

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

antaresns.com

Verdict

0

OUT OF 100

CRITICAL RISK

antaresns.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

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

What this site appears to be

Simple hosting account activation/marketing page (Serbian). Provides contact phone, email, link to provider site and offers paid website creation.

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.

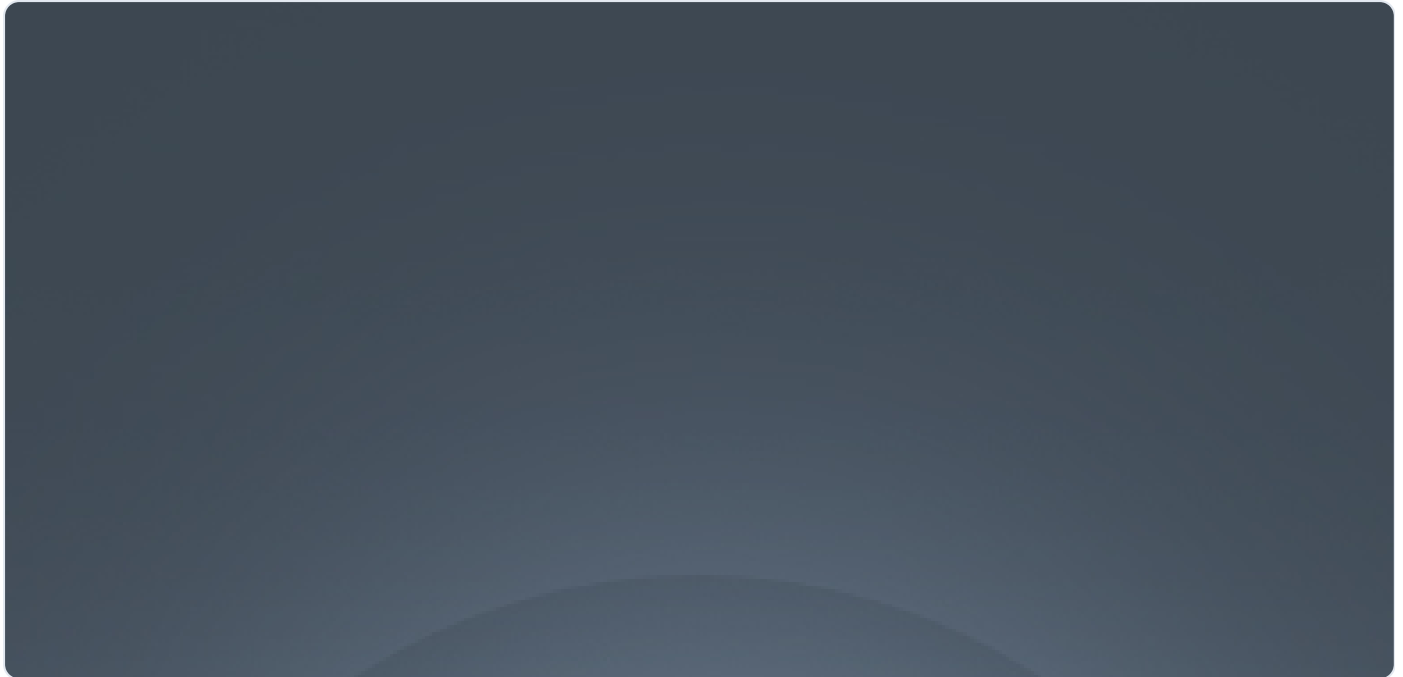
At a glance

The checks that decide most of this verdict.

Malware engines	10 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	7.4 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://antaresns.com/>



What antaresns.com served when TrustSniffer captured it on 2026-08-20. 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 2021.
- 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.

The website is a simple hosting-account activation and marketing page branded as “Orion Telekom Hosting.” It tells visitors that a hosting account is active, directs them to an external provider website for further information, publishes telephone and email contact details, and promotes paid website creation completed within 48 hours; its apparent business model is web hosting, domain registration, and one-time website-development services.

Scam/Impersonation Risk

The site presents a conventional hosting-service proposition and the homepage shows no login form, credential-collection form, wallet interaction, or explicit phishing content. However, this benign page presentation is outweighed by confirmed external threat detections and blacklist status: multiple security assessments classify the domain as malicious, including ten malicious detections and one suspicious detection. The available evidence does not establish a separate brand-impersonation or phishing identity conflict, but the external reputation signal is sufficient to create a critical risk for sensitive interaction. The domain’s apparent operator

identity also remains unverified, so the page's "Orion Telekom" branding should not be treated as independently authenticated.

