `GuidePage.tsx` · 7950 bytes · SHA-256
`1b0fb8d05894eb3fda903005cc09521bdc8a63bcf323530db123d1cfe3dbb787`
Location: lines 12, 22-24
Extraction: `sed -n '12p;22,24p' GuidePage.tsx`
Supports: E09 "an HTML guide retrieved through the unauthenticated route loaded by the administration frontend".

```
import { ADMIN_HOST } from "/src/api/admin.tsx";
        fetch(`${ADMIN_HOST}/guide/`).then((response)=>{
            if (!response.ok) throw new Error("Failed to load guide");
            return response.text();
```

A raw `fetch` to `/guide/` (not the JWT `adminBase` instance), so the endpoint is public; no authenticated mailbox or admin API is queried. No redaction applied.

Exhibit E09-2. Guide sections: server setup, business email, GitHub collection, spam filtering

Artifact: operator runbook — `guide.html` · 13192 bytes · SHA-256
`918b9e4f132bea24215fdb5005e6ac32e61cc745fc9318a81b2f801981f64746`

Location: `<h1>` headings at lines 37, 117, 196, 268, 355

Extraction: `grep -n '<h1>' guide.html`

Supports: E09 "covers server setup, business email configuration, GitHub-user collection and spam-filter troubleshooting".

```
<h1>How to Set Up a Virtual Private Server (VPS)</h1>
<h1>How to Get a Business Email</h1>
<h1>Logic for Scraping GitHub Users</h1>
<h1>To <strong>fix this Gmail block</strong> and ensure successful delivery, ...</h1>
<h1>Reference Links</h1>
```

The four topical sections match the report. No redaction applied to headings.

Exhibit E09-3. Example DNS points at Namecheap Private Email

Artifact: operator runbook — `guide.html`

Location: lines 349-353

Extraction: `sed -n '349,353p' guide.html`

Supports: E09 "Example DNS configuration refers to Namecheap Private Email ... `mail.privateemail[.]com`".

```
hostname    Record type Priority    Value
@   MX  10  mx1.privateemail[.]com
@   MX  10  mx2.privateemail[.]com
@   TXT     v=spf1 include:spf.privateemail[.]com ~all
_dmarc   TXT    v=DMARC1; p=reject
```

Persona mail is configured for Namecheap Private Email (MX/SPF), with `_dmarc p=reject`. URLs defanged. The sender tooling's host `mail.privateemail[.]com` (with any username/password [REDACTED]) is corroborated by this DNS, though the report notes some sender variable names contain ZOHO — a label, not provider proof.

Exhibit E09-4. Spam-filter section contains verbatim copied assistant output

Artifact: operator runbook — `guide.html`

Location: lines 284, 300, 343, 347 (first-person assistant phrasing)

Extraction: `grep -n -E 'I can help|if needed|Would you like me' guide.html`

Supports: E09 "text resembling copied assistant output in the troubleshooting section".

```
If you're unsure how to set them up, I can help you generate the correct DNS records ...
If you'd like, I can show you how to route your emails via Gmail SMTP or another service.
Use it in PHPMailer or your email-sending script — I can help set that up if needed.
Would you like me to generate the correct DNS records or show you how to switch to Gmail SMTP ...
```

First-person assistant offers pasted into the runbook support a limited observation about the document's composition only; they do not identify an author or measure skill. No personal data present in these lines. Note: the guide's own example `[email protected]` placeholders are Cloudflare-obfuscated in the source and carry no real address.

Claims without a retained primary artifact

- The operator mail-sending IP and its PTR/relay enumeration, and the Mailgun-related evidence in "later received-message records": these are analysis-note findings (`GUIDE-operator-runbook.md`, mail maps). The three retained genuine lure `.eml` files (the retained message set) route via SimpleLogin forwarding and do not themselves carry the Private Email relay or a Mailgun header, so they neither confirm nor contradict the provider narrative and are not cited as E09 exhibits.
- Account values and operational credentials: the report states these are omitted; none 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.

rms-platform admin client — GuidePage.tsx · 7,950 bytes

`SHA-256 1b0fb8d05894eb3fda903005cc09521bdc8a63bcf323530db123d1cfe3dbb787`

Operator internal runbook — guide.html (unauthenticated /guide/ body) · 13,192 bytes

`SHA-256 918b9e4f132bea24215fdb5005e6ac32e61cc745fc9318a81b2f801981f64746`

Source records and fingerprints

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

[S1] Deployment and mail-guide analysis, 23 July 2026 · 5,396 bytes

`SHA-256 8cf0e86faba0d7ce95bd325ea1f81f528c5a2a843d0149721fcc155050fc4b6e`