

Is api-relay.cc a scam? TrustSniffer's high-risk assessment: 0/100

api-relay.cc

Verdict

0

OUT OF 100

CRITICAL RISK

api-relay.cc 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 2026-09-18 by automated analysis. Classification confidence 55%.

What this site appears to be

The page is a minimal JSON error response: {"detail":"Not Found"}. No links, forms, or monetization detected.

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	1 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	1 days old Most scam domains are under a year old	RISK
Web archive	Archived since 2026 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YE1	NOTED

The page as captured

<https://api-relay.cc/>

Pretty-print ☐

```
{"detail": "Not Found"}
```

What api-relay.cc served when TrustSniffer captured it on 2026-09-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- Public web-archive history exists since 2026.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

api-relay.cc presents a minimal JSON “Not Found” response rather than a functioning public website, with no visible service interface, business explanation, links, forms, or monetization; its apparent purpose cannot be established from the observed page.

Scam/Impersonation Risk

The site has a **confirmed blacklist finding**, which is the decisive adverse signal and warrants a security-forward posture for sensitive interactions. External reputation checks also recorded one malicious and one suspicious detection, although no direct brand impersonation, login form, phishing form, or malicious browser behavior was observed in the captured page. The available evidence does not establish a real-world operator identity, and the domain’s extremely recent registration provides little operating history against which the blacklist finding could be contextualized.

EVIDENCE

- External reputation results mark api-relay.cc as blacklisted and record one malicious and one suspicious detection.
- Registration records show creation on 2026-09-16 and an age of approximately 0.00 years.
- Historical records contain 2 archive snapshots spanning 2026–2026, with 1 year tracked.
- The homepage capture returned HTTP 404 content and contained no login form, sensitive form, external submission, wallet connection, or clipboard activity.

Regulatory Verification Notes

No license claim, registration number, or identifiable legal-entity disclosure is present in the supplied site content. This is a regulatory-transparency gap rather than, by itself, proof of misconduct; however, the absence of a functioning service or legal-information presentation prevents meaningful validation of what entity, if any, operates the domain. The observed transport security is a technical control only and does not validate licensing or operator identity.

EVIDENCE

- The observed site content contains no stated license authority, license number, or regulated-entity disclosure.
- The TLS certificate uses DV validation, was issued by YE1, and is valid to 2026-12-15T17:00:52+00:00.
- The available third-party broker-reputation dataset returned no matching broker record.

What to Verify Next

Before any credential, account, payment, or other sensitive interaction, the domain should be independently connected to a known legal entity through an authoritative corporate or regulatory registry. Any claimed authorization should be checked directly with the relevant regulator, and official support or contact channels should be confirmed through an independent, offline source. The domain should not be treated as an operational service until its intended function and ownership are clearly established.

EVIDENCE

- The homepage provides only a “Not Found” response, leaving the intended service and operating entity unconfirmed.
- The site content contains no visible links, forms, service description, or identity documentation.
- The available identity-verification evidence does not independently connect the domain to a real-world organization or person.

Summary Verdict

The overall posture is **critical risk for sensitive interaction**. A confirmed blacklist signal, unverified identity, minimal non-functional content, and lack of meaningful operating context converge on a conclusion that the domain should not be trusted for credentials, financial activity, or account access.

Infrastructure Integrity

The website is protected by Cloudflare’s CDN/WAF, and all observed addresses were CDN edge servers rather than an exposed origin. This reduces direct infrastructure exposure but is only a mitigating technical characteristic and cannot offset the adverse external reputation evidence.

EVIDENCE

- Served from AS13335 (CLOUDFLARENET - Cloudflare, Inc., US).
- Observed edge addresses were 104.21.62.184, 172.67.138.37, 2606:4700:3030::ac43:8a25, and 2606:4700:3032::6815:3eb8.
- Four unique edge IPs were observed, with 0 likely origin IPs identified.

Closing Assessment

Sensitive interaction with the domain should be withheld unless independent identity, authorization, and operational purpose are first established through authoritative channels.

Written analysis generated 2026-09-18 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.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	25%

- 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 api-relay.cc.

- The request stayed on api-relay.cc. It was not redirected to another domain. CLEAR
- Registration is published under NameSilo, LLC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-09-16. NOTED
- The earliest public archive of this site is from 2026-09-17. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NameSilo, LLC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3032::6815:3eb8
Name servers	ALDO.NS.CLOUDFLARE.COM, TERESA.NS.CLOUDFLARE.COM
SSL issuer	YE1
SSL expiry	2026-12-15
Domain age	0.00 years (continuous registration)
Domain expiry	2027-09-16
Archive first seen	2026-09-17
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 1 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about api-relay.cc 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.