

Is proishestviyagoodru.vercel.app a scam? TrustSniffer's high-risk assessment: 20/100

proishestviyagoodru.vercel.app

Verdict



20
OUT OF 100

CRITICAL RISK

proishestviyagoodru.vercel.app 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 2026-09-25 by automated analysis. Classification confidence 55%.

What this site appears to be

Russian-language page presenting a "Материалы дела" video and step-by-step instructions that instruct the user to download a file and enable installation from unknown sources. This pattern strongly suggests malicious payload distribution and social-engineering to bypass device security.

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.

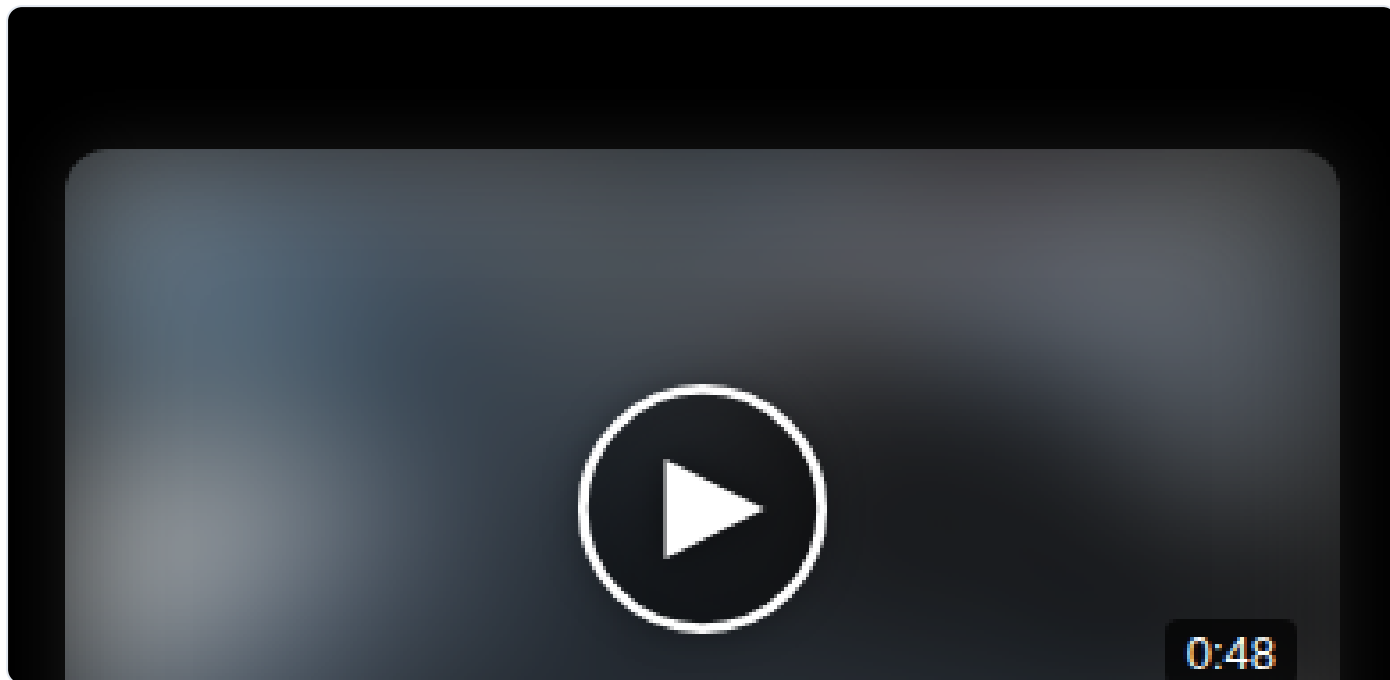
At a glance

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% confidence AbuseIPDB, 51 reports; shared hosting inflates reports	CLEAR
Domain age	Not available No registration record was returned	NOTED
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by WR1	NOTED

The page as captured

<https://proishestviyagoodru.vercel.app/>



What proishestviyagoodru.vercel.app served when TrustSniffer captured it on 2026-09-25. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- 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

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

The website is a Russian-language single-page site presenting itself as a restricted official case-record viewer, with an apparent purpose of directing visitors toward a downloadable file rather than providing a conventional commercial or institutional service.

