

Is 19199.vip a scam? TrustSniffer's high-risk assessment: 0/100

19199.vip

Verdict

0

OUT OF 100

CRITICAL RISK

19199.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 60%.

What this site appears to be

Minimal page stating 'Security' and 'Redirecting to 19199.vip ...'. No product, contact, or forms; functions as a redirector to an external domain.

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.

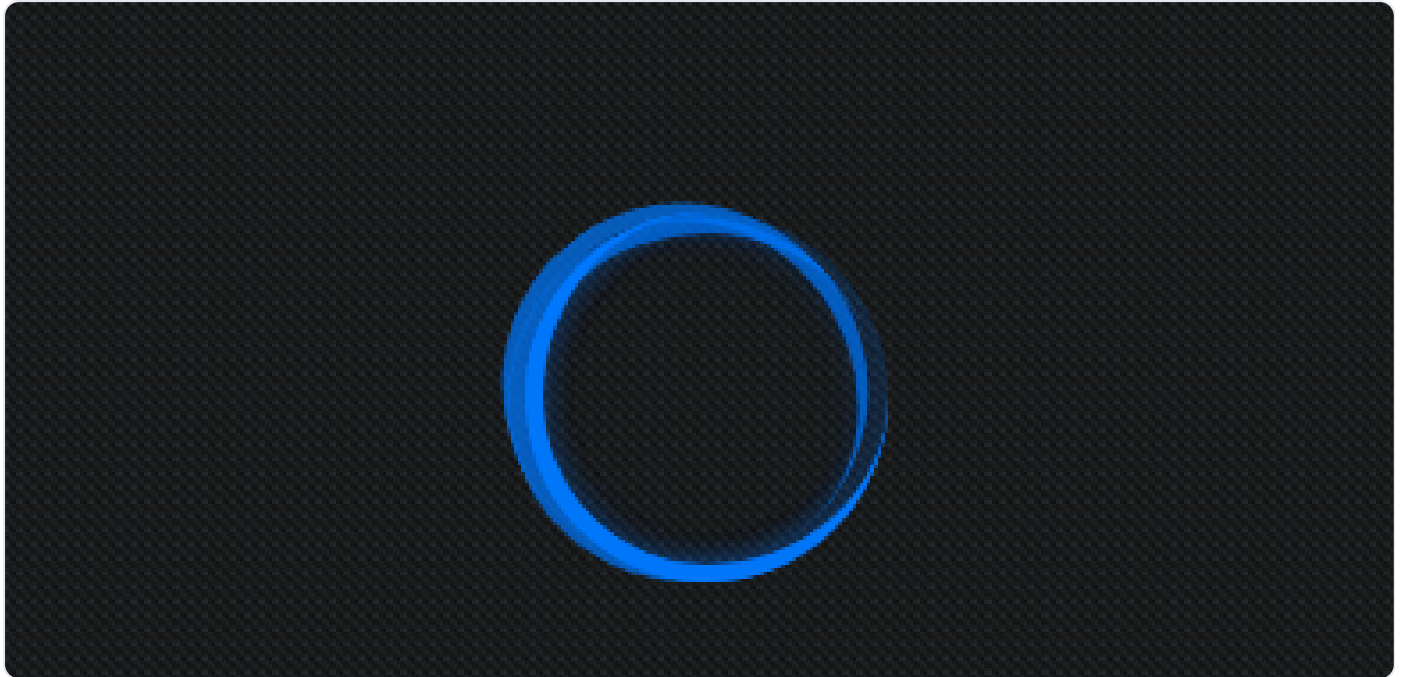
At a glance

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 2023 23 snapshots	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

<https://19199.vip/>



What 19199.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 2023.
- 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 landing page labelled “Security” that automatically redirects visitors to 19199.vip, without presenting a clear operator, product, service, pricing model, or contact channel; its apparent function is traffic redirection rather than a transparent customer-facing business.

Scam/Impersonation Risk

Contradictory risk signals are present and warrant a clearly cautionary posture. External reputation systems recorded corroborated malicious detections and a confirmed blacklist hit, while the site itself provides only a redirect and no provenance or explanation for the destination. This combination creates a material risk that visitors could be routed into an untrusted or harmful environment, even though no separate brand-impersonation finding is established.

EVIDENCE

- The landing page states “Security” and “Redirecting to 19199.vip ...”, with automatic external-domain redirection.
- External reputation evaluation recorded 20 malicious detections, with the domain also present on an external blacklist.
- The domain was registered on 2022-03-14 and is 4.43 years old; the registration record lists Dynadot Inc.
- Archive records contain 23 snapshots spanning 3 years, from 2023-07-26 through 2025-12-07.

Regulatory Verification Notes

The site does not provide an identifiable business model, operator disclosure, licensing claim, registration number, terms, or other regulatory basis on the observed page. Identity verification remains unestablished, so the site's apparent legitimacy cannot be connected independently to a real-world entity. A valid transport certificate confirms encrypted delivery only; it does not validate the operator, destination, or any financial activity. The available third-party broker dataset produced no matching record, which is contextual only and does not constitute licensing or regulatory approval.

EVIDENCE

- The homepage contains no product, pricing, contact, operator, or licensing information and is classified as a redirect/minimal-content page.
- Served from AS35251 (ANTI-DDOS - NetLab Global, US).
- TLS certificate issued by YE2 at DV validation level, valid to 2026-11-13.
- The site's hosting record identifies 45.138.71.205 in Hong Kong; this is a hosting fact, not evidence of regulatory authorization.

What to Verify Next

Before any interaction, an organization should identify the final destination independently rather than relying on the redirecting page. Any claimed operator should be matched to authoritative corporate and regulatory registers, and any proposed payment, account, or credential flow should be validated through independently sourced official contact channels. If the destination requests software installation, authentication, payment, or financial transfer, the request should be escalated for security review before proceeding.

EVIDENCE

- The observed page provides no operator, service, pricing, or contact material from which a business relationship can be validated.
- The page performs an automatic external-domain redirect and contains no forms or documented customer workflow.
- Browser analysis recorded 40 external XHR requests and 2 external POST requests during two successful runs, supporting independent review of the redirected destination.

Summary Verdict

The site has a **critical trust posture** and should not be treated as an established or reliable platform for sensitive interaction. The available evidence supports a high-risk assessment driven by the convergence of confirmed external threat detections, a blacklisting signal, and an opaque redirect-only presentation.

Infrastructure Integrity

No CDN/WAF or protected-origin evidence is supplied for this site, so the infrastructure record provides no meaningful mitigating basis for trust. The presence of functioning TLS and identifiable hosting should be regarded as delivery infrastructure only, not as proof of legitimacy.

Closing Assessment

Sensitive interaction should be withheld, including login, credential submission, financial activity, or transfer of funds; any unavoidable business requirement should proceed only through independently sourced channels and formal security review.

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, page content, 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 made background requests to destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR
- A form on the page submits to a destination TrustSniffer could not verify.
Page content rule:PAGE_FORM_UNTRUSTED_DEST
- The page exchanged network traffic with destinations TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC
- The page sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
- 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 19199.vip.

- The request stayed on 19199.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 2023-07-26. 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	2023-07-26
Archive snapshots	23
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 19199.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/19199.vip> · assessed 2026-08-18