

Is pub-8d59738861b849e5a38b795cc17b1019.r2.dev a scam?

TrustSniffer's high-risk assessment: 5/100

pub-8d59738861b849e5a38b795cc17b1019.r2.dev

Verdict

5

OUT OF 100

CRITICAL RISK

pub-8d59738861b849e5a38b795cc17b1019.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 2026-09-22 by automated analysis. Classification confidence 55%.

What this site appears to be

A 404 error page indicating an object or bucket is not publicly accessible. The page suggests checking the URL or enabling public access; no forms 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.

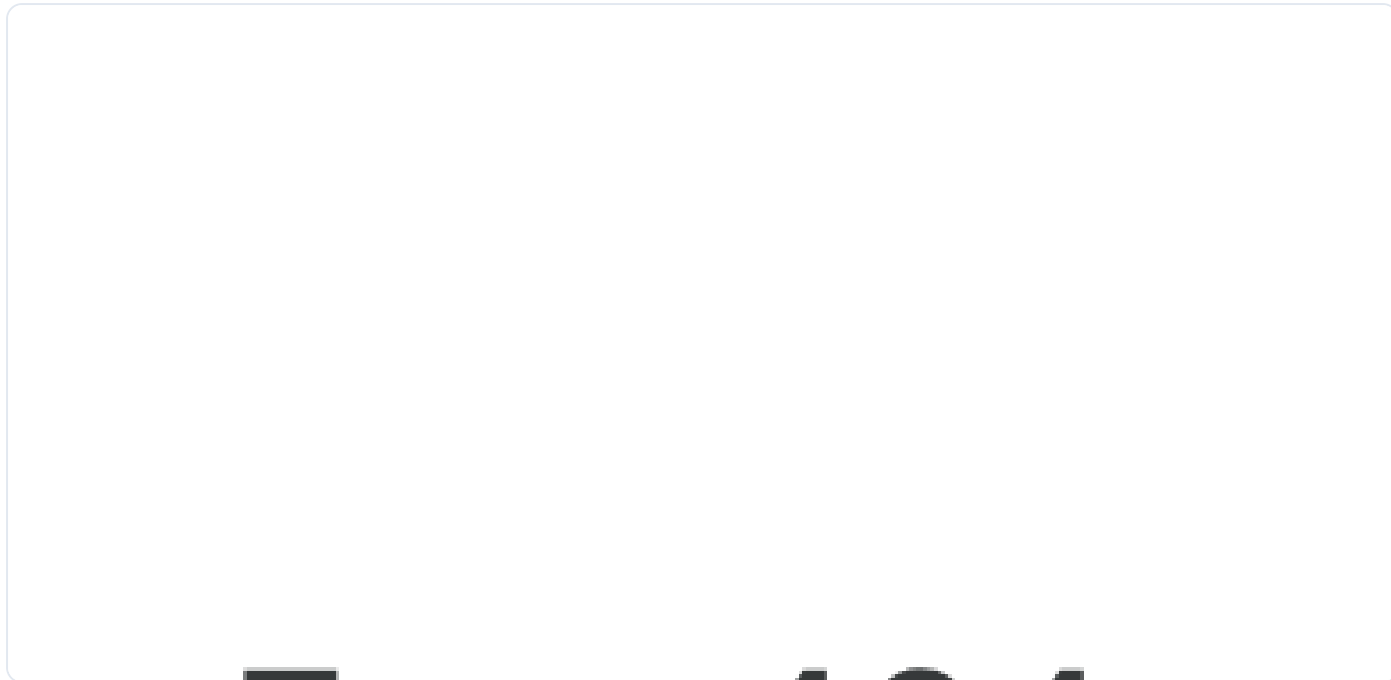
At a glance

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	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

<https://pub-8d59738861b849e5a38b795cc17b1019.r2.dev/>



What pub-8d59738861b849e5a38b795cc17b1019.r2.dev served when TrustSniffer captured it on 2026-09-22. 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.

