

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

massgravel.net

Verdict

0

OUT OF 100

CRITICAL RISK

massgravel.net 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 2026-09-18 by automated analysis. Classification confidence 55%.

What this site appears to be

Site documents and distributes MAS (Microsoft Activation Scripts) — open-source activator scripts and instructions that instruct users to download and execute remote scripts to activate Windows/Office. Content includes direct PowerShell commands that fetch and execute remote code and downloadable executables; poses significant security and legal risk despite being presented as a utility.

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.

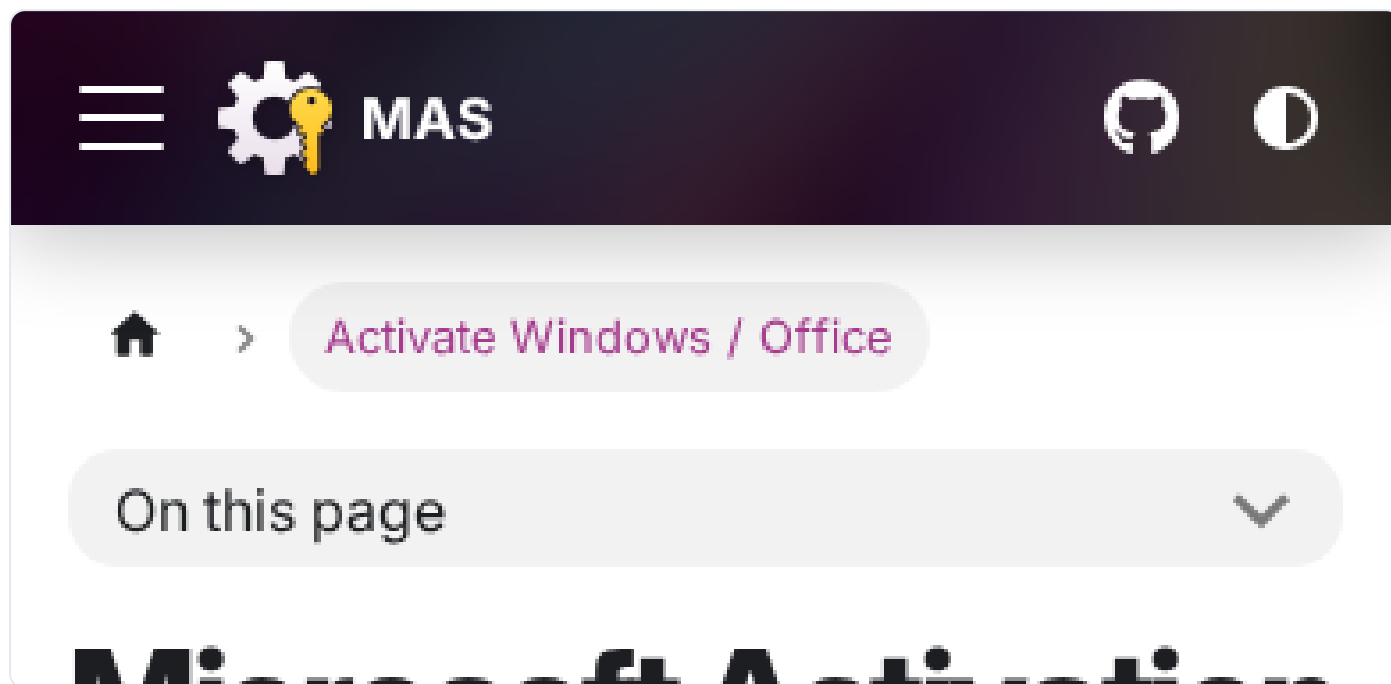
At a glance

The checks that decide most of this verdict.

Malware engines	6 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	18 days old Most scam domains are under a year old	RISK
Web archive	Never archived No public history of this site	WATCH

The page as captured

https://massgravel.net/



What massgravel.net served when TrustSniffer captured it on 2026-09-18. 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.

This website presents itself as a utility and software-distribution site for Microsoft Windows and Office activation, offering documentation, downloads, troubleshooting guidance, and links to source repositories for activation scripts and related tools.

