

Is meteorclients.com a scam? TrustSniffer's high-risk assessment:
5/100

meteorclients.com

Verdict

5

OUT OF 100

CRITICAL RISK

meteorclients.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 2026-09-22 by automated analysis. Classification confidence 55%.

What this site appears to be

Promotional download page for 'Meteor Client', a modular Minecraft utility/cheat client. Describes features (combat, ESP, movement, world tools), shows download instructions requiring Fabric Loader, counts of downloads/online players, and offers a \$2.99 lifetime Premium upgrade. Links to Fabric and Discord for support.

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.

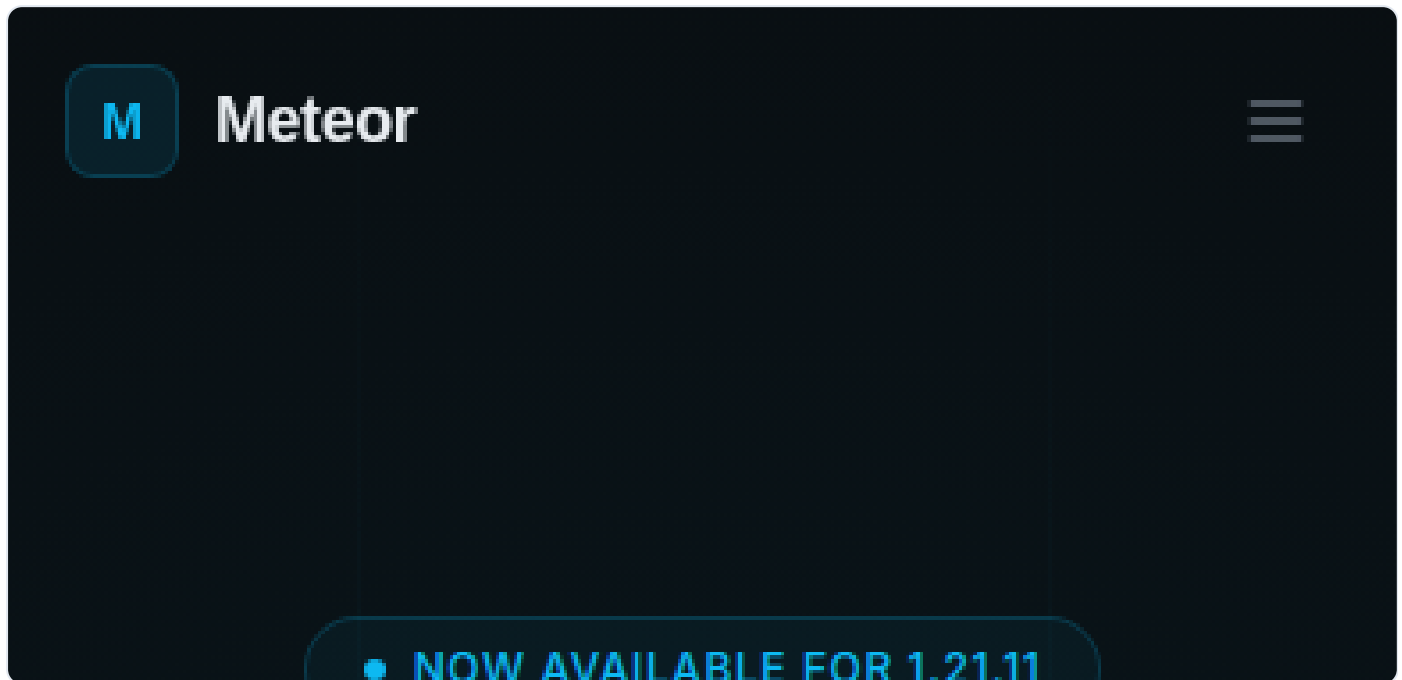
At a glance

The checks that decide most of this verdict.

Malware engines	21 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	49% confidence AbuseIPDB, 81 reports; shared hosting inflates reports	CLEAR
Domain age	6 months old Most scam domains are under a year old	WATCH
Web archive	Never archived No public history of this site	WATCH

The page as captured

<https://meteorclients.com/>



What meteorclients.com served when TrustSniffer captured it on 2026-09-22. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

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 promotional download site for Meteor Client, a Minecraft utility and cheat client offering free access alongside a paid lifetime Premium upgrade. Its apparent business model is software distribution and one-time monetization of additional client functionality.

