

Is pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev a scam?

TrustSniffer's high-risk assessment: 5/100

pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev

Verdict

5

OUT OF 100

CRITICAL RISK

pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev shows high-risk / scam indicators.

This assessment found strong scam indicators. Do not pay, sign in, or share personal details with this site.

Sensitive Interaction Risk

Governance Risk

Assessed 2026-10-01 by automated analysis. Classification confidence 75%.

What this site appears to be

Object-storage 404 error page indicating the requested object is not publicly accessible. No forms, third-party links, or monetization present.

Evidence status and limitations

Evidence completeness: UNKNOWN

- The real-world operator identity was not independently verified.
- Module-level completeness metadata is unavailable for this legacy report.

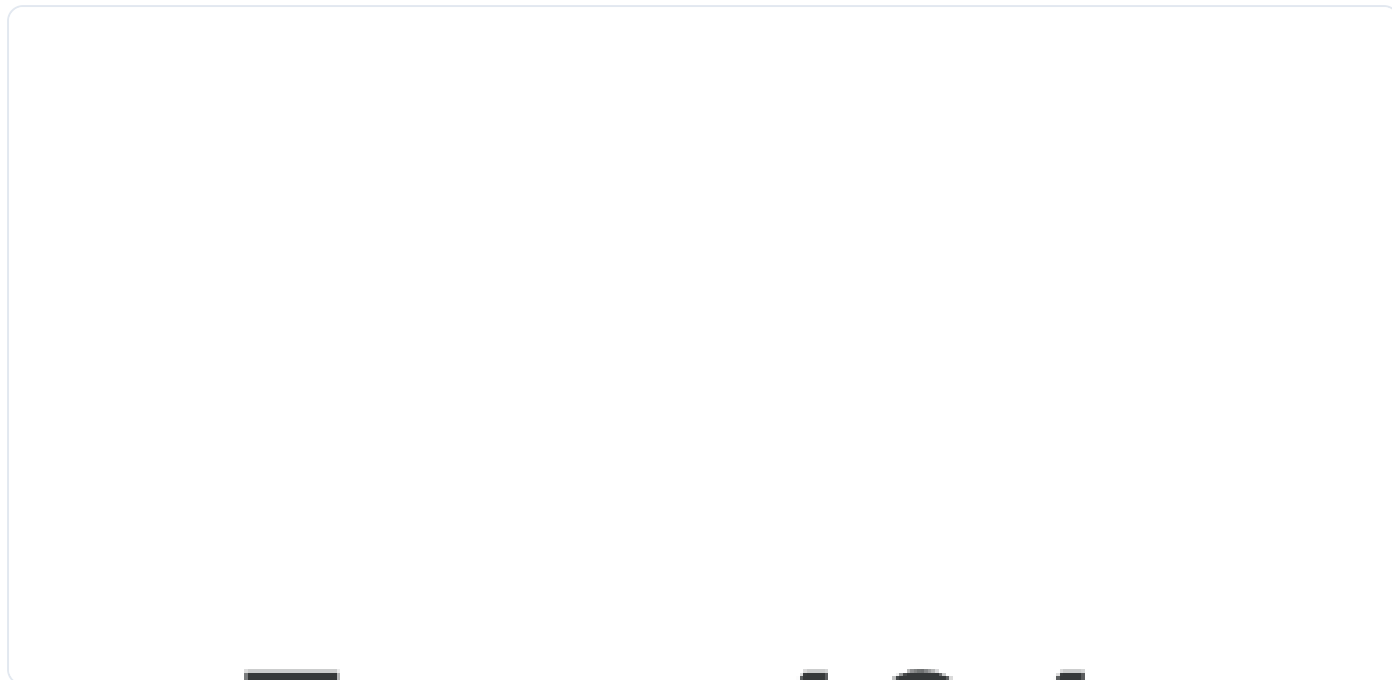
At a glance

The checks that decide most of this verdict.

Malware engines	13 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0% confidence AbuseIPDB, 1 report; shared hosting inflates reports	CLEAR
Domain age	2 months old Most scam domains are under a year old	RISK
Web archive	6 snapshots 6 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

<https://pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev/>



What pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev served when TrustSniffer captured it on 2026-10-01. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

Full analysis

Security Alert

Fortinet, Kaspersky, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website presents only a static object-storage “404 Not Found” page stating that the requested object does not exist or is not publicly accessible. It provides no identifiable commercial purpose, products, account functions, payment flows, or other substantive business content.

Scam/Impersonation Risk

The site has a **critical sensitive-interaction risk posture** because the hostname is listed by external blacklist sources and was classified as malicious by 13 evaluated security engines, including Fortinet, Kaspersky, and Sophos. These detections are materially inconsistent with the otherwise neutral appearance of the 404 page and constitute confirmed external threat indicators; no brand impersonation or phishing form was observed on the captured page itself. A separate abuse report associated with shared Cloudflare infrastructure is discounted because it applies to a provider edge address rather than being attributable to this site. The site’s apparent

operator identity is unverified, and the available evidence does not support credential, login, or financial interaction.

