

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

ariesmusic.com

Verdict

0

OUT OF 100

CRITICAL RISK

ariesmusic.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

Governance Risk

Assessed 2026-08-21 by automated analysis. Classification confidence 75%.

What this site appears to be

A music label/publishing website listing albums and genres with a newsletter signup. Content is catalog-driven, no payment forms or investment solicitations visible.

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	11 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	23 years old Registered history	CLEAR
Web archive	Archived since 2000 214 snapshots	CLEAR
Certificate	Encrypted connection Issued by YR2	NOTED

The page as captured

<https://ariesmusic.com/>



What ariesmusic.com served when TrustSniffer captured it on 2026-08-21. 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 2000.
- 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.

Ariesmusic.com presents itself as a music label and publishing website, displaying an artist and album catalog across genres including Chicano Rap, Regional Mexican, Karaoke, Children's, and Electronic/New Age, with a newsletter subscription mechanism and an apparent focus on music promotion, licensing, and catalog discovery.

Scam/Impersonation Risk

The site's visible content is comparatively benign and does not show payment forms, investment solicitations, login functionality, or obvious brand-impersonation content. However, this presentation conflicts materially with external security evidence: the domain is blacklisted, multiple threat-intelligence detections classify it as malicious, and Fortinet and Sophos are among the vendors identifying a threat. Controlled interaction also recorded two wallet-drainer runs, two non-whitelisted external post destinations, substantial DOM changes, and repeated console errors. These behavioral indicators are not explained by the visible music-catalog purpose and materially increase the risk of sensitive interaction. No separate identity inconsistency or confirmed brand-impersonation finding was observed.

EVIDENCE

- The homepage presents album listings, genre filters, videos, and a newsletter form, with no sensitive payment or login form visible.
- External security telemetry recorded 11 malicious detections and a confirmed blacklist hit, including Fortinet and Sophos.
- Controlled interaction recorded wallet-drainer behavior in 2 runs and 2 non-whitelisted external posts.
- The domain was registered in 2004 and is approximately 22.61 years old; archival records contain 214 snapshots spanning 2000–2025, covering 26 tracked years.

Regulatory Verification Notes

The apparent music-publishing purpose does not itself establish the legal identity or operating authority of the entity behind the website. Identity verification remains unconfirmed, and the available page analysis does not identify a claimed license, licensing authority, or license number. This is a verification gap rather than independent proof of misconduct, but it is significant when considered alongside the external security findings. The technical service configuration shows ordinary domain registration and encrypted transport, yet those controls do not validate the operator or neutralize the reputation warnings.

EVIDENCE

- The homepage is titled “Home - Aries Music Entertainment” and provides catalog and publishing-oriented content without a stated license authority or license number.
- The domain registrar is GoDaddy.com, LLC.
- The site is served from AS31898, identified as ORACLE-BMC-31898 – Oracle Corporation, US.
- TLS uses issuer YR2 with DV validation and is valid through 2026-10-24.

What to Verify Next

Any prospective engagement should first establish the responsible legal entity through independent corporate or rights-management records and confirm that the entity is authorized to provide the stated publishing or licensing services. Official contact channels should be confirmed through an independent source rather than relying solely on the website. Until the security detections and behavioral findings are independently resolved, interaction should remain limited to passive viewing; account creation, credential submission, downloads, financial activity, and any browser or wallet authorization should not occur.

EVIDENCE

- The site provides catalog and publishing material but does not present independently verified operator or licensing information.
- The visible form is a newsletter subscription form and is not identified as a payment or credential form.
- External security detections and controlled-interaction findings require resolution before sensitive use.

Summary Verdict

The overall posture is **critical risk for sensitive interaction**. The website's apparently ordinary public-facing content is outweighed by corroborated external threat detections, a confirmed blacklist status, and suspicious

controlled-interaction behavior. The operator’s real-world identity is not independently verified, so the site cannot be treated as an established legitimate service for sensitive activity.

Infrastructure Integrity

The site resolves to a single likely origin IP, with no CDN detected and no edge IPs identified. Its hosting infrastructure is associated with Oracle Corporation in the United States; the valid DV certificate provides transport encryption but is only a limited mitigating control and does not establish site legitimacy.

Closing Assessment

The appropriate enterprise posture is passive, read-only observation only; login, credential, financial, download, and authorization activity should remain blocked unless independent verification and security remediation produce clear contrary evidence.

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 registration and ownership, analysis engine, behaviour in a sandbox, external reputation.

01 Governance Risk

- The registration record withholds contact details for the operator.
Registration and ownership rule:KF_WHOIS_HIDDEN
- Registration details are held behind a privacy service, so no operator is named publicly. This is common and legal, and it also means there is nobody to check.
Registration and ownership rule:KF_WHOIS_PRIVATE

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 sent data to a destination TrustSniffer does not recognise.
Behaviour in a sandbox rule:BEHAV_NONWHITELISTED_POSTS
- The structure of the page changed sharply while it was loading.
Behaviour in a sandbox rule:BEHAV_DOM_DENSITY_SPIKE
- The page behaved in a way consistent with a crypto wallet drainer.
Behaviour in a sandbox rule:BEHAV_WALLET_DRAINER_SUSPECT
- 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	25%
----------------------------------	-----

- 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 ariesmusic.com.

- The request stayed on ariesmusic.com. It was not redirected to another domain. CLEAR
- Registration is published under GoDaddy.com, LLC. CLEAR
- DNS for this domain is served by midnites.net, across 2 name servers. NOTED
- The registration is paid up to 2027-01-15. NOTED
- The earliest public archive of this site is from 2000-11-10. CLEAR
- It is hosted on ORACLE-BMC-31898, from a server in US. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	ORACLE-BMC-31898 - Oracle Corporation, US
Country	US
Server IP	192.185.187.53
Name servers	NS1.MIDNITES.NET, NS2.MIDNITES.NET
SSL issuer	YR2
SSL expiry	2026-10-24
Domain age	22.61 years (continuous registration)
Domain expiry	2027-01-15
Archive first seen	2000-11-10
Archive snapshots	214
Reputation	VirusTotal: 11 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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

