

Is 052585.cc a scam? TrustSniffer's high-risk assessment: 0/100

052585.cc

Verdict

0

OUT OF 100

CRITICAL RISK

052585.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 2026-08-18 by automated analysis. Classification confidence 70%.

What this site appears to be

Short promotional landing for an online casino brand (K8), advertising large signup and first-deposit bonuses; lacks verifiable licensing, contact, or transactional detail.

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	1.9 years old Registered history	CLEAR
Web archive	Archived since 2024 1 snapshot	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://052585.cc/>



What 052585.cc 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

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

This website is a short promotional landing page for the K8 online casino brand, presenting signup and first-deposit incentives, including a large prize-pool claim and a stated 88,888-yuan first-deposit bonus, with the apparent purpose of driving gambling-account creation and deposits.

Scam/Impersonation Risk

The site presents a high-risk deposit-led gambling proposition while providing very limited substantive content to support its claims. The homepage promotes large rewards and a “billions” prize-pool message, but does not provide corresponding operational, transactional, or ownership evidence. This claim-evidence gap, combined with the requirement to deposit before receiving the promoted service, creates a material risk that financial interactions could expose users to loss or disputed withdrawals. Independent external reputation evidence records a confirmed **blacklist** condition and multiple malicious detections; no separate brand-impersonation or conflicting legal-entity finding is present in the supplied evidence. No contradictions were observed in the form of

a confirmed identity inconsistency, but the external threat signals are sufficient to support a clearly cautionary posture.

EVIDENCE

- Homepage: Displays “K8凯发娱乐” and promotes “注册送豪礼·亿万奖池·首存送88888元,” meaning signup rewards, a billion-level prize pool, and an 88,888-yuan first-deposit promotion.
- Homepage: Provides only approximately 48 characters of substantive DOM text, with no visible licensing, contact, or transactional detail.
- External reputation telemetry: 17 malicious detections were recorded, with a confirmed blacklist result and malicious classifications from two evaluated security providers.
- Domain and archive telemetry: 052585.cc was registered on 2025-11-24 and is recorded as 0.73 years old; the archive contains 1 snapshot spanning 2024–2024, or 1 year tracked.

Regulatory Verification Notes

The homepage does not disclose a verifiable gambling licence, licensing authority, licence number, or identifiable regulatory basis. That is a significant transparency gap for a business model involving player deposits and wagering, but it is treated here as a regulatory-verification issue rather than, by itself, proof of fraud. The available identity evidence does not independently connect the site to a verified real-world operator. A separate broker-reputation dataset returned no match; that result is contextual only and does not establish licensing or legitimacy.

EVIDENCE

- Homepage: No licence authority, licence number, corporate identity, or regulatory disclosure is visible in the supplied page content.
- Hosting telemetry: Served from AS13335, CLOUDFLARENET – Cloudflare, Inc., US.
- Transport-security telemetry: TLS certificate issued by WE1, validation level DV, valid to 2026-10-16T15:02:05+00:00.
- Identity telemetry: WHOIS lists Dynadot LLC as registrar and “Super Privacy Service LTD c/o Dynadot” as the registrant organization.

What to Verify Next

Before any account creation, deposit, or sharing of personal or payment information, the operator should be matched to an official gambling regulator’s public register using the exact legal entity and licence number. The applicable regulator should independently confirm that the domain is authorised for the relevant jurisdiction and that its withdrawal, dispute, age-verification, and responsible-gambling terms are enforceable. Official support and payment channels should also be confirmed through an independent, offline route, and any proposed payment recipient should match the verified licensed operator.

EVIDENCE

- Homepage: The promotional landing page contains no licence number or regulator reference that can be independently checked.
- Homepage: The page has no visible internal links, legal pages, or detailed transactional terms in the supplied capture.
- Behavioural telemetry: Two successful browser runs recorded 4 external POST requests, including 2 non-whitelisted POSTs, warranting confirmation of the destination and purpose of any future transaction flow.

Summary Verdict

The website has a **critical trust posture** and presents a sensitive-interaction risk that is not suitable for account, credential, or financial use. The combination of confirmed external threat reputation, minimal substantiating content, and an unverified operator identity outweighs the limited positive signals provided by basic transport security and identifiable hosting.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, and all observed addresses are CDN edge infrastructure in AS13335; no origin candidate was identified. This can reduce direct exposure of the underlying server, but it is only a mitigating infrastructure characteristic and does not validate the site's operator, content, or financial practices.

Closing Assessment

Enterprise controls should block or isolate this domain for sensitive interactions, and prospective users should refrain from deposits, account registration, credential submission, and payment activity unless the operator and licence are independently confirmed through authoritative channels.

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 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
- 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 052585.cc.

- The request stayed on 052585.cc. It was not redirected to another domain. CLEAR
- Registration is published under DYNADOT LLC. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2026-11-24. NOTED
- The earliest public archive of this site is from 2024-09-23. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	DYNADOT LLC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3032::ac43:9fb3
Name servers	ELAINE.NS.CLOUDFLARE.COM, JUSTIN.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-10-16
Domain age	1.90 years (continuous registration)
Domain expiry	2026-11-24

Archive first seen	2024-09-23
Archive snapshots	1
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 052585.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.

This report online: <https://trustsniffer.com/report/052585.cc> · assessed 2026-08-18