

Is 17dh01.com a scam? TrustSniffer's high-risk assessment: 0/100

17dh01.com

Verdict

0

OUT OF 100

CRITICAL RISK

17dh01.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

Very short Chinese-language landing page referencing "k8" and providing 'continue' and 'recommended routes' links. No contact, product details, or transactional flows are present in the captured HTML.

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.

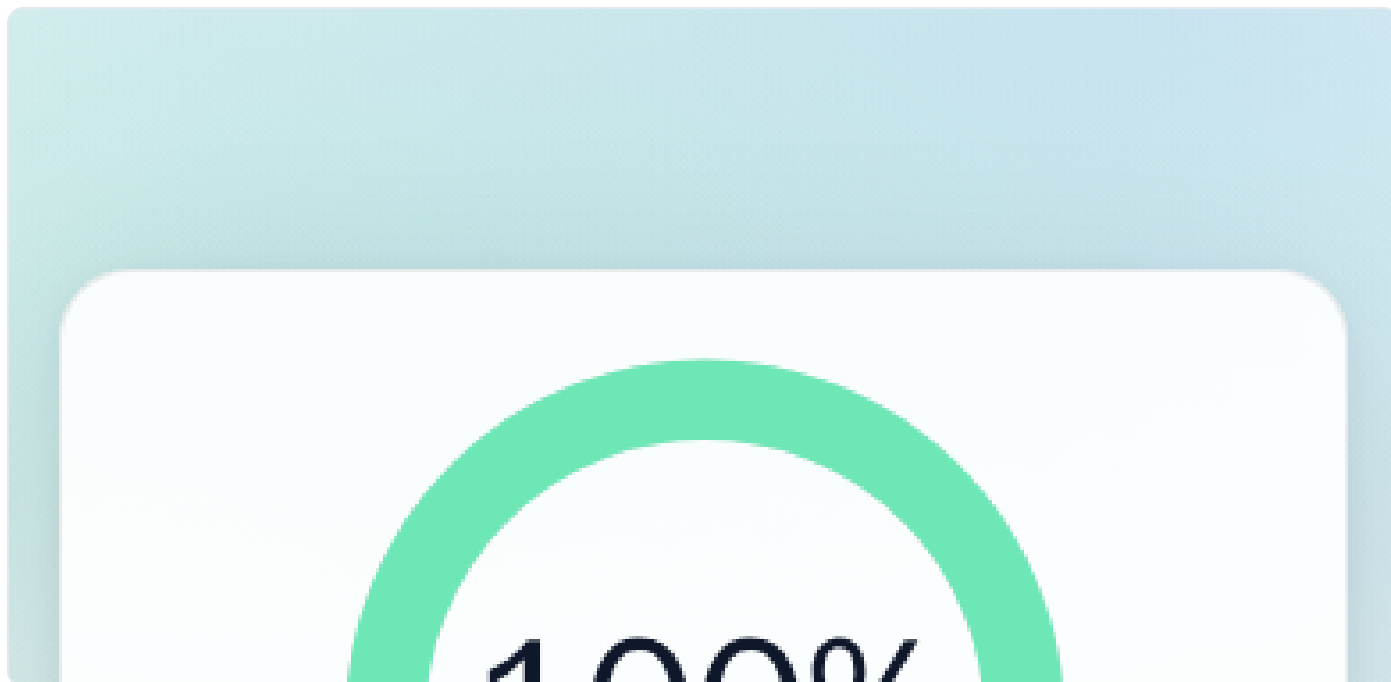
At a glance

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	2.6 years old Registered history	CLEAR
Web archive	Archived since 2024 40 snapshots	CLEAR
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://17dh01.com/>



What 17dh01.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

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

17dh01.com is a Chinese-language landing and redirect page referencing “k8” and presenting “continue” and “recommended route” links. It does not describe a clear product, service, operator, or transaction model, and appears to function primarily as an access gateway or promotional mirror.

