

Is 17000.vip a scam? TrustSniffer's high-risk assessment: 0/100

17000.vip

Verdict

0

OUT OF 100

CRITICAL RISK

17000.vip 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 page titled 'Security' that immediately redirects visitors to 17000.vip. No additional content, contact, or trust signals are present.

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.

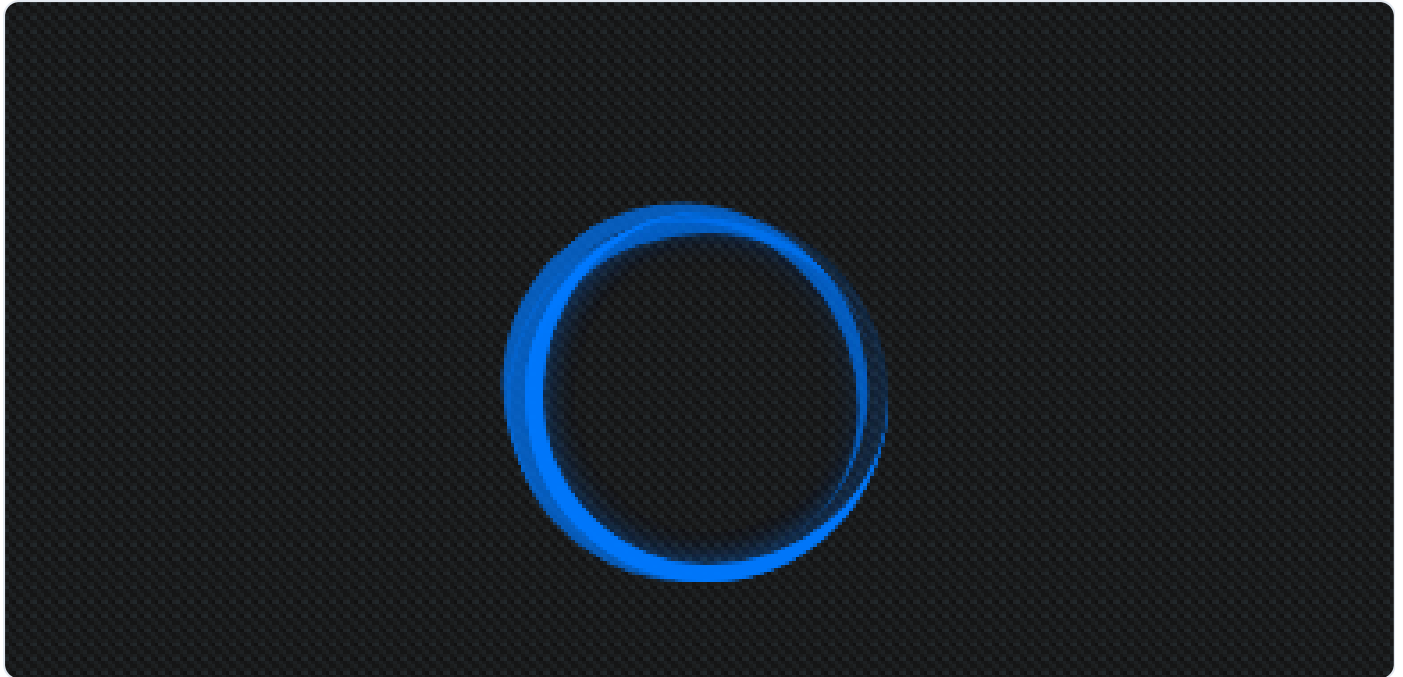
At a glance

The checks that decide most of this verdict.

Malware engines	20 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	4.4 years old Registered history	CLEAR
Web archive	Archived since 2018 14 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

<https://17000.vip/>



What 17000.vip served when TrustSniffer captured it on 2026-08-18. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2018.
- 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 interstitial page titled “Security” whose primary function is to redirect visitors to the external domain 17000.vip, without presenting a substantive service description, operator identity, contact channel, or clear business purpose; its apparent model is therefore a redirector, parking page, or affiliate landing page rather than an independently described service.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk**. External security intelligence records confirmed malicious detections and blacklist listings from multiple sources, including 20 malicious detections and flags from three major security providers. The page itself reinforces the concern: it contains only a short redirect message, uses both meta-refresh and JavaScript redirection, and exposes substantial external network activity relative to its limited content. No conflicting legal identities or direct brand-impersonation indicators were identified, but the confirmed blacklist status is sufficient to establish a serious contradiction to ordinary trust expectations. The

absence of a login or payment form on the captured page does not make the redirected destination suitable for sensitive activity.

