

Is 3115aa.top a scam? TrustSniffer's high-risk assessment: 0/100

3115aa.top

Verdict

0

OUT OF 100

CRITICAL RISK

3115aa.top 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

Short promotional landing page for K8 online casino (Chinese). Emphasizes being an official/direct brand with assurances of credibility and large payouts; appears focused on acquiring depositing users with minimal transparency.

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.

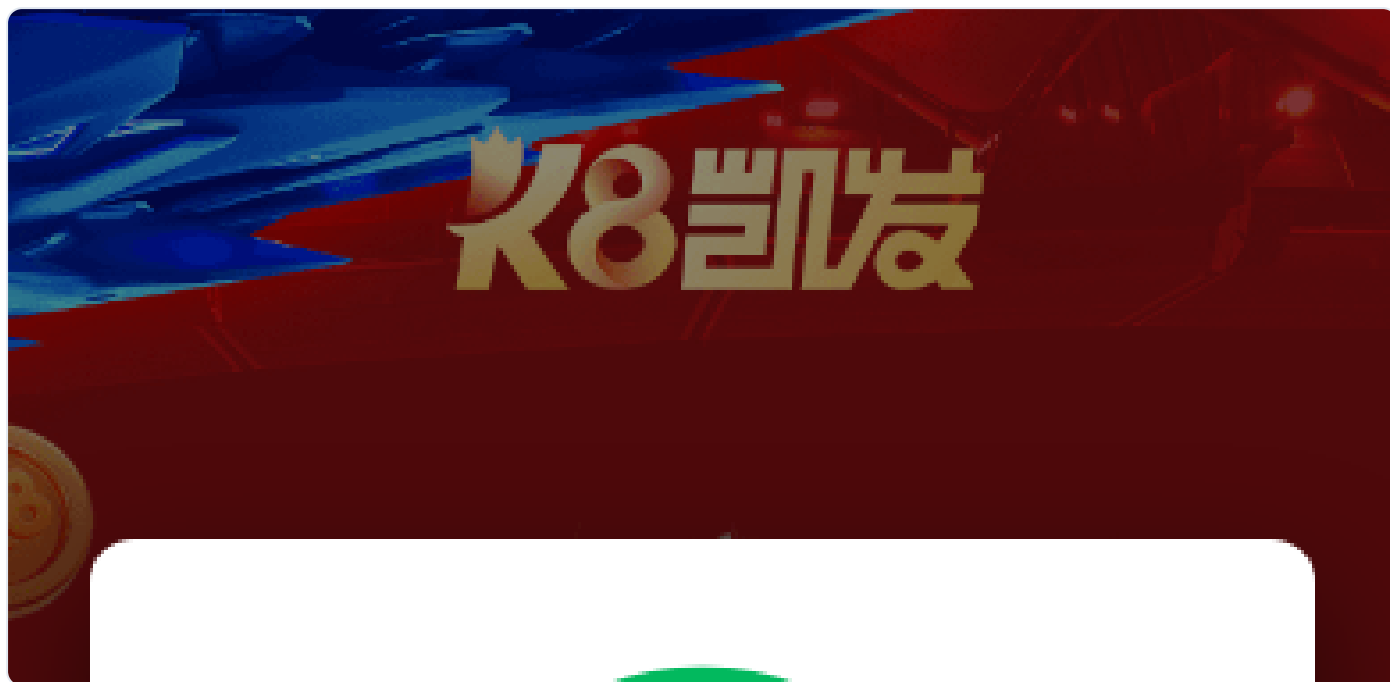
At a glance

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	2.5 years old Registered history	CLEAR
Web archive	Archived since 2024 19 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://3115aa.top/>



What 3115aa.top 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.

This website is a short Chinese-language promotional landing page for “K8,” presenting itself as a leading Asian online entertainment platform and a directly operated official brand. Its apparent business model is to attract users to an online casino where funds are deposited before gambling activity, while emphasizing credibility and large payouts.

