

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

agrocom.ge

Verdict

0

OUT OF 100

CRITICAL RISK

agrocom.ge 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 2026-08-20 by automated analysis. Classification confidence 55%.

What this site appears to be

Georgian-language ecommerce site 'აგრო-კომ' offering agricultural machinery, seeds, fertilizers, irrigation systems and related services with contact information and product listings.

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.

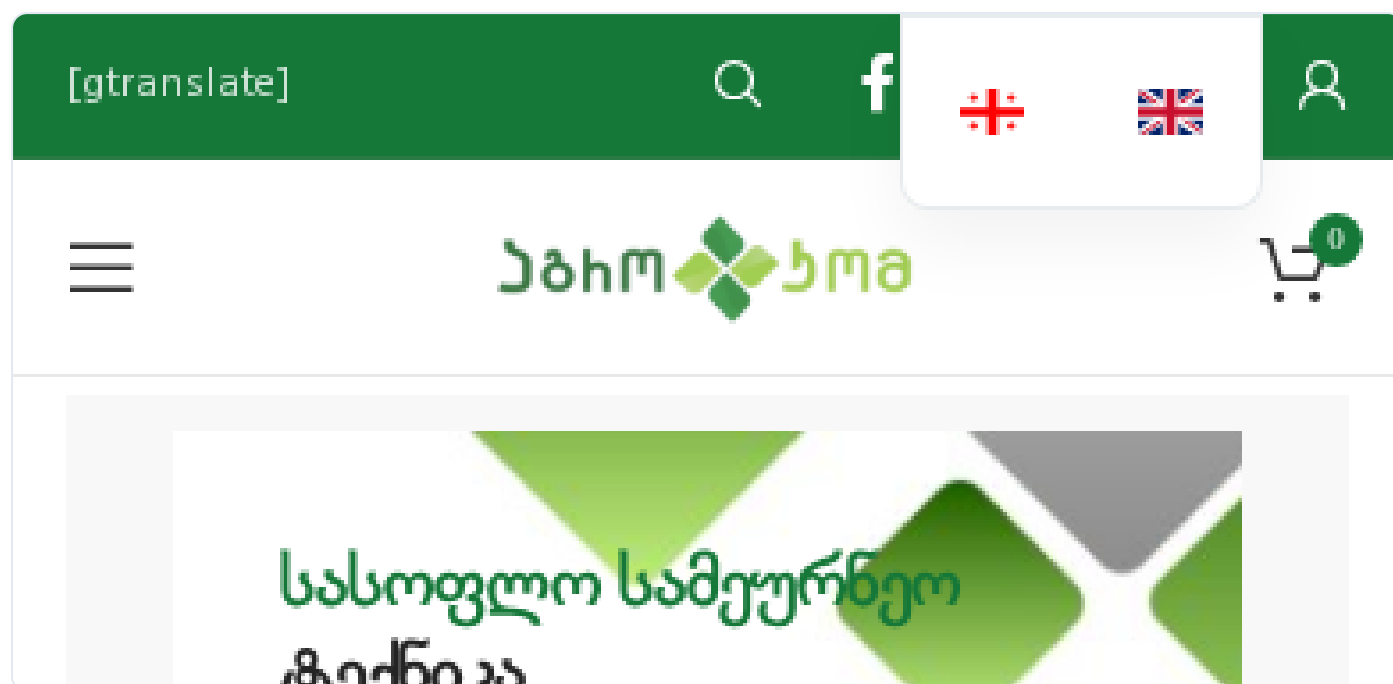
At a glance

The checks that decide most of this verdict.

Malware engines	13 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	14 years old Registered history	CLEAR
Web archive	Archived since 2013 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://agrocom.ge/>



What agrocom.ge served when TrustSniffer captured it on 2026-08-20. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2013.
- 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.

The website is a Georgian-language online agricultural-commerce storefront presenting agricultural machinery, seeds, fertilizers, plant-protection products, irrigation systems, cold-storage technology, installation services, and consulting, with the apparent business model of selling equipment and agricultural supplies through an online product catalogue.

Scam/Impersonation Risk

The site presents a coherent commercial storefront, and no page-level brand impersonation, phishing, or conflicting legal-entity identity was identified. However, the domain is subject to a confirmed blacklist finding supported by multiple external malicious detections, including 13 malicious classifications, which is a material contradiction to the otherwise ordinary ecommerce presentation. Browser analysis also recorded six suspicious inline scripts, substantial post-interaction DOM changes, elevated console errors, and a login form; these signals do not establish the site's purpose by themselves, but they materially increase the risk associated with

credentials and other sensitive interactions. The site's apparent agricultural business model therefore does not offset the external threat evidence.