EVIDENCE

- The external reputation assessment recorded 13 malicious detections, with Fortinet, Kaspersky, and Sophos among the flagged vendors.
- The hostname was recorded as present on external blacklist sources; the captured homepage nevertheless displayed only “Not Found / Error 404 / Object not found.”
- The hostname was registered 0.12594113620807665 years ago, and archive coverage records 6 snapshots across 1 year tracked.

Regulatory Verification Notes

The captured site does not provide a legal entity name, licensing statement, registration number, terms, privacy notice, or other governance disclosure; this is a substantive transparency gap because the only accessible content is an object-storage error page. No regulated-business claim is presented, and no broker-dataset match was identified. This absence does not independently establish fraud, but in combination with the confirmed external threat detections and unverified operator identity, it prevents meaningful regulatory or legal-entity validation.

EVIDENCE

- The homepage is an object-storage error page with 283 characters of text and no forms, business disclosures, or transactional content.
- The page title is “Not Found,” with no detected description, canonical identity information, or structured business metadata.
- The site’s transport certificate is a DV certificate issued by YE1 and is valid through 2026-12-06.

What to Verify Next

Before any sensitive interaction, an organization should identify the intended legal operator through an independent corporate or regulatory registry and confirm that the hostname is an officially documented domain for that operator. Any proposed service relationship should also be validated through an independently sourced contact channel and assessed using a controlled, isolated environment; credentials, payment details, wallet access, and downloads should not be provided to this hostname unless the external detections are resolved and the operator is independently authenticated.

EVIDENCE

- The captured page contains no login form, sensitive form, payment mechanism, or user financial flow to validate.
- Browser analysis recorded no wallet connection, wallet-sensitive operation, wallet drainer, clipboard hijack, or hidden form.
- The page identifies only an inaccessible object and instructs visitors to check the object URL or contact the owner.

Summary Verdict

The overall posture is critical and clearly unsuitable for sensitive interaction. The available evidence supports treating the site as an untrusted, high-risk endpoint rather than as an established service, with the external threat detections outweighing its otherwise limited informational page content.

Infrastructure Integrity

The site is served through Cloudflare's CDN/WAF infrastructure, with all observed addresses belonging to CDN edge servers and no origin server address observable in this analysis. This provides a degree of exposure mitigation but does not validate the site's operator or offset the external threat indicators; CDN edge infrastructure can also support rapid content changes and shared-address attribution.

EVIDENCE

- Hosted on AS13335, CLOUDFLARENET — Cloudflare, Inc., US; observed edge address: 104.18.50.34.
- The infrastructure record identifies 4 CDN edge IPs and 0 likely origin IPs.
- TLS certificate issuer: YE1; validation level: DV; valid to 2026-12-06T05:31:56+00:00.

Closing Assessment

The appropriate action is to avoid login, credential submission, financial activity, and downloads through this hostname unless independent operator validation and remediation of the external threat detections have been completed.

Written analysis generated 2026-10-01 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

5 findings contributed to this verdict, raised by governance, page content, external reputation, behaviour in a sandbox, hosting and network.

01 Governance

- What the site offers, as described on its own pages, limits how high the score can go until more of it can be verified.
Governance rule:gov_business_model_cap
- A confirmed external threat listing caps the score at the bottom of the scale.
Governance rule:gov_external_blacklist_kill_switch

02 Page content

- The page has very little readable content.
Page content rule:PAGE_CONTENT_THIN

03 External reputation

- A widely visited domain carries an external threat flag, which calls for a closer look rather than a conclusion on its own.

External reputation rule:EXT_BLACKLIST_HIGH_RANK_REVIEW

04 Behaviour in a sandbox

- Most of what the page loaded came from other domains rather than from this one.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH

05 Hosting and network

- The domain was registered less than three months ago.

Hosting and network rule:DNS_NEW_DOMAIN_90D

Signals weighed against the site

- AbuseIPDB: 1 report on hosting IP 2606:4700:311b::6812:3222 (Cloudflare, Inc., Content Delivery Network), 0% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	50%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev.

- The request stayed on pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev. It was not redirected to another domain. [CLEAR](#)
- It is hosted on CLOUDFLARENET, from a server in US. [NOTED](#)

Domain intelligence

Registrar	Not available
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:311b::6812:3222
Name servers	Not available

CDN / edge network	Detected (cloudflare)
Resolved IP addresses	4
Edge IP addresses	4
Likely origin IP addresses	0
SSL issuer	YE1
SSL expiry	2026-12-06
Domain age	0.13 years (continuous registration)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	6
Reputation	VirusTotal: 13 flagged AbuseIPDB: 0% confidence, 1 report Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/pub-a06eb79f0ebe4a6999bcc71a2227d8e3.r2.dev> · assessed 2026-10-01