EVIDENCE

- The homepage is titled "Security," contains 37 characters of visible text, and redirects visitors to 17000.vip through meta-refresh and JavaScript behavior.
- External reputation assessment recorded 20 malicious detections, zero suspicious-only detections, and an external blacklist hit; Google Safe Browsing did not mark the domain malicious, but that isolated result does not offset the corroborated negative detections.
- Browser telemetry recorded 19 external XHR requests, all classified as non-whitelisted, together with one suspicious inline script; no login form, password form, or wallet-drainer behavior was observed on the captured page.

Regulatory Verification Notes

The available material does not establish a regulated operating entity or a licensed service. The page contains no disclosed corporate identity, regulatory authority, registration number, product description, or meaningful terms for evaluating legal responsibility or consumer protections. Identity verification remains unconfirmed. The domain registration record identifies Dynadot Inc as registrar and uses a privacy service, which is an administrative registration detail rather than independent evidence of the operator's identity. A valid domain-validated certificate confirms encrypted transport only; it does not validate licensing, ownership, or the redirected business.

EVIDENCE

- Registration record: created 2022-03-14T12:38:55Z, approximately 4.43 years old, with Dynadot Inc listed as registrar.
- Archive records contain 14 snapshots from 2018-06-28T17:10:42Z through 2026-01-05T21:28:51Z, covering 9 years tracked.
- The site's TLS certificate is issued by YE2 at DV validation level and is valid until 2026-11-13T03:53:54+00:00.
- The captured page provides no legal, licensing, registration, contact, or service disclosures.

What to Verify Next

Before any sensitive interaction, an independent party should establish the real-world operator and confirm that the redirected destination is controlled by that operator. Any claimed regulated activity should be checked directly against the relevant jurisdiction's official register, using independently sourced contact details rather than channels supplied by the site. The final destination should also be inspected separately for payment requests, credential collection, downloads, or other actions not visible on the interstitial.

EVIDENCE

- Confirm the operator through an independently sourced corporate registry or official business record.
- Confirm any financial, gaming, investment, or other regulated authorization directly with the applicable regulator.
- Validate the final destination and official contact channels through an offline or independently obtained route.
- Apply enterprise web, endpoint, and transaction controls before allowing access from managed systems.

Summary Verdict

The site has a critical trust posture and should not be treated as an established or verified service provider. Available evidence supports restricting sensitive interaction because the site combines confirmed external threat detections with an opaque redirect-only presentation and unverified operator identity.

Infrastructure Integrity

The domain resolves to two IP addresses with likely origin exposure and no detected CDN or WAF layer. Hosting is attributed to ANTI-DDOS - NetLab Global, US, with infrastructure registered in Hong Kong; the observed geographic and registry locations differ, which is a contextual infrastructure inconsistency rather than proof of malicious ownership. The hosting arrangement provides attribution but no legitimacy assurance.

EVIDENCE

- Served from AS35251, ANTI-DDOS - NetLab Global, US, with the resolved infrastructure located in HK.
- Infrastructure resolution returned 2 unique IP addresses, with 0 edge IPs and 2 likely origin IPs.
- No trusted CDN was detected.

Closing Assessment

Passive inspection may be retained for investigative purposes, but credentials, payments, downloads, wallet authorization, and other sensitive actions should be blocked until independent operator and destination validation 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

- Most of what the page loaded came from other domains rather than from this one.

Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH

- The page exchanged network traffic with destinations TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC

- The page made background requests to destinations TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR

- The page carried inline scripts written in a style TrustSniffer treats as suspicious.

Behaviour in a sandbox rule:BEHAV_SUSPICIOUS_INLINE_SCRIPTS

- 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 17000.vip.

- The request stayed on 17000.vip. It was not redirected to another domain. [CLEAR](#)
- Registration is published under Dynadot Inc. [CLEAR](#)
- DNS for this domain is served by xundns.com, across 2 name servers. [NOTED](#)
- The registration is paid up to 2028-03-14. [CLEAR](#)
- The earliest public archive of this site is from 2018-06-28. [CLEAR](#)
- It is hosted on ANTI-DDOS, from a server in HK. [NOTED](#)

Domain intelligence

Registrar	Dynadot Inc
Hosting	ANTI-DDOS - NetLab Global, US
Country	HK
Server IP	45.138.71.205
Name servers	n1.xundns.com, n2.xundns.com
SSL issuer	YE2
SSL expiry	2026-11-13
Domain age	4.43 years (continuous registration)
Domain expiry	2028-03-14
Archive first seen	2018-06-28
Archive snapshots	14
Reputation	VirusTotal: 20 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 17000.vip 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/17000.vip> · assessed 2026-08-18