

Is rcf.co.mz a scam? TrustSniffer's high-risk assessment: 0/100

rcf.co.mz

Verdict

0

OUT OF 100

CRITICAL RISK

rcf.co.mz 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 2026-09-22 by automated analysis. Classification confidence 55%.

What this site appears to be

Index-style directory exposing multiple .exe files and a cgi-bin; no site content, contact, or legitimacy signals. High risk for malware distribution or compromised hosting.

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	18 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	6.4 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://rcf.co.mz/

Index of /			
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Forbes.exe	2026-08-12 11:26	822K	
Quote.exe	2026-08-17 08:58	821K	

What rcf.co.mz served when TrustSniffer captured it on 2026-09-22. 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 currently presents as a bare directory index rather than a functioning public service, exposing downloadable Windows executables and a CGI directory with no visible business model, contact information, or legitimacy narrative.

Scam/Impersonation Risk

Confirmed contradictions are present. The homepage exposes executable files named Forbes.exe, Quote.exe, cashout.exe, google.exe, love.exe, and mytimeiswriten.exe, alongside a cgi-bin directory. This presentation is consistent with a possible malware-distribution point or compromised hosting environment, not a transparent legitimate service. External security intelligence recorded multiple malicious and suspicious detections and a confirmed blacklist status; the absence of a detected brand-impersonation pattern does not offset those direct threat indicators. The domain's registration history is older than the currently observed directory content, but the available historical record does not establish a legitimate operational continuity for this file listing.

EVIDENCE

- The homepage is titled "Index of /" and lists multiple downloadable `.exe` files and a `cgi-bin/` directory.
- External assessment recorded 18 malicious detections and 4 suspicious detections, with Fortinet and Sophos among the flagged security providers.
- The domain was registered on 2020-05-03 and is approximately 6.39 years old, according to the registration record.
- Historical capture data records observations from 2021-12-22 through 2025-03-04, covering five tracked years.

Regulatory Verification Notes

The site provides no visible corporate identity, service description, licensing statement, registration number, or accountable contact information from which its operator or legal status could be independently established. Identity therefore remains unverified, and the absence of a clear legitimate business purpose is a material governance and disclosure gap. A valid transport certificate confirms encrypted delivery only; it does not authenticate the operator, validate the executable files, or establish regulatory standing. No matching broker profile was identified in the available third-party context, but that absence is not a licensing or legal determination.

EVIDENCE

- The homepage contains no legal, licensing, corporate, or contact disclosure and instead presents only a raw directory listing.
- The site is hosted on AS329184, operated by Host Africa (Pty) Ltd in South Africa.
- The transport certificate is Domain Validated, issued by YR1, and valid until 2026-12-04.
- The registration record identifies CIUEM Registrar and an expiration date of 2027-05-03.

What to Verify Next

Before any interaction beyond passive viewing, an organization should independently confirm whether the domain is authorized by a known operator through an offline or previously trusted channel. Any executable associated with the site should be handled as untrusted: it should not be downloaded or executed on production, employee, or personal systems, and any required examination should occur only in a controlled malware-analysis environment. If the domain is encountered in an enterprise environment, security teams should review endpoint, proxy, DNS, and download telemetry for related activity and preserve relevant files for analysis.

EVIDENCE

- The homepage exposes executable downloads without a stated publisher, purpose, or verification mechanism.
- The observed site has no login, payment, or legitimate service workflow that would provide a trustworthy basis for sensitive interaction.
- The available assessment identifies the site as a directory listing and potential malicious or compromised file host.

Summary Verdict

The website has a **critical trust posture** with sensitive-interaction risk. The evidence supports treating it as an untrusted and potentially malicious file-hosting endpoint rather than as an established service or accountable business.

Infrastructure Integrity

The site resolves directly to a single hosting endpoint and has no detected CDN or WAF layer. Its infrastructure is associated with Host Africa on AS329184 in South Africa; this provides a concrete hosting attribution but no legitimacy assurance, and the lack of an intermediary protection layer leaves the serving endpoint directly exposed.

EVIDENCE

- Infrastructure resolution identified one IP address, 102.218.213.96, with no edge IPs and no detected CDN.
- Hosting is provided by Host Africa (Pty) Ltd on AS329184, with AFRINIC listed as the registry.
- The site uses a Domain Validated TLS certificate issued by YR1, valid to 2026-12-04.

Closing Assessment

Prospective users and organizations should treat the domain as hostile, avoid downloading or executing its files, and block or isolate related activity pending independent incident-response review.

Written analysis generated 2026-09-22 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 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
- 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 rcf.co.mz.

- The request stayed on rcf.co.mz. It was not redirected to another domain. CLEAR
- Registration is published under CIUEM Registrar. CLEAR
- DNS for this domain is served by co.mz, across 2 name servers. NOTED
- The registration is paid up to 2027-05-03. NOTED
- The earliest public archive of this site is from 2021-12-22. CLEAR
- It is hosted on Host Africa (Pty) Ltd, from a server in ZA. NOTED

Domain intelligence

Registrar	CIUEM Registrar
Hosting	Host Africa (Pty) Ltd - Host Africa (Pty) Ltd, ZA
Country	ZA
Server IP	102.218.213.96
Name servers	ns2.lcservicos.co.mz, ns1.lcservicos.co.mz
SSL issuer	YR1
SSL expiry	2026-12-04
Domain age	6.39 years (continuous registration)
Domain expiry	2027-05-03
Archive first seen	2021-12-22
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 18 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about rcf.co.mz 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.

