

Is 238wellbet.com a scam? TrustSniffer's high-risk assessment: 0/100

238wellbet.com

Verdict

0

OUT OF 100

CRITICAL RISK

238wellbet.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

Chinese-language streaming/media landing page promoting a catalog of movies, TV series, anime and variety shows with claims of free HD daily updates; minimal site/legal/monetization details present on the captured page.

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.

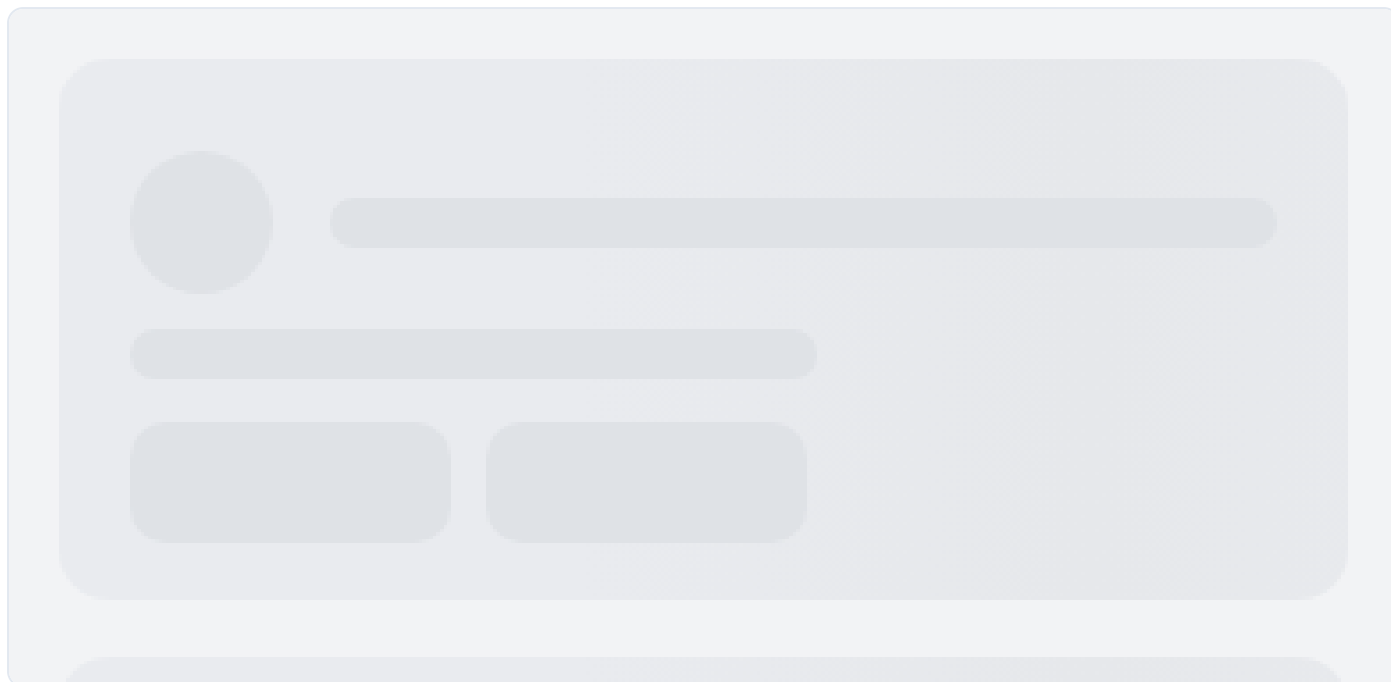
At a glance

The checks that decide most of this verdict.

Malware engines	18 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	2.2 years old Registered history	CLEAR
Web archive	Archived since 2018 9 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://238wellbet.com/>



What 238wellbet.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 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.

238wellbet.com presents a Chinese-language entertainment streaming landing page branded “九九影视,” offering visitors free HD access to movies, television series, anime, manga, and variety programming with claims of daily updates and an ad-free viewing experience. Its apparent business model is an online media catalogue, although monetization and content-licensing arrangements are not explained on the captured page.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk** because the domain has a confirmed blacklist status and multiple external security detections, including 18 malicious classifications from evaluated reputation sources. This is a substantive contradiction that outweighs the otherwise ordinary appearance of the streaming landing page. The homepage advertises access to named commercial titles such as *Dune: Part Two*, *Oppenheimer*, *Three-Body Problem: The Dark Forest*, *The Last of Us*, and *Jujutsu Kaisen*, but supplies no evidence that the content is authorized. The captured page did not show a login form, wallet connection, or confirmed brand impersonation; those absences do not resolve the external reputation conflict. Browser observation also

recorded a suspicious network pattern involving external requests and POST activity outside expected destinations.