Scam/Impersonation Risk

The site presents strong contradiction signals and should be treated as unsuitable for sensitive interaction. Its homepage uses claims equivalent to “Asia’s top online entertainment platform,” “official direct-operated brand,” “credibility assurance,” and “large payouts without worry,” but provides little supporting substance or evidence. The deposit-before-service model, aggressive payout assurances, unclear product detail, and opaque value flow create a material risk that the promotional claims are not reliable. Independent threat-intelligence results also associate the domain with a confirmed blacklist, including multiple malicious detections. No conflicting legal-

entity identity or confirmed brand impersonation was established, but the blacklist finding alone is a decisive adverse signal.

EVIDENCE

- Homepage: identifies “K8” and promotes an online casino using official-brand, credibility, and large-payout assurances.
- Homepage: presents a deposit-funded gambling model with no clearly described underlying product or transparent value flow.
- External reputation checks: recorded 17 malicious detections and 1 suspicious detection; blacklist status was confirmed.
- Registration and archive records: registered 2025-08-17 with a reconciled domain age of 2.55 years; 19 archive snapshots spanning 2024–2026, covering 3 years.

Regulatory Verification Notes

The available site presentation does not establish an independently verified operator identity. No gambling licensing authority, license number, or comparable regulatory credential is disclosed in the available content, and the page does not expose substantive legal or identity documentation. This is a regulatory-transparency gap rather than, by itself, proof of criminal conduct; in combination with the external threat findings and the deposit-based model, however, it materially weakens the basis for regulated engagement. The transport certificate and known hosting arrangements confirm technical deployment, not licensing or operator legitimacy.

EVIDENCE

- Homepage: no licensing authority or license number is disclosed.
- Site transport encryption: TLS certificate issued by WE1, validation level DV, valid to 2026-11-04T09:40:50+00:00.
- Available page navigation: no substantive legal, terms, corporate-identity, or regulatory documentation is exposed.

What to Verify Next

Before any engagement, an independent party should confirm the operator’s legal identity and gambling authorization directly through the relevant jurisdictional regulator, using registry details obtained independently of the site. Payment, withdrawal, dispute, and responsible-gambling terms should also be validated through independently sourced documentation, and any contact channel should be confirmed through an offline or separately authenticated route. Until those checks are completed, login, credential submission, and fund transfers should be deferred.

EVIDENCE

- Homepage: short promotional format provides insufficient documentation to validate operator identity, licensing, or payout obligations.
- Interaction testing: no login form, hidden form, password-external form, wallet connection, or clipboard-writing behavior was observed.
- Network behavior: 4 external non-whitelisted requests were observed, including 2 external non-whitelisted posts.

Summary Verdict

The overall posture is critical, with the available evidence supporting a clear sensitive-interaction risk determination. The website's legitimacy is not established, and the combination of confirmed external threat detections, weak substantive transparency, and a deposit-dependent business model does not support treating it as a trustworthy counterparty.

Infrastructure Integrity

The site is protected by Cloudflare's CDN/WAF infrastructure, which is a mitigating technical control against direct exposure of the hosting environment but is not evidence of legitimacy. All observed addresses were CDN edge addresses, and the origin server was not observable in this analysis.

EVIDENCE

- Hosting infrastructure: served from AS13335, CLOUDFLARENET — Cloudflare, Inc., US.
- Observed edge addresses: 104.21.76.184, 172.67.198.231, 2606:4700:3030::6815:4cb8, and 2606:4700:3037::ac43:c6e7, all associated with AS13335.

Closing Assessment

Prospective users should not log in, submit credentials, or transfer funds through the site; engagement should be deferred until independent validation of the service and its payment protections is complete.

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

- 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

- The registration record withholds contact details for the operator.

Registration and ownership rule:KF_WHOIS_HIDDEN

02 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- 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	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 3115aa.top.

- The request stayed on 3115aa.top. It was not redirected to another domain. CLEAR
- Registration is published under Spaceship, Inc.. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-08-17. NOTED
- The earliest public archive of this site is from 2024-01-28. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Spaceship, Inc.
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3030::6815:4cb8
Name servers	leia.ns.cloudflare.com, leo.ns.cloudflare.com
SSL issuer	WE1
SSL expiry	2026-11-04
Domain age	2.55 years (continuous registration)
Domain expiry	2027-08-17

Archive first seen	2024-01-28
Archive snapshots	19
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 3115aa.top 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/3115aa.top> · assessed 2026-08-18