

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

multiplay.at

Verdict

5

OUT OF 100

CRITICAL RISK

multiplay.at 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 for a free Chrome extension that lets users manage and launch multiple Roblox accounts locally. Describes features, installation steps (load unpacked in Developer Mode), FAQ, and reassures that account data stays on the device. No signup or payments shown.

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.

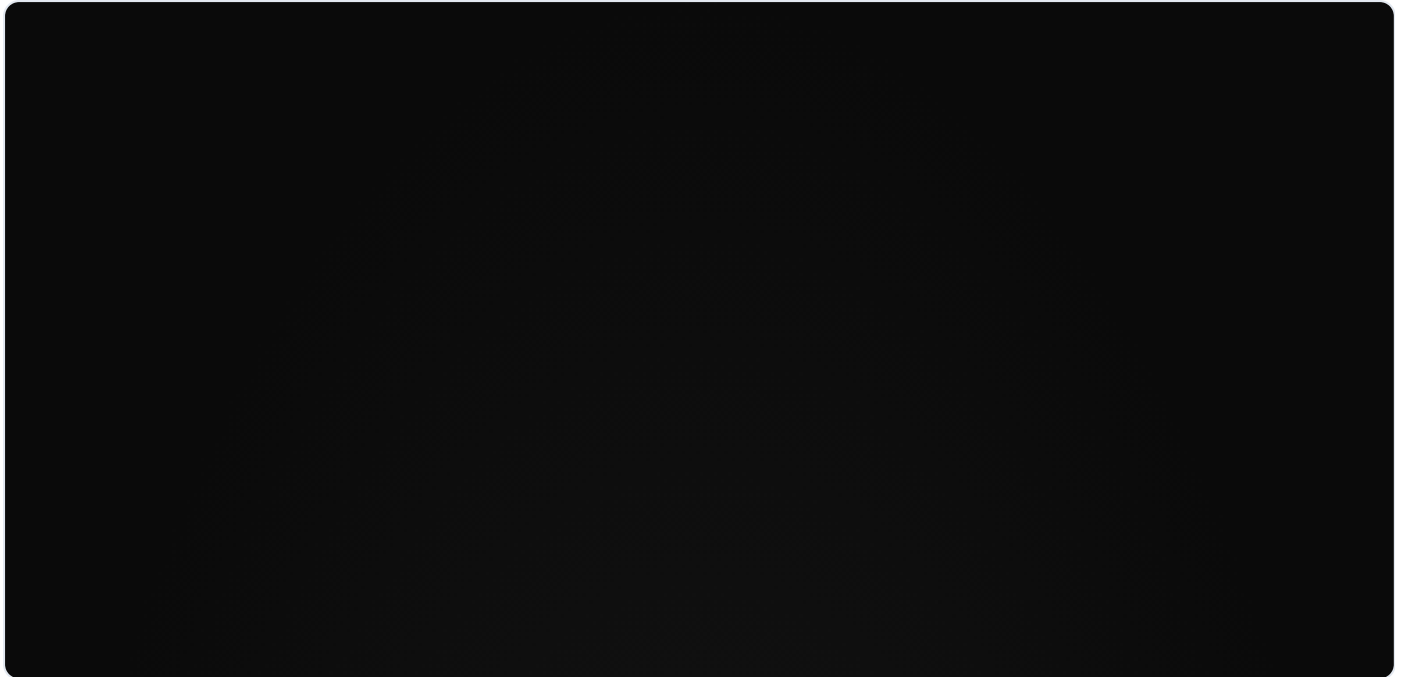
At a glance

The checks that decide most of this verdict.

Malware engines	15 flagged it VirusTotal	RISK
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	15% confidence AbuseIPDB, 4 reports; shared hosting inflates reports	CLEAR
Domain age	18 days old Most scam domains are under a year old	RISK
Web archive	Archived since 2026 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://multiplay.at/>



What multiplay.at 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).
- Public web-archive history exists since 2026.
- 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.

This website is a landing page for “Multi Roblox Manager,” a free Chrome extension that presents local management and simultaneous launching of multiple Roblox accounts. It offers a downloadable ZIP package and developer-mode installation instructions, with claims that account data remains on the device and that no account registration is required.

