

Is mycocorporation.com safe? TrustSniffer's low-trust assessment: 40/100

mycocorporation.com

Verdict

40

OUT OF 100

LOW TRUST

mycocorporation.com is low-trust and potentially risky.

Several risk patterns were present. Do not send money or personal details until you have verified this business another way.

Sensitive Interaction Risk

Governance Risk

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

What this site appears to be

A small administrative Antibot dashboard page (v2.0) showing configuration status and an API key snippet. No visible forms, monetization, or external links in the captured content. Sensitive credential appears in page text.

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	2 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	6.9 years old Registered history	CLEAR
Web archive	Archived since 2021 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YR1	NOTED

The page as captured

<https://mycocorporation.com/>

DASHBOARD (Antibot v.2.0)

Real Visitor Detection Manager.

What mycocorporation.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

Overview

The website presents a small administrative anti-bot dashboard labeled “Antibot v.2.0,” offering real-visitor detection, server-configuration status, and an API-key display rather than a clear consumer-facing commercial service.

Scam/Impersonation Risk

The site carries a clearly elevated interaction risk because external reputation evidence records two malicious determinations and a confirmed blacklist hit from two external sources. The captured dashboard also exposes a partially visible API credential in page text, indicating poor administrative security hygiene and creating a potential credential-compromise concern. The supplied content does not show brand impersonation or conflicting legal-entity names, so the principal contradiction is external reputation evidence rather than a demonstrated identity mismatch. The dashboard's limited content and absence of user-facing forms do not offset those findings.

EVIDENCE

- The homepage is titled “ANTIBOT DASHBOARD (Antibot v.2.0)” and displays an API-key snippet in the page text.
- External reputation evidence records `vt\_malicious: 2` and `external\_blacklist: true`.
- The domain was registered on 2019-10-12 and is recorded as approximately 6.86 years old.
- The archival record reports 0 snapshots, with first seen 2021-12-10, last seen 2025-07-12, and 5 years tracked.

Regulatory Verification Notes

The operator identity remains unverified, and the captured site material does not provide a clear legal entity, licensing status, registration number, or governance disclosure. This is a material verification gap for an organization considering the site as a managed security service, although the absence of a license claim is not by itself proof of fraud. The domain uses OnlineNIC, Inc. as registrar, and its transport security is valid but only domain-validated; these are technical or administrative facts, not independent confirmation of the operator's identity. No broker record was matched in the supplied third-party context.

EVIDENCE

- The captured homepage contains an administrative tool interface but no visible company, licensing, or registration disclosure.
- The domain registrar is OnlineNIC, Inc.
- TLS is issued by YR1 at DV validation level and is valid to 2026-10-07 11:39:37 UTC.
- The page capture contains no pricing, purchase flow, marketplace, or other visible commercial-service disclosure.

What to Verify Next

Before any operational adoption, an organization should independently identify the legal operator through a trusted corporate registry and confirm that the domain is authorized by that entity. Any security-service or managed anti-bot claims should be checked against contractual documentation, support contacts obtained through an independent route, and a controlled test environment. Any credential exposed by the administrative interface should be treated as compromised and revoked or replaced, and the domain should remain blocked from sensitive enterprise workflows until the external reputation contradiction is resolved.

EVIDENCE

- The homepage exposes an administrative configuration state and credential fragment without a visible authentication form.
- The captured page has no external links or visible contact pathway for independently validating the operator.
- Automated behavioral observation recorded 2 successful runs, 0 external XHR requests, and 0 hidden forms.

Summary Verdict

The overall posture is **low trust**, with a sensitive-interaction risk that is not suitable for routine credentialed, administrative, or financial use. The available evidence is insufficient to establish a trustworthy real-world operator, and the confirmed external reputation contradiction is decisive despite otherwise stable technical behavior.

Infrastructure Integrity

The website is protected by a CDN/WAF, which provides a mitigating layer against direct exposure and can reduce some forms of infrastructure abuse; it does not establish legitimacy. The observed edge infrastructure is associated with Hetzner Online GmbH in Germany, while the origin server was not observable in this analysis.

EVIDENCE

- Served from AS24940 (HETZNER-AS - Hetzner Online GmbH, DE), observed edge IP 65.108.131.33.
- CDN/WAF protection is present, with 1 observed edge IP and 0 origin candidates.
- The resolved infrastructure country is DE and the registry is RIPE NCC.

Closing Assessment

The appropriate posture is to restrict the site to controlled, read-only inspection and prevent login, credential submission, or financial activity until independent identity validation, credential remediation, and external reputation review are complete.

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.

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

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 mycocorporation.com.

- The request stayed on mycocorporation.com. It was not redirected to another domain. CLEAR
- Registration is published under OnlineNIC, Inc.. CLEAR
- DNS for this domain is served by futuresouls.com, across 2 name servers. NOTED
- The registration is paid up to 2029-10-12. CLEAR
- The earliest public archive of this site is from 2021-12-10. CLEAR
- It is hosted on HETZNER-AS, from a server in DE. NOTED

Domain intelligence

Registrar	OnlineNIC, Inc.
Hosting	HETZNER-AS - Hetzner Online GmbH, DE
Country	DE
Server IP	65.108.131.33
Name servers	WEBS00.FUTURESOULS.COM, WEBS01.FUTURESOULS.COM
SSL issuer	YR1
SSL expiry	2026-10-07
Domain age	6.86 years (continuous registration)
Domain expiry	2029-10-12
Archive first seen	2021-12-10
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 2 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

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