This website currently presents only a “Not Found” object-storage error page, indicating that the requested object is unavailable or not publicly accessible; it does not present a commercial service, financial product, credential workflow, or stated business purpose to visitors.

Scam/Impersonation Risk

The site carries a clearly cautionary risk posture because external security intelligence recorded 13 malicious detections and one suspicious detection, with the domain also appearing on confirmed blacklist sources. These signals materially outweigh the otherwise benign content of the captured page. No brand impersonation, phishing form, or identity contradiction was observed on the page itself, and a single abuse report associated with shared Cloudflare infrastructure is discounted because it applies to a common CDN address rather than being attributable to this site. The operator identity remains unverified, so the available evidence does not establish who controls the endpoint.

EVIDENCE

- External security assessment recorded 13 malicious detections and 1 suspicious detection for the domain; Fortinet, Kaspersky, and Sophos were among the flagged vendors.
- The captured homepage returned a standard 404 object-storage message with no login form, sensitive form, payment request, or monetization mechanism.
- Domain registration continuity indicates an age of 72 days (~0.20 years).

Regulatory Verification Notes

The captured site does not provide an operating entity, legal identity, licensing statement, registration number, or regulatory disclosure. Because the page is only an object-access error, this is a verification and transparency gap rather than evidence of a regulated financial business. No broker match was identified in the available third-party context. The transport layer is technically valid, but domain-validated encryption confirms connection security only and does not authenticate the operator or establish authorization to conduct regulated activity.

EVIDENCE

- The captured page title is “Not Found,” and its text provides only object-access and public-access instructions rather than legal or regulatory information.
- The site is hosted on AS13335, CLOUDFLARENET — Cloudflare, Inc., US.
- TLS is issued by YE1 at DV validation level and is valid through 2026-12-06.

What to Verify Next

Before any sensitive interaction, an independent party should establish the responsible operator, confirm any claimed authorization directly with the relevant regulator or registry, and validate that the intended service is being delivered through an independently confirmed official domain. Contact channels and ownership claims should be confirmed through an offline or independently sourced route rather than relying solely on information presented by the endpoint.

EVIDENCE

- The captured site does not expose a usable business, legal, or account workflow against which operator claims can be validated.
- The available identity-verification evidence does not independently connect the endpoint to a real-world organization or person.
- The page contains no product, service, licensing, or ownership disclosures that would support a direct regulatory validation.

Summary Verdict

The overall posture is **critical trust risk** with a substantial risk to sensitive interactions. The available evidence is not sufficient to establish a legitimate operator, and the confirmed external threat signals require the endpoint to be treated as untrusted.

Infrastructure Integrity

Cloudflare CDN/WAF protection provides a mitigating network-control layer, but it is not proof of legitimacy. Observed resolution was limited to Cloudflare edge infrastructure, with no origin candidate identified; this limits independent assessment of the underlying host and could permit rapid changes in served content.

EVIDENCE

- The site resolved through four observed Cloudflare edge addresses, with no likely origin address identified.
- Hosting infrastructure is associated with Cloudflare’s AS13335 network and uses Cloudflare CDN/WAF protection.

Closing Assessment

Sensitive actions should not proceed through this endpoint unless the operator, authorization, and intended destination have first been independently confirmed through trusted channels.

Written analysis generated 2026-09-22 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by registration and ownership, analysis engine, behaviour in a sandbox.

01 Governance Risk

- The public registration record for this domain is incomplete.
Registration and ownership rule:KF_WHOIS_INCOMPLETE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH

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-8d59738861b849e5a38b795cc17b1019.r2.dev`.

- The request stayed on `pub-8d59738861b849e5a38b795cc17b1019.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
SSL issuer	YE1
SSL expiry	2026-12-06
Domain age	0.20 years (continuous registration)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
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-8d59738861b849e5a38b795cc17b1019.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.