

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

threatdetect.org

Verdict

0

OUT OF 100

CRITICAL RISK

threatdetect.org 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

Russian-language minimal authorization/login page asking users to enter credentials; no explanatory content or trust signals present.

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	3 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	4.6 years old Registered history	CLEAR
Web archive	Archived since 2011 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://threatdetect.org/auth.php>



MONEY
BADGERS

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

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: 3 to 10 years (registration continuity).
- Public web-archive history exists since 2011.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Security Alert

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

This website is a Russian-language authorization page that presents only the prompts “Авторизация,” “Введите свои данные,” and an authorization control, with no visible explanation of the service, company, products, pricing, or business purpose; its apparent function is to collect user credentials.

Scam/Impersonation Risk

The site presents a **critical sensitive-interaction risk**. External security intelligence records the domain as blacklisted by multiple sources, including VT and EXTERNAL_BLACKLIST, with three malicious and four suspicious detections; one Tier 1 vendor also flagged it. The login-only presentation materially amplifies that concern because the page requests credentials while providing no context that would allow the operator, purpose, or destination of the authentication process to be understood. The supplied evidence does not establish a named-brand impersonation or conflicting legal identities, but the confirmed blacklist and malicious detections are sufficient to treat credential and financial interaction as unsafe.

EVIDENCE

- The authorization page contains only the Russian-language login prompts and no service or company explanation.
- The page contains one sensitive login form whose destination is classified as untrusted.
- External security assessment recorded 3 malicious and 4 suspicious detections, with Kaspersky listed among the flagged vendors; the domain was also recorded as blacklisted.
- Registration records identify GoDaddy.com, LLC and a creation date of 2022-01-28, with an age of 4.56 years; archival coverage is recorded from 2011-09-06 through 2025-07-19, spanning 15 years tracked.

Regulatory Verification Notes

No company name, license, registration number, regulated-service disclosure, terms, or other accountability information is visible in the inspected content. This is a significant transparency gap for a page soliciting credentials, although the absence of a licensing statement alone is not proof of fraud. The available broker-reputation dataset contains no match, which is only a limited contextual signal and does not establish licensing or legitimacy. The site has transport encryption, but a domain-validated certificate confirms control of the domain rather than the identity or authorization of its operator.

EVIDENCE

- The inspected page provides no visible corporate, licensing, registration, terms, or regulated-entity disclosure.
- The site's hosting infrastructure is AS20860, IOMART-AS — IOMART CLOUD SERVICES LIMITED, GB.
- TLS uses issuer YR1 with DV validation and is valid to 2026-10-23T00:02:02+00:00.
- The broker-reputation lookup returned no match.

What to Verify Next

Sensitive interaction should remain suspended while the domain's role and operator are independently established. Any claimed financial or regulated function should be checked directly against the relevant regulator's registry using an independently sourced organization name, and official contact channels should be confirmed through an offline or separately trusted route. If credentials have already been entered, affected passwords should be changed from a known-clean device, reused credentials should be rotated, and relevant account activity should be reviewed.

EVIDENCE

- The only observed page is a login-only page with unclear purpose and no visible business context.
- The submitted form is classified as sensitive and directed to an untrusted destination.
- The available identity-verification status is unverified.

Summary Verdict

The overall posture is critical, with the available evidence indicating that the website is not suitable for login, credential submission, or financial interaction. Its apparent legitimacy and connection to a real-world operator

are not established, and the adverse external signals outweigh the limited technical evidence of normal site operation.

Infrastructure Integrity

The site resolves to a single likely origin IP hosted by IOMART Cloud Services Limited in Great Britain on AS20860, with no detected CDN or edge-IP layer. This provides a technically identifiable hosting position but no legitimacy assurance; the use of standard hosting and TLS does not offset the site’s content and reputation risks.

Closing Assessment

The domain should be treated as unsuitable for sensitive use unless an independent investigation confirms its operator, purpose, and accountability through trusted channels.

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 governance, page content, registration and ownership, analysis engine, external reputation.

01 Governance Risk

- A form asking for sensitive information submits somewhere TrustSniffer could not verify, which caps how far the score can rise.

Governance rule:GOV_SENSITIVE_FORM_UNTRUSTED

- The page presents a sign-in form, and the operator behind it could not be independently verified.

Page content rule:PAGE_TYPE_LOGIN_UNVERIFIED

- 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 form on the page submits to a destination TrustSniffer could not verify.

Page content rule:PAGE_FORM_UNTRUSTED_DEST

- The page asks visitors for sensitive information.

Page content rule:PAGE_FORM_SENSITIVE

- A sign-in path on this site handles sensitive information.

Page content rule:PAGE_LOGIN_PATH_SENSITIVE

- 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 threatdetect.org.

- The request stayed on threatdetect.org. 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 2027-01-28. NOTED
- The earliest public archive of this site is from 2011-09-06. CLEAR
- It is hosted on IOMART-AS, from a server in GB. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	IOMART-AS - IOMART CLOUD SERVICES LIMITED, GB
Country	GB
Server IP	78.129.252.31
Name servers	ns67.domaincontrol.com, ns68.domaincontrol.com
SSL issuer	YR1
SSL expiry	2026-10-23
Domain age	4.56 years (continuous registration)
Domain expiry	2027-01-28
Archive first seen	2011-09-06
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 3 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about threatdetect.org 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/threatdetect.org> · assessed 2026-08-21