EVIDENCE

- The homepage is a hosting-account notification and marketing page with no login form, hidden form, password-external form, wallet connection, or clipboard-hijacking behavior.
- External reputation telemetry records 10 malicious detections and 1 suspicious detection; the domain is listed on external blacklists.
- The domain was registered on 2019-04-05 and is approximately 7.38 years old.
- Archive coverage spans 2021-11-25 through 2025-07-10, with 5 years tracked.

Regulatory Verification Notes

The homepage describes hosting, domain-registration, and website-development services but does not state a licensing authority or license number. That is a disclosure gap requiring clarification rather than, by itself, proof of wrongdoing. The page links its branding to the Orion Telekom web presence, but the available evidence does not independently verify the legal entity operating this domain. A valid domain-validated TLS certificate and identifiable Serbian hosting infrastructure provide technical continuity, not regulatory or corporate authentication.

EVIDENCE

- The homepage presents the service model as hosting, domain registration, and paid website creation and contains no stated license number or licensing authority.
- The domain registrar is PDR Ltd. d/b/a PublicDomainRegistry.com.
- The site resolves through AS9125, operated by ORIONTELEKOM-AS - Društvo za komunikacije Orion telekom doo Beograd-Zemun, RS.
- TLS is issued by YR2 at DV validation level and is valid until 2026-10-10.

What to Verify Next

Sensitive interaction should remain suspended until the domain's security reputation has been independently resolved and the operating entity has been authenticated through authoritative records. Any prospective commercial engagement should confirm the provider's legal identity, service terms, refund arrangements, and applicable business registration or licensing position through an independent registry; contact channels should also be validated through an independently obtained route rather than relying solely on the webpage.

EVIDENCE

- The homepage directs visitors to a separate provider website, creating a specific opportunity to compare branding, domain ownership, service terms, and contact details across the two sites.
- The published page offers paid services but does not provide the legal or licensing particulars needed for independent regulatory confirmation.
- The external security detections remain the principal unresolved blocker for account, credential, or payment activity.

Summary Verdict

The website has a **critical trust posture** for sensitive interaction. Its ordinary hosting-page appearance and technically valid transport encryption do not offset the confirmed malicious detections and blacklist status, while the real-world operator remains unverified.

Infrastructure Integrity

The site is protected by Cloudflare CDN/WAF infrastructure, with observed Cloudflare edge addresses including 104.21.7.234, 172.67.156.135, 2606:4700:3031::6815:7ea, and 2606:4700:3031::ac43:9c87 on AS13335. The resolved hosting infrastructure also identifies AS9125 and the Orion Telekom hosting organization at 77.105.36.229. These protections mitigate direct exposure and provide identifiable network context, but they do not establish legitimacy.

Closing Assessment

Sensitive actions, including credential submission, account access, and payment activity, should not proceed unless the external detections are independently cleared and the operator is authenticated through authoritative, out-of-band channels.

Written analysis generated 2026-08-20 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by analysis engine, behaviour in a sandbox, external reputation.

01 Sensitive Interaction Risk

- The analysis matched a pattern TrustSniffer treats as a direct threat to a visitor.
Analysis engine signal:direct_threat
- Most of what the page loaded came from other domains rather than from this one.
Behaviour in a sandbox rule:BEHAV_EXTERNAL_RATIO_HIGH
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- 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
- 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 antaresns.com.

- The request stayed on antaresns.com. It was not redirected to another domain. CLEAR
- Registration is published under PDR Ltd. d/b/a PublicDomainRegistry.com. CLEAR
- DNS for this domain is served by orion.rs, across 4 name servers. NOTED
- The registration is paid up to 2027-04-05. NOTED
- The earliest public archive of this site is from 2021-11-25. CLEAR
- It is hosted on ORIONTELEKOM-AS, from a server in RS. NOTED

Domain intelligence

Registrar	PDR Ltd. d/b/a PublicDomainRegistry.com
Hosting	ORIONTELEKOM-AS - Drustvo za telekomunikacije Orion telekom doo Beograd-Zemun, RS
Country	RS
Server IP	77.105.36.229
Name servers	DNS1.ORION.RS, DNS2.ORION.RS, DNS3.ORION.RS, DNS4.ORION.RS
SSL issuer	YR2
SSL expiry	2026-10-10
Domain age	7.38 years (continuous registration)
Domain expiry	2027-04-05
Archive first seen	2021-11-25
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 10 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about antaresns.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.