Scam/Impersonation Risk

The site presents a material security and trust contradiction. Its homepage instructs visitors to use PowerShell to retrieve and execute remote code, offers downloadable activation scripts and executables, and describes methods including HWID, Ohook, TSforge, and Online KMS. It also provides bypass guidance involving alternate DNS resolution and VPN use. These mechanics create substantial exposure to untrusted code execution and potential malware distribution, while the legal status and provenance of the software are not

established by the site. Independent security intelligence records multiple malicious and suspicious detections, including a confirmed blacklist, which is the decisive external contradiction. No separate two-name legal-identity conflict or explicit brand-impersonation finding was identified, but the blacklist and malicious detections independently support a clearly cautionary posture.

EVIDENCE

- The homepage documents remote PowerShell retrieval and execution and presents activation methods under the “Microsoft Activation Scripts” service.
- The homepage offers downloadable script and executable packages and includes browser-behavior indicators for remote-script execution and potential malware distribution.
- External security assessment recorded 6 malicious and 3 suspicious detections, with blacklist status confirmed by two sources.
- Domain registration telemetry records 2026-08-30 as the creation date, approximately 0.05 years of age, with NICENIC INTERNATIONAL GROUP CO., LIMITED as registrar.

Regulatory Verification Notes

The available pages do not establish a clearly accountable legal operator, licensing authority, or license number for the software-distribution activity. The site's stated purpose involves activation of Microsoft products, but the pages do not provide a substantiated authorization or licensing basis for that activity. This is a significant verification gap rather than, by itself, a separate impersonation finding; in the present case it compounds the security concerns already identified. The operator identity remains unverified, and ordinary transport security does not resolve that issue. A valid domain-validated certificate is a technical protection, not evidence of authorization or legitimacy.

EVIDENCE

- The homepage and navigation identify the service as an activator and provide download, documentation, contact, and source-code links without a stated license authority or license number.
- The domain is registered through NICENIC INTERNATIONAL GROUP CO., LIMITED; registration telemetry records an expiry date of 2027-08-30.
- The site is hosted on AS61112 through AkileCloud - AKILE LTD, GB.
- TLS is domain-validated, issued by YE1, and valid through 2026-11-28.

What to Verify Next

Before any operational interaction, an organization should independently confirm whether the publisher has authorization to distribute or facilitate activation of the relevant software, using official vendor or registry channels rather than contact details supplied solely by the site. Any downloaded material should be treated as untrusted, inspected in a controlled isolated environment, and checked against independently obtained source provenance before execution. Security teams should also review endpoint, proxy, and identity telemetry for any system that has already run the supplied commands.

EVIDENCE

- The homepage provides direct instructions for fetching and executing code rather than limiting distribution to static documentation.
- The site includes Contact Us, GitHub, and other external-source references, creating a need to validate that each referenced channel is genuinely controlled by the same operator.
- Behavioral testing recorded no sensitive login form or hidden credential form, but did identify remote-script execution and executable-download indicators.

Summary Verdict

The overall posture is critical and the site is not suitable for sensitive interaction or execution of supplied content. Available evidence does not independently verify the operator, and the combination of external malicious detections, blacklist status, and unsafe distribution mechanics outweighs the site's functional content and valid transport encryption.

Infrastructure Integrity

The observed configuration lacks a detected CDN or WAF layer and resolves directly to a likely origin host, so no meaningful edge-layer mitigation was observed. This infrastructure posture does not establish maliciousness on its own, but it provides limited protective separation between the public service and its hosting environment.

EVIDENCE

- Infrastructure resolution identified one unique IP, with zero edge IPs and one likely origin IP.
- No CDN or WAF vendor was detected in the observed hosting configuration.
- The hosting environment is registered in the RIPE NCC registry and located in GB.

Closing Assessment

Prospective users should keep interaction to passive review, avoid executing supplied content or providing credentials, and require independent authorization and malware-safety validation before any further engagement.

Written analysis generated 2026-09-18 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 massgravel.net.

- The request stayed on massgravel.net. 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 my-ndns.com, across 2 name servers. NOTED
- The registration is paid up to 2027-08-30. NOTED
- It is hosted on AkileCloud, from a server in GB. NOTED

Domain intelligence

Registrar	NICENIC INTERNATIONAL GROUP CO., LIMITED
Hosting	AkileCloud - AKILE LTD, GB
Country	GB
Server IP	82.153.135.80
Name servers	NS3.MY-NDNS.COM, NS4.MY-NDNS.COM
SSL issuer	YE1
SSL expiry	2026-11-28
Domain age	0.05 years (continuous registration)
Domain expiry	2027-08-30
Archive first seen	Not available
Archive snapshots	0

About this assessment

A trust score summarises the evidence TrustSniffer could collect about massgravel.net 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/massgravel.net> · assessed 2026-09-18