EVIDENCE

- The domain is blacklisted in external reputation coverage, with 18 malicious detections and alerts from three major security vendors.
- Archive records contain 9 snapshots spanning 2018-08-19 to 2026-06-11, with 9 years tracked; the captures do not establish continuous provenance for the present operation.
- The domain was registered on 2024-05-27 and is approximately 2.23 years old according to registration records.
- The homepage's external behavior included 13 external XHR requests, 9 non-whitelisted XHR requests, and 3 non-whitelisted POST requests.

Regulatory Verification Notes

The available identity evidence is unverified. The captured homepage does not identify a legal entity, operator, licensing authority, registration number, or rights holder for the media catalogue, leaving a material disclosure gap for a service distributing or linking to commercial audiovisual content. This is a regulatory and transparency issue rather than independent proof of fraud, but it prevents the site's operating legitimacy from being established. The transport certificate confirms encrypted delivery only; it does not validate the operator, content rights, or regulatory standing.

EVIDENCE

- The homepage contains no verifiable corporate or legal disclosure supporting the operator's identity.
- No licensing authority, license number, or content-rights disclosure is shown on the captured page.
- The site is served from AS54801, ZILLION-NETWORK — Zillion Network Inc., US.
- The site uses a DV TLS certificate issued by YR1, valid to 2026-09-04.

What to Verify Next

Any prospective engagement should first confirm the operator through an independently sourced business registry and confirm that the relevant copyright or media regulator recognizes the service and its licensing arrangements. Contact channels should be validated through an offline or independently obtained route rather than relying solely on information presented by the site. Sensitive interaction should not proceed unless those checks resolve the reputation and identity concerns; passive viewing in an isolated environment is the only proportionate interim use.

EVIDENCE

- The captured page provides no internal links to legal, corporate, licensing, or contact documentation.
- The page has no login form or sensitive-input form, so there is no demonstrated need for credential submission during the captured interaction.
- The page capture returned successfully, but successful page delivery does not establish operator legitimacy or content authorization.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The available evidence does not establish a trustworthy connection between the website and a legitimate, accountable operating entity, while the external reputation contradiction is material and confirmed. Identity and legitimacy therefore remain unverified.

Infrastructure Integrity

The site resolves directly to a single likely origin address rather than a detected CDN or WAF edge, and the hosting provider is ZILLION-NETWORK — Zillion Network Inc., US. This infrastructure provides limited protective mediation compared with mainstream edge-delivery arrangements; in any event, hosting infrastructure is only a mitigating or contextual signal and is not evidence of legitimacy.

Closing Assessment

The appropriate enterprise posture is to avoid logins, credential submission, downloads, payments, and other sensitive interaction, and to permit only controlled, passive observation if business necessity requires further examination.

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 made background requests to destinations TrustSniffer does not recognise.

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_XHR

- 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

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

Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_TRAFFIC

- 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 238wellbet.com.

- The request stayed on 238wellbet.com. It was not redirected to another domain. CLEAR
- Registration is published under Gname.com Pte. Ltd.. CLEAR
- DNS for this domain is served by share-dns.com, across 2 name servers. NOTED
- The registration is paid up to 2027-05-27. NOTED
- The earliest public archive of this site is from 2018-08-19. CLEAR
- It is hosted on ZILLION-NETWORK, from a server in US. NOTED

Domain intelligence

Registrar	Gname.com Pte. Ltd.
Hosting	ZILLION-NETWORK - Zillion Network Inc., US
Country	US
Server IP	38.4.64.34
Name servers	A4.SHARE-DNS.COM, B4.SHARE-DNS.NET
SSL issuer	YR1
SSL expiry	2026-09-04
Domain age	2.23 years (continuous registration)
Domain expiry	2027-05-27
Archive first seen	2018-08-19
Archive snapshots	9
Reputation	VirusTotal: 18 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 238wellbet.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/238wellbet.com> · assessed 2026-08-18