

Is 198-macros.com a scam? TrustSniffer's high-risk assessment: 0/100

198-macros.com

Verdict

0

OUT OF 100

CRITICAL RISK

198-macros.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

Landing page distributing a cracked version of a paid Minecraft macro client (198 Macros). Contains feature descriptions, installation instructions (double-click jar or drop in mods folder), and download links. Presents the mod as free and cracked; carries elevated risk (malware, copyright infringement).

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.

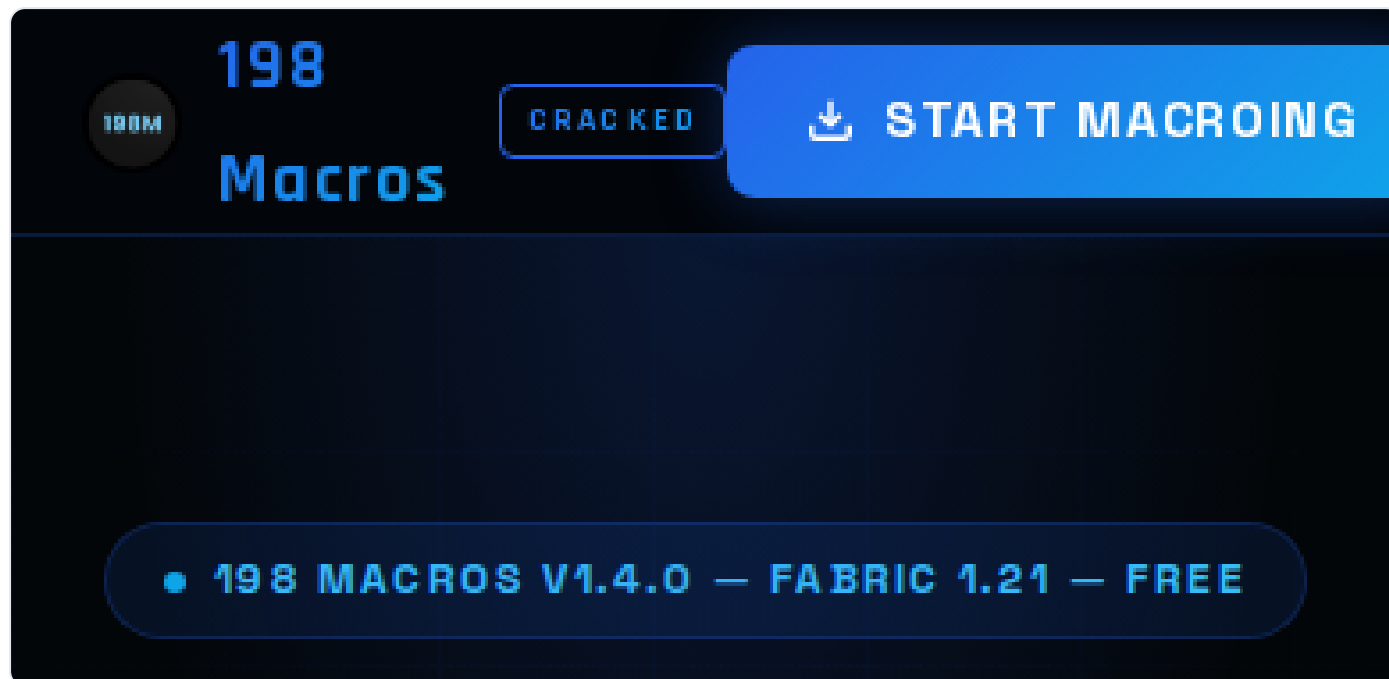
At a glance

The checks that decide most of this verdict.

Malware engines	6 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	RISK
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

https://198-macros.com/



What 198-macros.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 flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

198-macros.com is a download-oriented website presenting a cracked version of the paid “198 Macros” Minecraft modification as a free Fabric 1.21 client, with automation features for competitive player-versus-player use and instructions to install or auto-inject a JAR file into Minecraft.

