

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

funrat.co

## Verdict

0

OUT OF 100

CRITICAL RISK

funrat.co 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

Marketing page for 'FunRAT' offering a Remote Access Trojan and related illicit tools that harvest credentials, session tokens, and provide remote control capabilities; clearly malicious.

## 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.

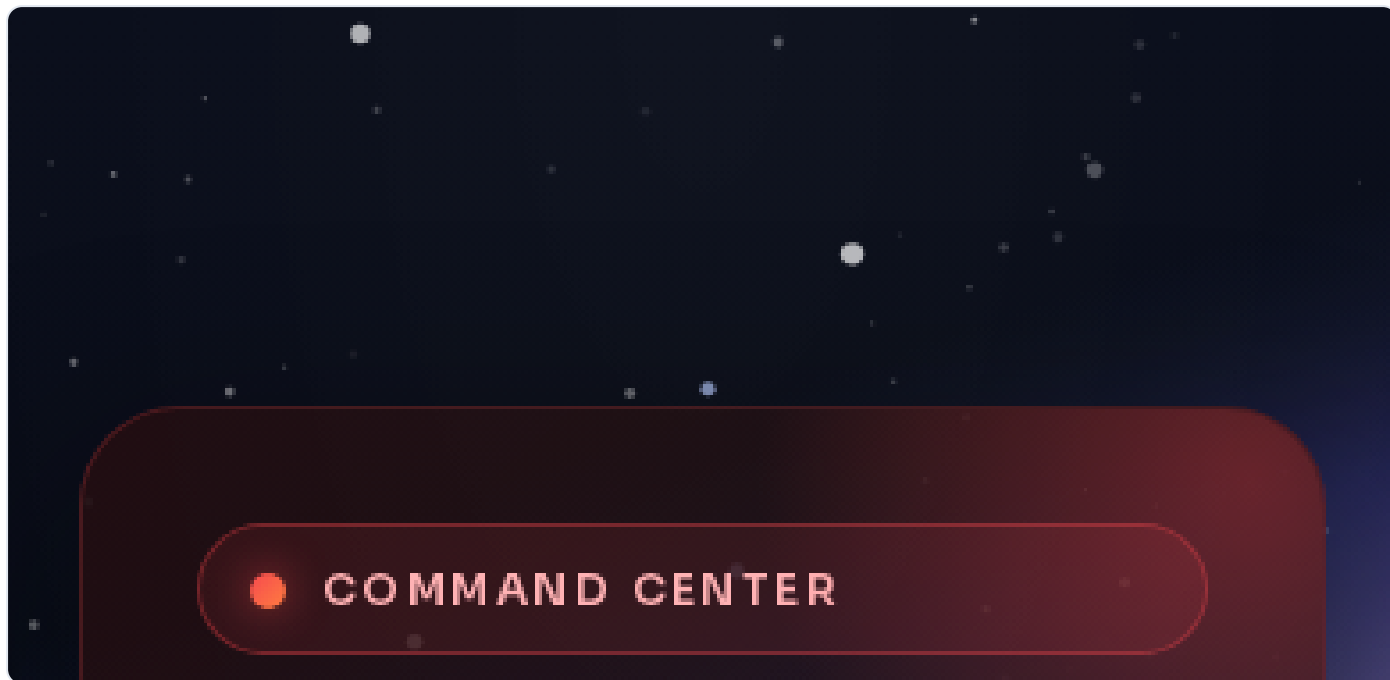
## At a glance

The checks that decide most of this verdict.

|                           |                                                                               |       |
|---------------------------|-------------------------------------------------------------------------------|-------|
| Malware engines           | <div>15 flagged it</div> <div>VirusTotal</div>                                | RISK  |
| Google Safe Browsing      | <div>Not listed</div> <div>Google</div>                                       | CLEAR |
| Abuse reports on the host | <div>0 reports</div> <div>AbuseIPDB; shared hosting inflates this count</div> | NOTED |
| Domain age                | <div>3 months old</div> <div>Most scam domains are under a year old</div>     | RISK  |
| Web archive               | <div>Never archived</div> <div>No public history of this site</div>           | WATCH |
| Certificate               | <div>Encrypted connection</div> <div>Issued by YE2</div>                      | NOTED |

## The page as captured

<https://funrat.co/>



What funrat.co 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).
- At least one reputation service TrustSniffer consulted had flagged this domain 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, Sophos flagged this site in external intelligence checks, indicating elevated compromise/scam exposure that requires immediate caution.

The website presents “FunRAT” as an “industry-leading” Minecraft Remote Access Trojan marketplace, offering remote-control capabilities, credential and session-token collection, surveillance functions, and related illicit tools and services for direct sale.

### Scam/Impersonation Risk

The site presents a direct malware-distribution model rather than a legitimate software or service offering. Its homepage advertises collection of Minecraft session tokens, IP addresses and geolocation, screenshots, Discord and Telegram credentials, webcam and screen access, file-system control, and remote mouse and keyboard operation. It also promotes token-upgrader services, mass-DM and spam tools, and the sale of in-game items. These claims are consistent with a malicious remote-access and credential-harvesting operation, and the site’s browser behavior was associated with suspicious downloads, potential malware hosting, and described data-exfiltration capabilities. External reputation evidence includes a confirmed **blacklist** status and malicious detections, creating a direct contradiction to any implication that the site is a trustworthy software

provider. No separate legal-entity identity contradiction or brand-impersonation finding was recorded, but the malware purpose and confirmed blacklist status independently support a critical risk conclusion.

