

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

korexnode.xyz

Verdict

0

OUT OF 100

CRITICAL RISK

korexnode.xyz 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 2026-09-23 by automated analysis. Classification confidence 55%.

What this site appears to be

Dashboard for 'KorexNode' offering builder/Discord-bot driven malware: clipper, Exodus injection, token refresh, remote access and harvesting of credentials/sessions. Evident malicious intent to collect and relay stolen data.

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.

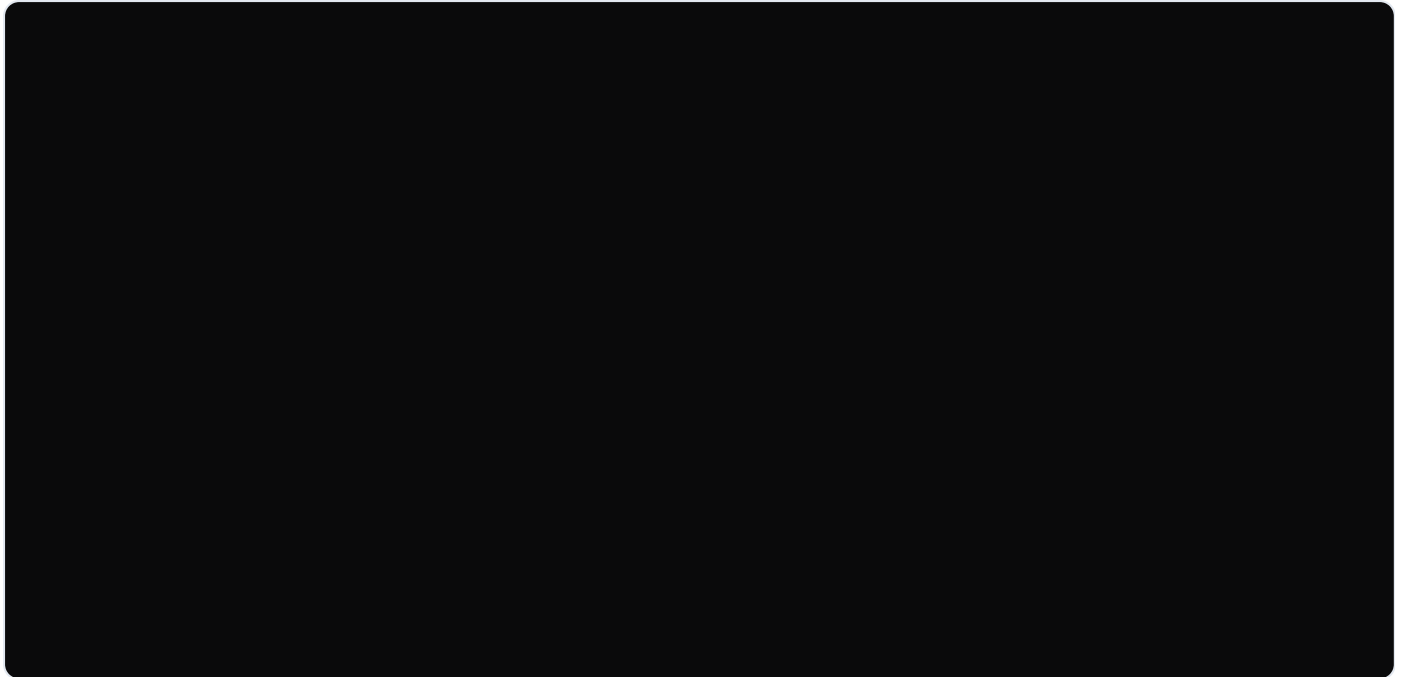
At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	11 days old Most scam domains are under a year old	RISK
Web archive	Archived since 2026 Public history exists	CLEAR
Certificate	Encrypted connection Issued by YE2	NOTED

The page as captured

<https://korexnode.xyz/>



What korexnode.xyz served when TrustSniffer captured it on 2026-09-23. The page may look different now.

Key findings

- Automated classification: Sensitive Interaction Risk.
- Domain age: less than 1 year (registration continuity).
- Public web-archive history exists since 2026.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Security Alert

Fortinet flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website is a KorexNode dashboard that presents tools for credential harvesting, session theft, wallet capture, remote access, and malware distribution, indicating an apparent malware-control and stolen-data monetization model rather than a legitimate consumer or business service.

