

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

metahuay.com

Verdict

0

OUT OF 100

CRITICAL RISK

metahuay.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 2026-08-21 by automated analysis. Classification confidence 55%.

What this site appears to be

Localized Chinese landing page for Mahjong Soul (雀魂) detailing game features, rules, character system, downloads for PC/mobile/Steam, gacha probabilities, changelog, and support contact. Primary purpose is user acquisition and driving downloads/in-app monetization.

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	16 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	6 months old Most scam domains are under a year old	WATCH
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

<https://metahuay.com/>

403 Forbidden

openresty

What metahuay.com served when TrustSniffer captured it on 2026-08-21. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- Public web-archive history exists since 2021.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

A localized Chinese landing page for a digital entertainment title, the site presents Mahjong Soul as a free-to-download online riichi-mahjong game with character collection, competitive play, PC/mobile/Steam access, and monetization through in-app purchases and gacha-style draws.

Scam/Impersonation Risk

Confirmed external threat indicators create a critical interaction risk despite the page's professional gaming presentation and the absence of an observed login form, hidden form, wallet connection, or explicit brand-impersonation marker. The site promotes downloads and account registration, while observed network activity included non-whitelisted external requests and posts; this creates additional uncertainty around the download and registration pathways. The domain is blacklisted by external sources, with multiple malicious detections including coverage from Fortinet and Sophos. The historical record also conflicts with the current registration record: archival captures predate the recorded 2026 creation date, so domain provenance cannot be

treated as straightforward. No conflicting legal-entity names were observed, but the external threat evidence is sufficient to require a clearly defensive posture. Evidence:

- The homepage presents Mahjong Soul gameplay, character acquisition, gacha probabilities, registration, and PC/mobile/Steam download routes.
- External reputation telemetry records 16 malicious detections and 1 suspicious detection, with Fortinet and Sophos among the flagged vendors; blacklist status is true.
- The observed page generated 2 external XHR requests and 2 external POST requests classified as non-whitelisted, with a maximum external activity proportion of 72.6%.
- Archive records show 11 snapshots spanning 2021–2025, covering 5 years, while the registration record states creation in 2026.

Regulatory Verification Notes

The site's on-page identity is presented through the title “雀魂集团|中国官网,” but the available evidence does not independently verify the operator behind that claim. The page describes a commercial entertainment model involving downloads, in-app purchases, character draws, and potentially premium content; no licensing authority or registration number is claimed in the available business information. This is a disclosure and operator-verification gap rather than, by itself, proof of wrongdoing. The site's valid transport encryption and identified hosting are technical properties only and do not establish ownership, publisher authorization, or regulatory standing. Evidence:

- The recorded registrar is Metaregistrar BV; the domain creation date is 2026-02-11T19:15:53Z and the recorded age is 0.52 years.
- The site is hosted on AS9294, GNETINC-AS-AP - GNET INC., US.
- The transport certificate is issued by YE2, uses DV validation, and is valid to 2026-11-05T19:03:48+00:00.
- The available business information records no claimed license authority or license number.

What to Verify Next

Before any interaction beyond passive viewing, the purported game publisher and the legitimacy of each download should be confirmed through independently established official app-store or platform listings, not solely through links supplied by this site. Any account or payment activity should wait until the publisher identity, software provenance, privacy terms, refund arrangements, and applicable consumer protections are confirmed through independent channels. Downloaded software should be obtained from a verified platform source and subjected to enterprise malware scanning and code-signature checks where available. Evidence:

- The site's stated purpose is user acquisition and download distribution rather than a purely informational game guide.
- The observed page contains no sensitive form, but it does direct visitors toward registration and client downloads.
- The page includes external destinations and a support channel, requiring independent confirmation that those destinations belong to the authorized publisher.

Summary Verdict

The overall posture is **critical and unsuitable for sensitive interaction**. The site's coherent gaming content does not offset the confirmed external threat detections, unresolved provenance conflict, and lack of

independently verified operator identity. Passive reference may be possible, but the evidence does not support trust for credentials, account access, downloads, or financial activity.

Infrastructure Integrity

The site resolves to one likely origin IP without a detected CDN or edge-IP layer. Hosting is provided through GNETINC-AS-AP, and the direct origin posture offers limited infrastructure separation; the presence of basic transport encryption should be regarded only as a narrow protective measure, not as evidence of legitimacy.

Closing Assessment

The appropriate course is to avoid login, credential submission, downloads, and financial transactions through the site, and to use only independently verified official channels until the publisher and software provenance have been established.

Written analysis generated 2026-08-21 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
 - 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	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 metahuay.com.

- The request stayed on metahuay.com. It was not redirected to another domain. CLEAR
- Registration is published under Metaregistrar BV. CLEAR
- DNS for this domain is served by xundns.com, across 2 name servers. NOTED
- The registration is paid up to 2027-02-11. NOTED
- The earliest public archive of this site is from 2021-12-17. CLEAR
- It is hosted on GNETINC-AS-AP, from a server in SC. NOTED

Domain intelligence

Registrar	Metaregistrar BV
Hosting	GNETINC-AS-AP - GNET INC., US
Country	SC
Server IP	156.247.116.198
Name servers	N1.XUNDNS.COM, N2.XUNDNS.COM
SSL issuer	YE2
SSL expiry	2026-11-05
Domain age	0.52 years (continuous registration)
Domain expiry	2027-02-11
Archive first seen	2021-12-17
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 16 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about metahuay.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.