

Is broadnetla.net a scam? TrustSniffer's high-risk assessment: 5/100

broadnetla.net

Verdict

5

OUT OF 100

CRITICAL RISK

broadnetla.net 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

Broadnet (PonleMás) is an Ecuadorian corporate site describing a large independent retail network for prepaid services and POS solutions, with contact details and service descriptions. No forms requesting credentials or payments visible on this page.

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 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	18 years old Registered history	CLEAR
Web archive	Archived since 2011 Public history exists	CLEAR
Certificate	Encrypted connection Issued by Sectigo Public Server Authentication CA DV R36	NOTED

The page as captured

https://broadnetla.net/



What broadnetla.net 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 2011.
- At least one reputation service TrustSniffer consulted had flagged this domain at assessment time.

Full analysis

Overview

Broadnet's website presents PonleMás as an Ecuadorian independent retail-services network offering prepaid electronic top-ups, merchant services, POS and virtual POS solutions, network-management tools, and customer or retailer support; its apparent business model is transaction processing and related platform services for retail points and merchants.

Scam/Impersonation Risk

Confirmed external threat detections and blacklist results create a material risk for sensitive interaction with the site, despite the absence of obvious malicious mechanics in the observed page. The homepage presents a coherent corporate-service proposition, and testing found no login form, credential-collection form, hidden sensitive form, wallet connection, or payment-request workflow. No separate legal-entity conflict or brand-impersonation finding was identified, but those benign page characteristics do not offset the confirmed reputation contradiction. The website's published contact channel also contains a contact-channel integrity anomaly: info@broadnetla.come appears to use a deliverability-breaking typo or possible typosquat domain ending.

EVIDENCE

- External reputation evaluation recorded 6 malicious and 1 suspicious detections, with the domain also identified by confirmed blacklist sources.
- The homepage is classified as a corporate/service page and contains no visible login form, sensitive form, hidden form, or credential request.
- Behavioral testing recorded no wallet connection, wallet-drainer activity, clipboard hijacking, cloaking, or suspicious inline scripts on the homepage.

Regulatory Verification Notes

The site identifies itself as “Broadnet, Red de Servicios Independiente del Ecuador” and describes the PonleMás network, prepaid services, electronic services, POS products, and network-management functions. The available material does not show a claimed license, regulatory authority, or license number; this is a verification and disclosure gap rather than, by itself, proof of fraud. The operator’s real-world identity remains unverified, while the site’s long registration history and stable technical presentation provide background continuity but do not resolve the external threat findings. No broker-sector match was identified in the available third-party context.

EVIDENCE

- Domain registered in 2008-08-15T23:21:34Z, with an age of 18.02 years; registrar: GoDaddy.com, LLC.
- Archive coverage records a first observation on 2011-02-27T03:45:58Z, a last observation on 2026-01-08T00:21:28Z, and 16 years tracked.
- The homepage title is “Broadnet, Red de Servicios Independiente del Ecuador,” and its navigation includes “Quienes Somos,” “Certificaciones y políticas,” and “Denuncias.”
- The site’s transport encryption uses a DV certificate issued by Sectigo Public Server Authentication CA DV R36, valid until 2026-09-30T23:59:59+00:00.

What to Verify Next

Before any login, credential submission, merchant onboarding, or financial transaction, the prospective user should independently confirm the operating entity and the applicable authorization status through the relevant Ecuadorian corporate or regulatory registries. Official contact channels should be validated through an independently sourced business record or offline route rather than relying solely on contact details presented on the site. Any proposed payment or account action should remain suspended until those checks are consistent with the intended Broadnet or PonleMás relationship.

EVIDENCE

- The homepage identifies the business as an Ecuadorian retail-services network and claims more than 14,000 points of sale.
- The homepage provides “CALL CENTER,” “Contáctenos,” “Afiliate a la Red,” and “Ingresar” pathways, creating identifiable channels for independent confirmation.
- The available page analysis found no visible forms requesting credentials or payments, so verification should focus on the legitimacy of any subsequent interaction reached through those pathways.

Summary Verdict

The overall posture is critical and unsuitable for sensitive interaction. Apparent corporate content and technically stable presentation are outweighed by confirmed external threat detections and blacklist status, while the site's real-world operator identity is not independently verified.

Infrastructure Integrity

The site resolves directly to a single likely origin address rather than through a detected CDN or WAF edge network. Hosting is provided by Unified Layer in the United States; this is ordinary hosting infrastructure and offers no independent assurance of legitimacy.

EVIDENCE

- Served from AS46606, Unified Layer, US, at 143.95.108.238.
- Infrastructure resolution identified 1 unique IP, 0 edge IPs, and 1 likely origin IP.
- No CDN was detected; the infrastructure record nevertheless marks the hosting environment as resolved and identifies ARIN as the registry.

Closing Assessment

Sensitive actions should not proceed until the operator, applicable authorization, and official communication channels have been independently validated; read-only observation is the proportionate interim posture.

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, 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
- 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 broadnetla.net.

- The request stayed on broadnetla.net. 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 2027-08-15. NOTED
- The earliest public archive of this site is from 2011-02-27. CLEAR
- It is hosted on UNIFIEDLAYER-AS-1, from a server in US. NOTED

Domain intelligence

Registrar	GoDaddy.com, LLC
Hosting	UNIFIEDLAYER-AS-1 - Unified Layer, US
Country	US
Server IP	143.95.108.238
Name servers	NS29.DOMAINCONTROL.COM, NS30.DOMAINCONTROL.COM
SSL issuer	Sectigo Public Server Authentication CA DV R36
SSL expiry	2026-09-30
Domain age	18.02 years (continuous registration)
Domain expiry	2027-08-15
Archive first seen	2011-02-27
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 6 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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