

Is 1056787.com a scam? TrustSniffer's high-risk assessment: 0/100

1056787.com

Verdict

0

OUT OF 100

CRITICAL RISK

1056787.com 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 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

A short Chinese/English navigation page offering selectable 'access routes' or 'lines' (线路) and a continue button; functions as an interstitial/redirect with minimal descriptive content or calls for payment.

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	17 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	2.3 years old Registered history	CLEAR
Web archive	Archived since 2024 15 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

https://1056787.com/



What 1056787.com served when TrustSniffer captured it on 2026-08-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 1 to 3 years (registration continuity).
- Public web-archive history exists since 2024.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

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 is a minimal Chinese/English navigation interstitial that presents selectable access routes, including a recommended and a backup line, followed by a continue action. Its apparent purpose is to redirect visitors to an onward destination rather than provide a substantive commercial, financial, or informational service.

Scam/Impersonation Risk

Confirmed external threat indicators create a **critical risk posture** despite the absence of a login form, payment request, or explicit brand-impersonation signal on the captured page. The domain has a confirmed blacklist hit, with multiple malicious detections from external security services; this is materially stronger than the page-level content assessment, which found only a low-context navigation screen. The page also generated non-whitelisted external requests and posts during interaction, increasing uncertainty about the destinations and functions behind the route-selection controls. The historical record does not indicate suspicious repurposing, but the registration chronology and archival chronology are inconsistent, so provenance should not be treated as established.

EVIDENCE

- External reputation checks recorded 17 malicious detections, a blacklist hit, and tier-one detections associated with Fortinet, Kaspersky, and Sophos.
- The registration record identifies Zname Ltd and records creation on 2026-07-15T18:05:11Z, with an age of 0.09 years; the archival record separately reports domain_age_years of 2.302532511978097.
- Web archives contain 15 snapshots spanning 2024-04-28T11:19:12Z through 2025-04-16T17:28:16Z, covering 2 years.
- The homepage exposed 2 external XHR requests and 2 external POST requests; all were classified as non-whitelisted during 2 successful browser runs.

Regulatory Verification Notes

The available page does not present a substantive legal or corporate identity, and no license, licensing authority, or registration number is claimed. Identity verification is therefore unverified, while ownership and governance transparency remain insufficient for regulated or financially sensitive engagement. The absence of a broker-dataset match provides no affirmative regulatory assurance and should be treated only as a neutral reputational-context result, not as a licensing determination.

EVIDENCE

- The homepage contains approximately 136 characters of visible text and functions as a “Navigation / Interstitial” page rather than a legal, corporate, or service disclosure page.
- No license claim, license authority, or license number is present in the available business-model evidence.
- The site is served on AS13335 through CLOUDFLARENET - Cloudflare, Inc., US.
- The transport certificate is issued by WE1 at DV validation level and is valid to 2026-10-22T06:40:48+00:00.

What to Verify Next

Before any sensitive interaction, an independent registry check should establish whether a real operator exists and whether the intended onward service holds the relevant authorization. The onward destination reached through each access route should be inspected separately, with particular attention to its legal identity, licensing evidence, privacy terms, and payment or credential-handling practices. Official contact channels should also be confirmed through an independent route rather than relying solely on the interstitial.

EVIDENCE

- The homepage provides route choices and a continue control but no substantive description of the destination service.
- The page contains no login form, hidden form, password submission field, or sensitive form.
- The observed browser behavior recorded zero wallet-connect runs, zero wallet-sensitive runs, and zero clipboard-write detections.

Summary Verdict

The overall posture is critical, with sensitive interaction risk driven by corroborated external threat findings and unresolved provenance and identity concerns. The site may be a simple access gateway, but the available evidence does not support treating it as a trusted entry point for credentials, accounts, or financial activity.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, and all observed addresses were CDN edge servers rather than identified origin infrastructure. This provides a mitigating layer against direct origin exposure, but it does not establish legitimacy or offset the external reputation findings.

Closing Assessment

Until independent identity, destination, and authorization checks produce satisfactory results, activity should be limited to passive observation and the site should not be used for login, credential submission, or financial transactions.

Written analysis generated 2026-08-18 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, behaviour in a sandbox, external reputation.

- 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
 - A large share of what the page loaded came from other domains.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE
 - The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
 - An external threat feed lists this domain: either Google Safe Browsing marked it malicious, or a significant number of malware engines flagged it.
External reputation rule:EXT_BLACKLIST_CRITICAL

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 1056787.com.

- The request stayed on 1056787.com. It was not redirected to another domain. CLEAR
- Registration is published under Zname Ltd. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-07-15. NOTED
- The earliest public archive of this site is from 2024-04-28. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Zname Ltd
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3034::ac43:8781
Name servers	ARIADNE.NS.CLOUDFLARE.COM, DAMIETE.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-10-22
Domain age	2.30 years (continuous registration)
Domain expiry	2027-07-15
Archive first seen	2024-04-28
Archive snapshots	15
Reputation	VirusTotal: 17 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 1056787.com 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.