S

Spigot Adware: Symptoms, Removal, and SpigotMC Confusion

Identify Spigot adware and browser extensions, remove associated apps and settings safely, and distinguish the detection from the unrelated SpigotMC server project.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is the Spigot browser extension?
02 Spigot adware versus SpigotMC
03 Common symptoms
04 How it is installed
05 Remove Spigot adware from Windows
06 Remove it from macOS
07 Is SpigotMC safe?
08 Prevent another bundled installation

Spigot adware is a family of potentially unwanted browser components and applications commonly installed through software bundles or misleading download offers. It can replace the homepage or search engine, add extensions, redirect searches, display advertising, and collect browsing-related information. It is unrelated to **SpigotMC**, the open-source Minecraft server project.

01 What is the Spigot browser extension?

“Spigot browser extension” does not identify one current add-on with a single fixed filename. Security vendors use names such as **PUP.Optional.Spigot** for a broader family of search extensions and browser hijackers that may be promoted as converters, shopping helpers, or specialized search tools. Identify the actual extension by its name, ID, permissions, installation source, and browser policy rather than searching for one universal Spigot file.

02 Spigot adware versus SpigotMC

The word “Spigot” can refer to two very different things:

- **Adware.Spigot or PUP.Optional.Spigot** is a security-product detection associated with browser hijackers, bundled applications, extensions, and advertising components.
- **SpigotMC** is server software used to run Minecraft plugins. Its name alone does not indicate adware.

Always examine the detected file path, signer, download source, and associated application. A detection inside an unfamiliar browser extension or bundled installer is different from a server file deliberately downloaded from the official SpigotMC project. Do not create a broad antivirus exclusion based only on the word “Spigot.”

03 Common symptoms

- The browser homepage, new-tab page, or default search engine changes unexpectedly.

- Searches pass through an unfamiliar domain before results appear.
- An extension, toolbar, search helper, or shopping component appears without a clear installation choice.
- Pages contain additional advertisements, sponsored links, or pop-ups.
- The unwanted browser setting returns after you change it.
- A security scan reports Adware.Spigot, PUP.Optional.Spigot, or a related bundled component.

04 How it is installed

Spigot-associated components have historically been distributed with free application installers, download portals, browser add-ons, and preselected “recommended” offers. The user may technically approve the bundle while moving quickly through setup, but the effect is still unwanted when the offer is unclear or difficult to decline.

Removing only the visible extension may not be enough. A companion application, login item, scheduled task, browser policy, profile, notification permission, or synchronization setting can restore the change.

05 Remove Spigot adware from Windows

1. Open **Settings → Apps → Installed apps** and sort by installation date.
2. Remove unfamiliar search assistants, download managers, converters, toolbars, or other software installed when the problem began.
3. Inspect extensions in every installed browser and remove components you did not intentionally install.
4. Restore the expected homepage, new-tab page, and search engine. If changes return, reset the affected browser.
5. Remove unfamiliar sites from the browser’s allowed notification list.
6. Run a full security scan and quarantine related adware, bundlers, and persistence items.

7. Restart Windows and confirm the settings remain correct.

06 Remove it from macOS

1. Quit affected browsers and remove unfamiliar applications from the Applications folder.
2. Review browser extensions and search settings.
3. Open **System Settings → General → Login Items & Extensions** and investigate unknown background items.
4. Check **System Settings → Privacy & Security → Profiles** if that section is present. Do not remove an employer or school profile without authorization.
5. Run a reputable macOS security scan, restart, and test the browser again.

07 Is SpigotMC safe?

Confirm that the file came from the official SpigotMC resource and compare its checksum or signature information when the publisher provides one. Plugins are third-party code and should be evaluated separately from the server platform. Remove an unknown plugin from production until its origin and behavior are verified.

If a trusted file appears to be misclassified, submit the exact file and detection details to the relevant security vendor for review. Do not upload private server configurations, credentials, player data, or license keys.

08 Prevent another bundled installation

- Download software from the original publisher rather than a repackaging portal.
- Use Custom or Advanced setup when available and decline unrelated offers.
- Review requested browser permissions before adding an extension.
- Avoid cracked installers and unofficial plugin bundles.
- Keep browsers and the operating system updated.

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