

Is sandboxle.com.cn safe? TrustSniffer's low-trust assessment: 41/100

sandboxle.com.cn

Verdict

41

OUT OF 100

LOW TRUST

sandboxle.com.cn 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.

Safe for Read-Only

Governance Risk

Assessed 2026-09-19 by automated analysis. Classification confidence 55%.

What this site appears to be

Non-official Sandboxie information site in Chinese offering downloads, feature descriptions, installation and advanced usage tutorials, and FAQs. No forms requesting credentials or payments are present.

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.

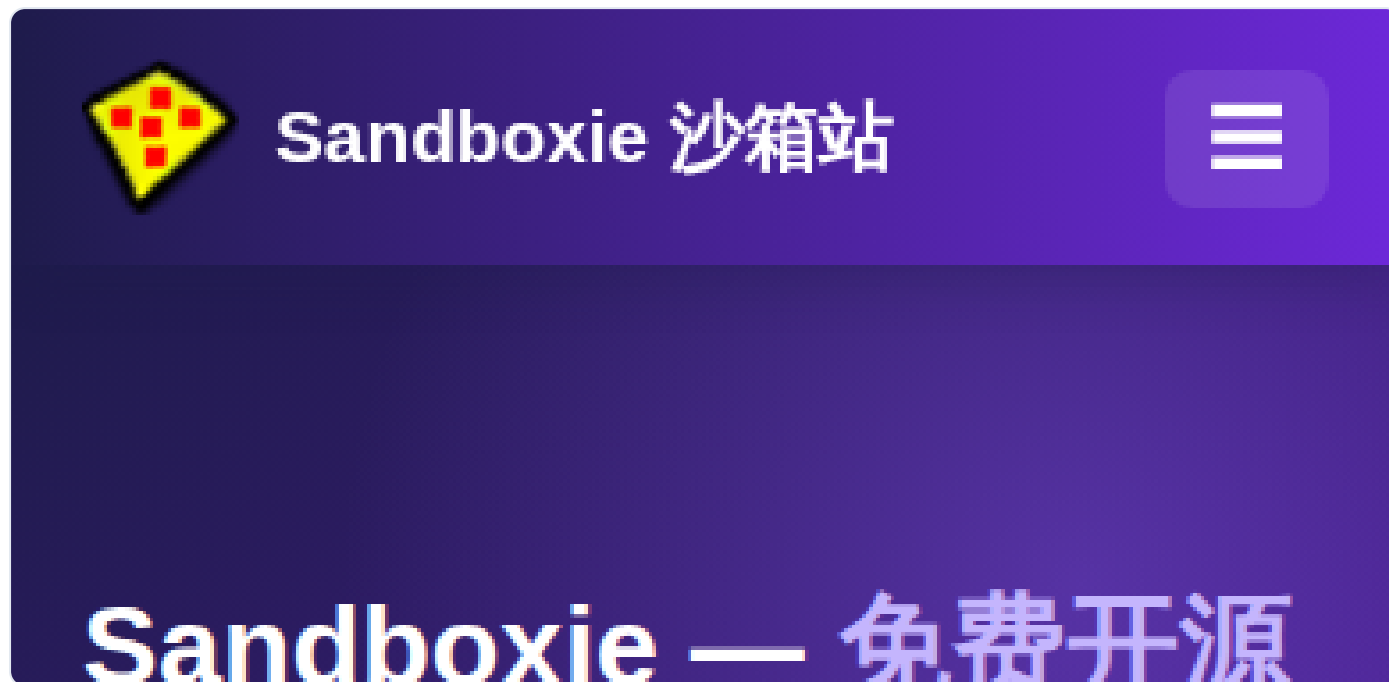
At a glance

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	29 days old Most scam domains are under a year old	RISK
Web archive	Never archived No public history of this site	WATCH
Certificate	Encrypted connection Issued by WE1	NOTED

The page as captured

<https://sandboxle.com.cn/>



What sandboxle.com.cn served when TrustSniffer captured it on 2026-09-19. The page may look different now.

Key findings

- Automated classification: Safe for Read-Only.
- Domain age: less than 1 year (registration continuity).
- No flags from the reputation services TrustSniffer consulted at assessment time.
- The operator behind the site could not be independently connected to a real-world brand or person.

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 non-official Chinese-language informational site about Sandboxie, presenting software downloads, installation guidance, troubleshooting, feature comparisons, advanced usage tutorials, and frequently asked questions; its apparent model is informational distribution rather than paid or financial activity.

