FAQ

I have a virus but Trojan Killer doesn’t detect it.

Update Trojan Killer, run the appropriate scan, verify whether the symptom is malware, and send a focused diagnostic report or sample to Support safely.

PUBLISHER
Gridinsoft Support

UPDATED
Jul 10, 2026

READ TIME
1 min

CONTENTS

In this guide

01 Run a current, complete check

02 Check the symptom

03 Send a useful report

A pop-up, redirect, unfamiliar process, or slow computer does not always prove that malware is present. Start by updating Trojan Killer and collecting enough evidence to distinguish malware from a browser setting, damaged application, or Windows problem.

01 Run a current, complete check

1. Connect to the internet and update the threat database.
2. Restart Windows if the suspicious process is still active.
3. Run a **Full** scan. Use a custom scan as well when you know the affected folder, archive, or removable drive.
4. Record the time of the symptom and the exact file path, URL, process name, or warning shown.

02 Check the symptom

- For browser redirects, inspect extensions, search settings, proxy settings, and notification permissions.
- For an unfamiliar process, verify its digital signature and installation folder before deciding it is malicious.
- For a suspicious file, do not open it again and do not upload confidential documents to public scanners.

03 Send a useful report

Export the scan result with **Save to file** and open a Support request. Include the symptom, time, relevant path or URL, and the exported report. If Support requests a sample, use the secure upload method they provide; do not email an active malware sample or send passwords and personal documents.

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