N

Nemucod Downloader: Detection, Removal, and Cache Alerts

Nemucod is a JavaScript Trojan downloader historically delivered by malicious email attachments. Learn how to interpret paths, handle cache detections, and check for downloaded payloads.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 What TrojanDownloader:JS/Nemucod means

02 How Nemucod infections work

03 What to do after a Nemucod alert

04 How to handle a browser or WebView cache detection

05 What if Defender says remediation incomplete?

06 Enterprise investigation checklist

07 How to prevent script downloaders

08 Frequently asked questions

09 References

Nemucod is a detection family associated with malicious JavaScript downloaders. Classic campaigns delivered scripts in ZIP email attachments; if executed, the script contacted remote infrastructure and downloaded additional malware such as information stealers or ransomware. The downloaded payload, not the script alone, may cause the main damage.

A modern Nemucod alert can also point to a browser or application WebView cache. Path and execution evidence matter: cached content that security software blocked is different from a script launched from an attachment, Downloads, Temp, or a startup location. Do not restore the file in either case.

01 What TrojanDownloader:JS/Nemucod means

TrojanDownloader describes its role: obtain another malicious file. JS identifies JavaScript. Nemucod is a family or generic label, and exact names vary by vendor. A detection does not automatically prove that a secondary payload executed, but it requires checking the process chain and other alerts.

Detection location	Likely context	What to do
Email attachment, Downloads, or extracted ZIP	Direct delivery of a script	Quarantine; determine whether it was opened or executed
Temp, AppData, Startup, or scheduled-task path	Execution or persistence is more plausible	Isolate the device and investigate as a compromise
Browser cache	A page or download may have been cached, possibly without execution	Keep quarantined, update and rescan, review browsing and download history
Discord, Teams, Roblox, or another WebView2 cache	Embedded web content or an application cache may be involved	Update the app and WebView runtime; verify no child process executed

Detection location	Likely context	What to do
The same file returns after cleanup	A page, sync source, app, task, or other process is recreating it	Identify and remove the source rather than repeatedly deleting the cache file

02 How Nemucod infections work

1. A phishing message or malicious site delivers an archive, script, or disguised file.
2. The user opens the extracted JavaScript, or another process launches it.
3. The script uses Windows scripting components or another trusted process to contact attacker infrastructure.
4. It downloads and executes a secondary payload.
5. The payload steals data, encrypts files, establishes persistence, or performs another objective.

Campaign details and downloaded families change. Historical Nemucod activity delivered threats including Locky and TeslaCrypt ransomware, but do not assume every alert is the same campaign.

03 What to do after a Nemucod alert

1. **Leave the item quarantined.** Record the detection name, full path, hash, time, and associated application.
2. **Determine whether the script executed.** Review endpoint telemetry for script hosts, command shells, downloads, and child processes near the alert time.
3. **Contain when execution is possible.** Disconnect or use endpoint isolation if the file was opened, a process launched, or a secondary payload appeared.
4. **Update and scan.** Install current security intelligence and run a full scan. Use an offline scan for repeated detections, security interference, or persistent malware.

5. **Find the downloaded payload.** Review other detections, recent files, startup entries, tasks, services, and network connections.
6. **Protect affected data and accounts.** If an infostealer or RAT ran, revoke sessions and rotate credentials from a clean device. If ransomware ran, isolate shared storage and follow the incident plan.

04 How to handle a browser or WebView cache detection

A cache path can mean that an application stored web content that the scanner later recognized. It may be a blocked artifact rather than an executed program, but the cache label alone cannot prove that nothing ran.

- Update Windows, the detecting product, the browser or affected app, and Microsoft Edge WebView2.
- Close the affected application, keep the item quarantined, then rescan.
- Review downloads and the process tree for script-host or executable launches from the same time.
- Clear the specific application's cache only after recording the path and preserving evidence required by your organization.
- If the alert returns, identify which page, server, advertisement, extension, or app content recreates it.

Do not exclude a cache directory. Broad exclusions create a durable place in which future threats can hide.

05 What if Defender says remediation incomplete?

An incomplete action can occur when the file changed, was locked, disappeared with the cache, or is being recreated. Update protection, restart if prompted, run a full scan, and then use Microsoft Defender Offline when the alert persists or execution is suspected. Confirm the

protection history shows a completed action and no related threats remain.

06 Enterprise investigation checklist

- Search email for matching senders, subjects, attachment names, hashes, and URLs.
- Identify all recipients and whether the content was opened or executed.
- Hunt for scripting engines, suspicious child processes, outbound connections, and follow-on payloads.
- Review web proxy and endpoint data to distinguish cached content from execution.
- Block confirmed malicious infrastructure and remove the original message or web source.
- Reimage devices when a damaging payload executed or system trust cannot be established.

07 How to prevent script downloaders

- Filter script attachments and inspect archives before mail delivery.
- Show file extensions and do not open unexpected invoice or shipping attachments.
- Restrict Windows script hosts and execution from user-writable paths where business needs permit.
- Patch browsers, WebView runtimes, email clients, and operating systems.
- Use least privilege and application control for managed endpoints.

08 Frequently asked questions

Is Nemucod ransomware?

Nemucod is primarily a downloader. It has historically delivered ransomware, but it can deliver other payloads too.

Does a cache detection mean my account was hacked?

Not by itself. Establish whether content executed and whether the related app or account shows suspicious activity. Keep the artifact quarantined and investigate the time and process context.

Can I restore a detected JavaScript file?

No, unless a qualified analysis has conclusively identified a false positive and there is a legitimate reason to keep that exact script. Ordinary users should leave it quarantined or delete it.

09 References

- F-Secure: Trojan-Downloader:JS/Nemucod
- Gridinsoft research: Nemucod detections in current application caches

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com