#### EVIDENCE

- The homepage describes “Full Remote Control,” collection of Minecraft session tokens, Discord and Telegram credentials, screenshots, webcam streams, and file-system access.
- The homepage offers a “Live Token Upgrader/Refresher,” Discord mass-DM/spam tools, and sales of Hypixel and DonutSMP items.
- External reputation checks recorded 15 malicious detections and 4 suspicious detections, with a confirmed blacklist result.
- Registration evidence records the domain as created on 2026-06-16 and approximately 0.27 years old.

#### Regulatory Verification Notes

The site does not present a license, registration number, or clearly attributable operating entity for a business selling malware and related services. Its real-world operator identity remains unverified, and the available page content does not provide a credible compliance or governance basis for engagement. A valid transport certificate and a named registrar establish technical administration only; they do not validate the business, its operators, or its activities. No matching broker-reputation profile was identified, but that absence does not offset the site's direct malware-related content or external threat findings.

#### EVIDENCE

- The homepage contains no stated licensing authority, license number, or identifiable legal operator in the supplied content.
- The domain is registered through NICENIC INTERNATIONAL GROUP CO., LIMITED.
- The site uses a DV TLS certificate issued by YE2, valid to 2026-11-30.
- The homepage has no structured legal or corporate identity information sufficient to independently connect it to a verified real-world entity.

#### What to Verify Next

The appropriate response is to avoid interacting with the site from production systems and to prevent downloads, authentication, or transactions associated with it. Security teams should block the domain and investigate any endpoint that accessed it, particularly for unauthorized files, credential exposure, or unusual outbound activity. If prior interaction occurred, credentials that may have been entered or exposed should be rotated through trusted channels and affected systems should be examined by incident-response personnel.

#### EVIDENCE

- The homepage explicitly describes credential collection and remote-control functionality, supporting endpoint-protection and incident-response treatment.
- Browser analysis recorded suspicious inline scripts and suspicious download or malware-hosting behavior.
- The site's identity and operating authority cannot be independently established from its published content.

### Summary Verdict

The website has a critical trust posture and should be treated as a malicious or untrusted service rather than a legitimate software provider. The combination of explicit credential-theft and remote-control functionality, confirmed external blacklist status, and unverified operator identity makes sensitive interaction inappropriate.

### Infrastructure Integrity

The site resolves directly to hosting infrastructure operated by VDSINA - SERVERS TECH FZCO, with no detected CDN or WAF layer and a likely origin exposure. This infrastructure fact is not proof of maliciousness, but it provides no meaningful protective or legitimacy signal capable of offsetting the site's content and reputation evidence.

#### EVIDENCE

- Hosted on AS216071, VDSINA - SERVERS TECH FZCO, AE.
- Infrastructure analysis identified one resolved IP, no CDN, no detected vendors, and one likely origin IP.

### Closing Assessment

Organizations should block access, preserve relevant telemetry, and treat any prior interaction as a potential security incident requiring proportionate endpoint and credential review.

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 registration and ownership, analysis engine, behaviour in a sandbox, 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
- The page carried inline scripts written in a style TrustSniffer treats as suspicious.  
Behaviour in a sandbox rule:BEHAV\_SUSPICIOUS\_INLINE\_SCRIPTS
- Most of what the page loaded came from other domains rather than from this one.  
Behaviour in a sandbox rule:BEHAV\_EXTERNAL\_RATIO\_HIGH
- 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 funrat.co.

- The request stayed on funrat.co. 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 desec.io, across 2 name servers. NOTED
- The registration is paid up to 2027-06-16. NOTED
- It is hosted on VDSINA, from a server in AE. NOTED

Domain intelligence

|              |                                          |
|--------------|------------------------------------------|
| Registrar    | NICENIC INTERNATIONAL GROUP CO., LIMITED |
| Hosting      | VDSINA - SERVERS TECH FZCO, AE           |
| Country      | AE                                       |
| Server IP    | 144.124.237.234                          |
| Name servers | NS1.DESEC.IO, NS2.DESEC.ORG              |
| SSL issuer   | YE2                                      |
| SSL expiry   | 2026-11-30                               |
| Domain age   | 0.27 years (continuous registration)     |

|                    |                                                                                 |
|--------------------|---------------------------------------------------------------------------------|
| Domain expiry      | 2027-06-16                                                                      |
| Archive first seen | Not available                                                                   |
| Archive snapshots  | 0                                                                               |
| Reputation         | VirusTotal: 15 flagged   AbuseIPDB: 0 reports   Google Safe Browsing: 0 matches |

---

## About this assessment

A trust score summarises the evidence TrustSniffer could collect about funrat.co 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/funrat.co> · assessed 2026-09-23