Scam/Impersonation Risk

The website’s stated purpose is a benign utility, and its homepage contains no login form, payment request, or obvious phishing mechanism. However, this positive page-level presentation is outweighed by confirmed external malicious detections and blacklist findings associated with the assessed domain. The site also distributes executable browser-extension content through a developer-mode unpacked installation, which increases the consequences of any compromise or supply-chain manipulation. Four abuse reports concern the observed shared hosting IP rather than being conclusively attributed to this site, but that attribution does not

remove the independent domain-level reputation concern. The available evidence therefore supports a clearly cautionary posture for installation, credential handling, or other sensitive interaction.

EVIDENCE

- The homepage presents a downloadable Chrome extension ZIP and instructs visitors to use Chrome Developer Mode to load it unpacked.
- External reputation checks recorded 15 malicious detections and confirmed blacklist status for the assessed domain.
- The hosting IP had 4 abuse reports; the records attribute these reports to shared provider infrastructure rather than specifically to the website.

Regulatory Verification Notes

The site presents a software utility rather than a regulated financial service, and no licensing claim is relevant to the stated product. Nevertheless, the supplied page evidence does not identify a legal operating entity, publisher identity, or accountable organization, leaving the real-world operator unverified. The absence of visible legal and publisher disclosures is a material transparency gap for software distributed outside a conventional extension marketplace. A separate broker-reputation dataset produced no match; that is limited contextual information and does not establish legitimacy or regulatory standing.

EVIDENCE

- The homepage and FAQ describe the extension and its installation process but do not identify a legal entity or publisher.
- The supplied site content contains no license number, registration detail, or regulatory authorization claim.
- The site's transport encryption uses a DV certificate issued by YR2, valid through 2026-12-20; certificate validity authenticates encrypted transport, not the operator's identity.

What to Verify Next

An independent publisher identity should be established before any installation, including confirmation of the developer through an official, independently sourced channel and validation that the extension package has an authentic, reproducible provenance. The package should be analyzed in an isolated environment for permissions, update behavior, credential access, and network activity. Any claimed association with Roblox or another organization should be confirmed through that organization's independently published channels. The relevant domain and publisher details should also be checked against applicable registry or abuse-reporting records before deployment.

EVIDENCE

- The homepage offers a ZIP-based developer-mode installation rather than a conventional marketplace installation path.
- The site provides feature claims and usage counters but does not supply an independently verifiable publisher identity.
- Behavioral testing recorded no external XHR or POST activity, but this observation does not validate the downloaded extension package itself.

Summary Verdict

The overall posture is **critical trust risk**, with confirmed external reputation contradictions and insufficiently verified operator identity. The website's benign utility presentation does not provide a reliable basis for treating sensitive interaction or software installation as acceptable.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, which provides a mitigating layer against direct exposure but is not evidence of legitimacy; the origin server was not observable in the assessment. The observed hosting record identifies OVH - OVH SAS, France, on AS16276.

EVIDENCE

- Served through Cloudflare CDN/WAF; one observed edge IP was 162.19.136.21 and no origin candidate was identified.
- Hosted on AS16276 (OVH - OVH SAS, FR).
- TLS certificate validation level is DV, issued by YR2, with expiry at 2026-12-20T19:36:18+00:00.

Closing Assessment

Prospective users should limit activity to passive review until the publisher, package provenance, and software behavior have been independently validated; installation, credential use, and deployment on production systems should not proceed on the current evidence.

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, 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
- A large share of what the page loaded came from other domains.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_MODERATE
- 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: 4 reports on hosting IP 162.19.136.21 (OVH GmbH, Data Center/Web Hosting/Transit), 15% confidence. The reports are attributed to shared infrastructure, not specifically to this website.

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 multiplay.at.

- The request stayed on multiplay.at. It was not redirected to another domain. [CLEAR](#)
- DNS for this domain is served by cloudflare.com, across 2 name servers. [NOTED](#)
- The earliest public archive of this site is from 2026-09-05. [CLEAR](#)
- It is hosted on OVH, from a server in FR. [NOTED](#)

Domain intelligence

Registrar	Not available
Hosting	OVH - OVH SAS, FR
Country	FR
Server IP	162.19.136.21
Name servers	carmelo.ns.cloudflare.com, mimi.ns.cloudflare.com
SSL issuer	YR2
SSL expiry	2026-12-20
Domain age	0.05 years (continuous registration)

Domain expiry	Not available
Archive first seen	2026-09-05
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 15 flagged AbuseIPDB: 15% confidence, 4 reports Google Safe Browsing: 0 matches

About this assessment

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