Scam/Impersonation Risk

A confirmed blacklist signal and multiple malicious detections create a material risk for sensitive interaction with the site. External security intelligence recorded 17 malicious detections, including signals from Kaspersky and Sophos, and the assessment’s protective control was activated on that basis. The page itself reinforces the concern: it is exceptionally sparse, provides routing links without explaining their destinations or purpose, and offers no clear business context. No separate evidence of a named-brand impersonation or conflicting legal identities was observed, but the blacklist evidence is sufficient to establish a clearly cautionary posture.

EVIDENCE

- External reputation assessment recorded 17 malicious detections and identified Kaspersky and Sophos among the flagged vendors.
- The homepage is classified as a landing, redirect, or access-gateway page and contains only 113 characters of visible text.
- Domain registration records show creation on 2026-02-05 and an age of 0.53 years; the registrar is NameMart Pte. Ltd.
- Web archives contain 40 snapshots spanning 2024–2026, with three years tracked and a maximum recorded gap of one year.

Regulatory Verification Notes

The site does not present a sufficiently identifiable legal or regulatory profile for a financial, wagering, or other high-stakes service. The captured homepage provides no company name, license claim, registration number, terms, or substantive description of the service, leaving the real-world operator unverified and governance disclosure unclear. This is a regulatory and transparency gap rather than independent proof of criminality; however, it is significant when considered alongside the external security detections. The site's valid transport encryption and identifiable hosting infrastructure are technical controls only and do not establish licensing or operator legitimacy.

EVIDENCE

- The captured homepage contains no identifiable legal entity, licensing statement, registration number, contact details, or terms of service.
- The site is hosted on AS13335, CLOUDFLARENET — Cloudflare, Inc., US.
- The site's TLS certificate is issued by WE1, uses domain validation (DV), and is valid until 2026-11-03.
- The page presents no product, monetization, or regulated-activity description from which an applicable supervisory regime could be determined.

What to Verify Next

Before any sensitive interaction, an institution should identify the operator through an independent corporate or regulatory registry and confirm that any claimed activity is authorized in the relevant jurisdiction. The destination of each routing link should be assessed separately rather than treating the landing page as an endorsement of the linked service. Contact and support channels should be confirmed through an independently sourced route, and endpoint security controls should block or isolate the domain pending a documented risk decision.

EVIDENCE

- The homepage offers “continue” and two “recommended route” links without explaining their destination or commercial purpose.
- No login form, password form, wallet connection, or other sensitive input form was present in the captured HTML.
- Browser testing recorded two external XHR requests and two external POST requests classified as non-whitelisted.
- No company, product, legal, or transactional content was available on the captured page to support independent due diligence.

Summary Verdict

The website has a **critical trust posture** and should be treated as unsuitable for credentials, account access, financial activity, or other sensitive interaction. Its identity remains unverified, while the combination of confirmed external security warnings and an unexplained redirect-oriented presentation materially undermines confidence in the site.

Infrastructure Integrity

Cloudflare provides CDN and WAF protection, and all observed addresses were Cloudflare edge infrastructure, including 104.21.59.222 and 172.67.184.151 on AS13335; the origin server was not observable. This reduces direct exposure of the underlying host but is only a mitigating infrastructure characteristic and does not offset the site's reputation risk.

Closing Assessment

Enterprise controls should block or isolate the domain and require documented security, legal, and operator validation before any future access is permitted.

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
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- A large share of what the page loaded came from other domains.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE
- 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 17dh01.com.

- The request stayed on 17dh01.com. It was not redirected to another domain. CLEAR
- Registration is published under NameMart Pte. Ltd.. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-02-05. NOTED
- The earliest public archive of this site is from 2024-01-17. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NameMart Pte. Ltd.
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3037::6815:3bde
Name servers	APOLLO.NS.CLOUDFLARE.COM, STEPHANE.NS.CLOUDFLARE.COM
SSL issuer	WE1
SSL expiry	2026-11-03

Domain age	2.58 years (continuous registration)
Domain expiry	2027-02-05
Archive first seen	2024-01-17
Archive snapshots	40
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 17dh01.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.

This report online: <https://trustsniffer.com/report/17dh01.com> · assessed 2026-08-18