Scam/Impersonation Risk

The site presents a clearly unsafe software-distribution model rather than an ordinary commercial service. Its homepage advertises “198 Macros v1.4.0” as a cracked and free premium client, including Crystal, Mace, and Sword automation, configurable delays, keybinds, and slot assignments. The installation material instructs visitors to place the JAR in the Minecraft mods folder or double-click it to auto-inject into a running game. That combination creates material malware, unauthorized-modification, and copyright risks. Independent reputation evidence records malicious and suspicious detections and a confirmed blacklist status. No identity contradiction, brand impersonation, or phishing form was observed in the supplied page findings, but the confirmed blacklist and malicious detections are sufficient to establish a critical interaction risk.

EVIDENCE

- The homepage states that the paid macro suite is “cracked” and available free of charge, with Crystal, Mace, and Sword automation features.
- The installation page describes placing a JAR in the mods folder or double-clicking it to auto-inject into a running Minecraft instance.
- External reputation telemetry recorded 6 malicious detections, 5 suspicious detections, and a confirmed blacklist result for the domain.
- The domain was registered in 2026 and is approximately 0.46 years old; the registrar is Web Commerce Communications Limited dba WebNic.cc.

Regulatory Verification Notes

The available privacy, terms, FAQ, and informational pages do not establish a verifiable operating entity, licensing position, or lawful authorization to redistribute the paid software. The page-level assessment specifically identifies unverifiable legal status, opaque value flow, and a disconnect between the site’s free-distribution claims and the absence of substantiating authorization. Identity verification remains unverified, so the site’s apparent operation cannot be independently connected to a real-world organization. The valid transport certificate and identified hosting arrangement are technical properties only and do not cure the legal or governance deficiencies.

EVIDENCE

- The terms and privacy pages are present, but the supplied content does not establish a named legal operator or licensing authorization for the redistributed software.
- The site’s hosting was identified as AS214351, FEMOIT – FEMO IT SOLUTIONS LIMITED, GB.
- The site uses a DV TLS certificate issued by YR1, valid to 2026-12-20T14:06:27+00:00.

What to Verify Next

Before any interaction beyond passive viewing, an organization should obtain the software only from the original publisher or another independently authenticated distribution channel, validate the publisher’s authorization, and subject any downloaded artifact to controlled malware analysis. Security teams should also confirm the site’s official contact and ownership details through an independent, offline route rather than relying solely on the site’s own pages. Credentials, payments, and execution of downloaded files should remain outside the permitted interaction scope unless those checks produce authoritative contrary evidence.

EVIDENCE

- The tested homepage contains no login form or sensitive submission form, so there is no supplied evidence supporting account-based engagement.
- Browser analysis flagged executable-file distribution, claimed JAR auto-injection, and potential malware risk.
- Observed testing recorded no external XHR or POST activity, but that limited behavior does not validate the safety of files offered for download.

Summary Verdict

The website has a **critical trust posture** driven by converging malicious-reputation, unsafe software-distribution, governance, and identity-verification concerns. Its content is consistent with an untrusted cracked-software distribution site, and the available evidence does not support sensitive interaction.

Infrastructure Integrity

Cloudflare CDN/WAF protection provides a mitigating layer against direct exposure of the service infrastructure, but it is not evidence of legitimacy. The observed address was a CDN edge address, and the origin server was not independently visible in the supplied infrastructure assessment.

EVIDENCE

- The site is protected by Cloudflare CDN/WAF infrastructure.
- One observed edge IP was recorded: 196.251.107.204.
- The infrastructure assessment identified no likely origin IP candidate.

Closing Assessment

Prospective users and enterprise controls should restrict activity to passive viewing and block downloading, execution, credential submission, and payment interaction associated with the site.

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

- 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
- 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 198-macros.com.

- The request stayed on 198-macros.com. It was not redirected to another domain. CLEAR
- Registration is published under Web Commerce Communications Limited dba WebNic.cc. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-04-05. NOTED
- It is hosted on FEMOIT, from a server in SC. NOTED

Domain intelligence

Registrar	Web Commerce Communications Limited dba WebNic.cc
Hosting	FEMOIT - FEMO IT SOLUTIONS LIMITED, GB
Country	SC
Server IP	196.251.107.204
Name servers	ANDY.NS.CLOUDFLARE.COM, BRENNAN.NS.CLOUDFLARE.COM
SSL issuer	YR1
SSL expiry	2026-12-20
Domain age	0.46 years (continuous registration)
Domain expiry	2027-04-05
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about 198-macros.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.