Scam/Impersonation Risk

The site presents a technically coherent product page, but that benign presentation is outweighed by confirmed external threat detections and blacklist status. The homepage promotes combat automation, ESP and x-ray functions, movement hacks, world-scanning tools, “100% Undetected” operation, and claims that the client can bypass anti-cheat systems; these claims create material software-integrity and account-abuse concerns even though the page itself contains no login form, hidden form, wallet interaction, or observed external posting

behavior. Abuse reports associated with the observed IP are attributed to shared CDN infrastructure, so they are not by themselves conclusive evidence about the website; however, the domain-level malicious detections and confirmed blacklist findings remain decisive. No separate identity contradiction or explicit brand-impersonation finding was observed.

EVIDENCE

- Homepage: advertises combat automation, ESP/x-ray, movement hacks, world scanning, “100% Undetected” operation, and anti-cheat bypass claims.
- External reputation telemetry: 21 malicious detections and 1 suspicious detection were recorded, with three security providers flagging the site; the domain was also present on an external blacklist.
- Hosting-IP telemetry: 81 abuse reports were associated with 185.158.133.1, with the attribution recorded as shared CDN infrastructure rather than uniquely attributable to the site.
- Domain registration: registered 2026-03-18, approximately 0.52 years old, through GoDaddy.com, LLC.

Regulatory Verification Notes

The available material does not independently verify the real-world operator. The captured homepage provides a product description and payment proposition but does not establish a corporate entity, licensing position, publisher registration, or accountable legal contact. For downloadable software, a financial-services license may not be applicable; nevertheless, the absence of independently verifiable publisher and consumer-protection information is a material transparency gap before installation or payment. No matching third-party broker profile was identified, but that contextual result does not establish legitimacy or regulatory standing.

EVIDENCE

- Homepage: presents the software and Premium purchase proposition without a separately verified legal-entity or publisher disclosure.
- Homepage: no license claim, license number, or licensing authority is identified.
- Technical transport: TLS is issued by WE1 at DV validation level and is valid to 2026-12-10.
- Hosting telemetry: served on AS13335, CLOUDFLARENET - Cloudflare, Inc., US.

What to Verify Next

Before any installation or payment, an enterprise or consumer should obtain independent confirmation of the publisher’s legal identity, verify the software through a trusted official distribution channel, and compare downloaded files against independently published hashes or signatures. The advertised anti-cheat and automation capabilities should also be assessed against the applicable game platform’s rules, while payment terms, refund rights, update delivery, and support ownership should be confirmed through independently sourced channels.

EVIDENCE

- Publisher verification: the captured material does not provide an independently confirmed operator identity.
- Software provenance: the available page evidence does not document an independent file-signing, hash-verification, or malware-analysis process.
- Consumer terms: the captured material does not establish refund, support, or dispute-resolution arrangements for the paid upgrade.

Summary Verdict

The overall posture is critical and clearly unsuitable for sensitive interaction. The website's coherent promotional presentation and limited benign browser behavior do not overcome the confirmed external threat and blacklist contradictions. Operator identity and legitimacy remain unverified.

Infrastructure Integrity

Cloudflare CDN/WAF protection provides a mitigating layer against direct exposure of the underlying service, but it is an infrastructure control rather than evidence of publisher legitimacy. The observed infrastructure resolved through Cloudflare, with no origin candidate identified in this analysis.

Closing Assessment

Prospective users should restrict activity to non-interactive observation unless independent publisher, software-integrity, and transaction checks produce satisfactory confirmation.

Written analysis generated 2026-09-22 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, 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

- 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

Signals weighed against the site

- AbuseIPDB: 81 reports on hosting IP 185.158.133.1 (Internet Utilities Europe and Asia Limited, Content Delivery Network), 49% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

Identity verification

Status	UNVERIFIED
Identity score	55/100
Identity verification confidence	30%

- 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 meteorclients.com.

- The request stayed on meteorclients.com. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- DNS for this domain is served by domaincontrol.com, across 2 name servers. NOTED
- The registration is paid up to 2027-03-18. NOTED
- It is hosted on CLOUDFLARENET, from a server in AE. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	AE
Server IP	185.158.133.1
Name servers	NS23.DOMAINCONTROL.COM, NS24.DOMAINCONTROL.COM
SSL issuer	WE1
SSL expiry	2026-12-10
Domain age	0.52 years (continuous registration)
Domain expiry	2027-03-18
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 21 flagged AbuseIPDB: 49% confidence, 81 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about meteorclients.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/meteorclients.com> · assessed 2026-09-22