Scam/Impersonation Risk

No confirmed blacklist, phishing, brand-impersonation, or conflicting-identity signal is present in the supplied evidence. The site explicitly describes itself as a non-official information site, which reduces the likelihood that it is presenting itself as the official Sandboxie operator, but the independently verified identity of the operator remains unresolved. The principal concern is external reputation: one suspicious detection was recorded and Fortinet identified a threat-related signal, despite the absence of malicious detections from another evaluated source. The site itself presents no login or payment forms, and observed behavior showed no credential harvesting, hidden forms, wallet activity, external posting, or suspicious script activity.

EVIDENCE

- The homepage contains no login or payment form and has no detected phishing or brand-impersonation indicator.
- External assessment recorded 0 malicious detections and 1 suspicious detection; Fortinet was the flagged security vendor.
- The registration record lists creation on 2026-08-21, with an age of 0.08 years, through Web Commerce Communications Limited.

Regulatory Verification Notes

The reviewed pages describe the site as non-official and identify it as an information resource rather than the Sandboxie publisher. The About and legal-content areas provide site-level descriptions and links to official resources, but do not establish an independently verified corporate operator, licensing relationship, or regulatory authorization. For this informational model, the absence of financial or regulated-service claims is relevant; nevertheless, the operator's identity and authority to distribute software remain verification matters. The low authority profile and limited independent identity evidence support a cautious posture rather than a conclusion of fraud.

EVIDENCE

- The About page states that the site is a non-official Sandboxie information site and provides an "Official Resources" area.
- The homepage presents downloads, tutorials, comparisons, and FAQs, with no visible paywall, investment solicitation, or regulated financial service.
- The site's transport encryption is a DV certificate issued by WE1, valid to 2026-11-19.

What to Verify Next

Before downloading or executing software, independently compare the offered version, publisher, file hash, and release information with the official Sandboxie website or official open-source repository. Confirm that any download is obtained from an authenticated publisher-controlled source and scan it with current endpoint security before execution. The site's stated non-official status should also be reconciled with the official project's own documentation before relying on its installation or troubleshooting instructions.

EVIDENCE

- The homepage offers a download centre and describes an approximately 8 MB Windows installation package.
- The About page separately identifies official-resource links, creating a practical basis for cross-checking the software source.
- The site provides installation, advanced-configuration, troubleshooting, and FAQ content that should be compared with current official documentation.

Summary Verdict

The overall posture is **low trust with read-only suitability**, not a confirmed scam or impersonation. The content is coherent and non-financial, but the combination of an unverified operator identity, very recent registration, and an external threat-related detection means legitimacy should be treated as apparent rather than established.

Infrastructure Integrity

The site is served through Cloudflare’s CDN/WAF infrastructure, with observed edge addresses only and no origin candidate identified. This provides a meaningful protective layer against direct exposure but is a mitigating technical control, not evidence that the site or its downloads are legitimate.

EVIDENCE

- Hosted on AS13335, CLOUDFLARENET—Cloudflare, Inc., US.
- Four observed addresses were CDN edge addresses: 104.21.39.2, 172.67.141.178, 2606:4700:3036::ac43:8db2, and 2606:4700:3037::6815:2702.
- TLS validation level is DV; the certificate issuer is WE1 and expiry is 2026-11-19T02:25:48+00:00.

Closing Assessment

Prospective users should limit activity to passive review until the software source, file integrity, and connection to the official Sandboxie project have been independently confirmed.

Written analysis generated 2026-09-19 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

1 finding contributed to this verdict, raised by registration and ownership.

01 Governance Risk

- The public registration record for this domain is incomplete.

Registration and ownership rule:KF_WHOIS_INCOMPLETE

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 sandboxle.com.cn.

- The request stayed on sandboxle.com.cn. It was not redirected to another domain.

CLEAR

- Registration is published under Web Commerce Communications Limited. CLEAR
- DNS for this domain is served by cloudflare.com, across 2 name servers. NOTED
- The registration is paid up to 2027-08-21. NOTED
- It is hosted on CLOUDFLARENET, from a server in US. NOTED

Domain intelligence

Registrar	Web Commerce Communications Limited
Hosting	CLOUDFLARENET - Cloudflare, Inc., US
Country	US
Server IP	2606:4700:3036::ac43:8db2
Name servers	nero.ns.cloudflare.com, leia.ns.cloudflare.com
SSL issuer	WE1
SSL expiry	2026-11-19
Domain age	0.08 years (continuous registration)
Domain expiry	2027-08-21
Archive first seen	Not available
Archive snapshots	0
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 sandboxle.com.cn 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/sandboxle.com.cn> · assessed 2026-09-19