Scam/Impersonation Risk

The site presents a **confirmed high-risk malicious-use pattern**. Its dashboard includes a clipper, Exodus wallet injection, Discord-based payload building, token refresh, remote access, keylogging, file management, shell access, and collection of browser, Discord, Telegram, and wallet data. It explicitly states that harvested credentials are relayed through a dualhook channel and that stolen sessions can be browsed through client files. The site also contains a login and token-submission surface, while observed page behavior includes credential-harvesting endpoints and automated exfiltration to webhooks. These are direct indicators of harmful activity, not merely ambiguous security weaknesses. The domain is blacklisted, and external threat detections reinforce the

page-level evidence. No separate brand-impersonation or conflicting legal-entity finding was established, but the confirmed blacklist and malicious functionality are sufficient to require a strongly cautionary posture.

EVIDENCE

- The dashboard page labels and exposes “Clipper,” “Exodus injection,” “Token Refresh,” “Keylogger,” “Shell Terminal,” “File Manager,” and remote-control functions.
- The dashboard page states that harvested credentials are sent to a dualhook channel and that client Discord, Telegram, and browser profiles can be browsed.
- The page contains a sensitive login, token-submission, and command-submission form with an untrusted destination.
- External reputation evidence records a confirmed blacklist hit and additional threat detections.

Regulatory Verification Notes

The apparent operator identity remains unverified, and the site does not present a credible licensing or legal-status basis for the activities shown. Its governance and ownership disclosures are opaque, while the available third-party broker context contains no matching record; that absence is contextual only and is not a legal or regulatory finding. The registration record identifies NICENIC INTERNATIONAL GROUP CO., LIMITED as registrar. The site's transport security provides encryption but does not establish operator identity, authorization, or legitimacy.

EVIDENCE

- The domain was registered in 2026 and is approximately 0.03 years old.
- The domain is registered through NICENIC INTERNATIONAL GROUP CO., LIMITED.
- The site is served on AS13335, CLOUDFLARENET - Cloudflare, Inc., US.
- The TLS certificate uses issuer YE2 with DV validation and is valid to 2026-12-12.

What to Verify Next

No account login, token submission, file upload, wallet interaction, or other sensitive exchange should occur. Security teams should block the domain and preserve relevant browser, endpoint, and network evidence if an individual or system has already interacted with it. Any purported association with a legitimate organization should be confirmed through an independently sourced channel rather than through the site itself. If credentials or session tokens were submitted, affected credentials should be rotated and active sessions revoked using the genuine service provider's established recovery process.

EVIDENCE

- The dashboard exposes credential, token, command, and client-control functionality requiring containment-oriented handling.
- The page analysis identifies credential-harvesting endpoints, malicious tooling, and automated webhook exfiltration.
- The available identity evidence does not independently connect the site to a verified real-world operator.

Summary Verdict

The website has a critical trust posture and should be treated as an actively harmful service rather than a legitimate platform. The convergence of malicious dashboard functionality, sensitive data-collection mechanisms, external threat detections, and confirmed blacklisting makes sensitive interaction inappropriate.

Infrastructure Integrity

Cloudflare CDN/WAF protection is present, and all observed addresses were CDN edge infrastructure on AS13335; an origin server was not observable in this analysis. This may reduce direct origin exposure but does not validate the site or offset the security findings.

Closing Assessment

The appropriate enterprise response is to prevent interaction, block the domain, and initiate credential or endpoint review wherever prior access may have occurred.

Written analysis generated 2026-09-23 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

2 findings contributed to this verdict, raised by governance, registration and ownership, page content.

01 Governance Risk

- A form asking for sensitive information submits somewhere TrustSniffer could not verify, which caps how far the score can rise.
Governance rule:GOV_SENSITIVE_FORM_UNTRUSTED
- The public registration record for this domain is incomplete.
Registration and ownership rule:KF_WHOIS_INCOMPLETE

02 Sensitive Interaction Risk

- A form on the page submits to a destination TrustSniffer could not verify.
Page content rule:PAGE_FORM_UNTRUSTED_DEST
- The page asks visitors for sensitive information.
Page content rule:PAGE_FORM_SENSITIVE

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 korexnode.xyz.

- The request stayed on korexnode.xyz. It was not redirected to another domain. CLEAR
- Registration is published under NICENIC INTERNATIONAL GROUP CO., LIMITED. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-09-13. NOTED
- The earliest public archive of this site is from 2026-09-13. CLEAR
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	NICENIC INTERNATIONAL GROUP CO., LIMITED
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3037::6815:1a06
Name servers	BONNIE.NS.CLOUDFLARE.COM, MARTY.NS.CLOUDFLARE.COM
SSL issuer	YE2
SSL expiry	2026-12-12
Domain age	0.03 years (continuous registration)
Domain expiry	2027-09-13
Archive first seen	2026-09-13
Archive snapshots	Not counted (archive lookup incomplete)
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about korexnode.xyz 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.