EVIDENCE

- Homepage: Georgian-language agricultural product catalogue with machinery, seeds, fertilizers, irrigation systems, and related services; no page-level impersonation or phishing indicator was identified.
- Homepage and interactive pages: six suspicious inline scripts, 24 console errors, and a maximum post-interaction DOM difference of 7,382.
- Homepage: login, search, and contact/registration forms are present; no hidden sensitive form or external password-submission destination was detected.
- Domain registration record: registered 2012-11-06; age 13.79 years.

Regulatory Verification Notes

The available content does not present a licensing claim, license number, or clearly identified regulated status. That is a disclosure and verification gap rather than proof of fraud, particularly because the visible business model is general agricultural retail and services rather than an expressly regulated financial activity. The operator's real-world identity remains independently unverified, and the site should not be treated as legally established solely because it uses a commercial brand name. The available third-party broker dataset produced no match and therefore adds neither adverse nor affirmative regulatory evidence.

EVIDENCE

- Homepage: presents agricultural retail, installation, and consulting services but no license authority or license number.
- Domain registration record: registrar listed as domenebi.ge; creation date 2012-11-06 and expiration date 2026-11-07.
- Hosting and transport records: served through AS31898, identified as ORACLE-BMC-31898 — Oracle Corporation, US.
- TLS certificate: issued by YR2, domain-validated (DV), valid through 2026-10-22.

What to Verify Next

Before any credential submission, account creation, payment, or other sensitive action, an independent party should confirm the operator's legal name, business registration, physical trading presence, and applicable consumer-protection obligations through authoritative Georgian registries. Payment should be limited to methods offering chargeback or equivalent buyer protection until those checks are complete. Official contact channels should be confirmed through an independent, offline route, and any downloaded material or browser warnings associated with the domain should be investigated by the organization's security team.

EVIDENCE

- The identity-verification status is unverified, so operator attribution requires an independent registry check.
- The site's disclosed regulatory status is unclear, making confirmation of applicable registration or licensing requirements necessary.
- The external reputation assessment includes a confirmed blacklist finding and multiple malicious detections, warranting security review before sensitive interaction.

Summary Verdict

The website has a plausible agricultural-commerce presentation but carries a **critical sensitive-interaction risk posture** because confirmed external threat detections and blacklist status outweigh the benign appearance of its catalogue and contact functionality. Its legitimacy and operator identity should be regarded as unverified rather than established.

Infrastructure Integrity

The site resolves directly to a likely origin address on AS31898, operated by ORACLE-BMC-31898 — Oracle Corporation in the United States, with no CDN or WAF identified. The valid DV TLS certificate protects transport confidentiality but confirms domain control only; neither the hosting arrangement nor the certificate establishes operator legitimacy.

Closing Assessment

Organizational policy should restrict the site to carefully controlled, read-only review until independent identity, legal-status, and security checks have cleared the external threat findings.

Written analysis generated 2026-08-20 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 rewrote itself after it was interacted with, so what a visitor first sees is not what they end up on.
Behaviour in a sandbox rule:BEHAV_DOM_DIFF_AFTER_INTERACTION
- The page replaced a large part of its own content after loading.
Behaviour in a sandbox rule:BEHAV_DOM_CHANGE_HIGH
- The page carried inline scripts written in a style TrustSniffer treats as suspicious.
Behaviour in a sandbox rule:BEHAV_SUSPICIOUS_INLINE_SCRIPTS
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- 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 agrocom.ge.

- The request stayed on agrocom.ge. It was not redirected to another domain. CLEAR
- Registration is published under domenebi.ge. CLEAR
- DNS for this domain is served by websitewelcome.com, across 2 name servers. NOTED
- The registration is paid up to 2026-11-07. NOTED
- The earliest public archive of this site is from 2013-07-03. CLEAR
- It is hosted on ORACLE-BMC-31898, from a server in US. NOTED

Domain intelligence

Registrar	domenebi.ge
Hosting	ORACLE-BMC-31898 - Oracle Corporation, US
Country	US

Server IP	192.185.76.137
Name servers	ns655.websitewelcome.com, ns656.websitewelcome.com
SSL issuer	YR2
SSL expiry	2026-10-22
Domain age	13.79 years (continuous registration)
Domain expiry	2026-11-07
Archive first seen	2013-07-03
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 13 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about agrocom.ge 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/agrocom.ge> · assessed 2026-08-20