Scam/Impersonation Risk

The site presents a materially elevated risk of malicious distribution. Its homepage refers to restricted case materials and a video recording, then instructs visitors to download a file, dismiss security warnings, enable installation from unknown sources, and install the downloaded item. That workflow is consistent with social engineering intended to bypass device protections, not with a credible document- or video-viewing service. Independent threat intelligence also records multiple malicious detections and a confirmed blacklist hit. No conflicting legal-entity names or explicit brand impersonation were observed, but the absence of those specific indicators does not offset the confirmed technical and content-based contradictions. A separate IP-abuse signal is not treated as site-specific because it was attributed to shared provider infrastructure, was whitelisted, and carried zero confidence.

EVIDENCE

- The homepage, titled “Перистратоп,” instructs visitors to download a file, select “download anyway” if warned, enable installation from an unknown source, and install it.
- The homepage is classified as malicious download and installation-instruction content, with browser behavior flags for APK installation, security-prompt bypass, and executable-payload download.
- External reputation checks recorded 6 malicious detections, including Kaspersky and Sophos, and confirmed blacklist presence from two sources.
- Abuse reporting recorded 51 reports against the shared IP, but the signal was attributed to shared provider infrastructure, whitelisted, and assigned a zero confidence score.

Regulatory Verification Notes

The available page does not identify a verifiable operating entity, license, registration number, or responsible organization. Its apparent purpose is therefore not supported by the normal legal and governance disclosures expected of an institutional records or media service, and the real-world operator remains unverified. This is a regulatory and transparency gap rather than a standalone finding of fraud; in this case, it must be assessed alongside the homepage’s malicious-download behavior and the external blacklist result. Transport encryption is present, but domain-validation TLS establishes encrypted transport only and does not authenticate the operator or the site’s claims.

EVIDENCE

- The homepage presents no stated license authority, license number, corporate identity, or regulatory registration.
- The homepage title is “Перистратоп,” with no metadata description, structured identity data, or visible institutional affiliation.
- The site is hosted on AS16509 (AMAZON-02 - Amazon.com, Inc., US).
- The TLS certificate is issued by WR1 at DV validation level and is valid to 2026-11-27T19:48:08+00:00.

What to Verify Next

The purported case material and event status should be validated through an independently sourced official authority, using contact details obtained outside this website. The downloaded file should not be opened or installed; any device on which it was downloaded should be examined with current endpoint-security tooling, and organizational security staff should be engaged if execution occurred. Access controls should block the domain and preserve the page, file, and related indicators for investigation.

EVIDENCE

- The homepage provides a direct download workflow rather than an independently verifiable institutional reference.
- The homepage has no login form, sensitive-input form, or external links that would provide an alternate verification route.
- The page presents a purported protocol number, event date, government-check status, and GLONASS/GPS recording claim without supporting authority or linked documentation.

Summary Verdict

The website has a critical trust posture and should be treated as unsuitable for sensitive interaction. The convergence of malicious-download instructions, confirmed blacklist status, multiple threat detections, and unverified operator identity outweighs the presence of basic encrypted transport. The evidence is consistent with a site intended to induce unsafe file installation rather than provide a trustworthy public service.

Infrastructure Integrity

The site is positioned behind Cloudflare CDN/WAF infrastructure, and all observed addresses were edge addresses with no origin candidate identified. The hosting environment also includes Vercel and Amazon infrastructure; these protections may reduce direct exposure of the origin and support delivery resilience, but they do not establish legitimacy or counter the site-specific threat evidence.

Closing Assessment

Interaction should be suspended, the domain should be blocked in relevant security controls, and any affected device or account should be handled under the organization’s malware-response procedures.

Written analysis generated 2026-09-25 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.

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

Signals weighed against the site

- AbuseIPDB: 51 reports on hosting IP 216.198.79.3 (Vercel, Inc, Content Delivery Network), 0% 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 proishestviyagoodru.vercel.app.

- The request stayed on proishestviyagoodru.vercel.app. It was not redirected to another domain. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	Not available
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	216.198.79.3
Name servers	Not available
SSL issuer	WR1
SSL expiry	2026-11-27
Domain age	Not available (no registration date was returned)
Domain expiry	Not available
Archive first seen	Not available
Archive snapshots	0
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0% confidence, 51 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about proishestviyagoodru.vercel.app 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/proishestviyagoodru.vercel.app> · assessed 2026-09-25