Nemucod (JS.Nemucod) - What it is, how it spreads, and how to remove it safely

Gridinsoft Help Center

What it is

Nemucod is a trojan downloader/dropper that arrives as JavaScript or PHP and then pulls in ransomware or other malware. It’s commonly spread by email attachments and malicious links. Technical details and IOCs are in our Nemucod overview for defenders.

How it spreads - quick tour

- Phishing emails with .js, .zip, or fake invoice attachments
- Links to pages that serve malicious JS/PHP
- Compromised sites that auto-download the script

What you may notice

- Windows prompts to run "script host" or open a .js file
- Sudden browser redirects or silent downloads
- A second-stage payload appears - often ransomware or a stealer

Remove it now

- Disconnect from the internet to stop the next-stage download.
- Run a full anti-malware scan, reboot, then scan again.
- Delete suspicious .js/.vbs/.ps1 files and unknown scheduled tasks.
- Reset browsers and remove unknown extensions and proxy settings.
- From a clean device, change passwords and enable MFA.

Prevent it

- Do not open script attachments - verify invoices out of band.
- Keep Windows, browsers, and Office updated; block macros by default.
- Use email and web filtering plus DNS filtering for known-bad hosts.
- Show file extensions in Explorer so scripts are not disguised.
- Limit script engines - prefer signed PowerShell and disable WSH if not needed.