T

Trojan Malware: Types, Warning Signs, Removal, and Prevention

Learn why a Trojan does not self-replicate like a virus, how loaders, stealers, backdoors, and banking Trojans work, and how to respond safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What is a Trojan virus?
02 Common types of Trojans
03 How Trojans reach devices
04 Warning signs
05 Trojan vs. virus vs. worm
06 What to do after suspected infection
07 Removal and recovery
08 Why deleting the original installer is insufficient
09 Prevention

A **Trojan** is malware that appears useful, harmless, or expected so a user or system will run it. Unlike a virus or worm, a Trojan does not self-replicate by definition. It may arrive through phishing, fake software, cracks, malicious ads, or another malware loader.

“Trojan virus” is a common phrase, but technically a Trojan and a computer virus use different propagation methods.

01 What is a Trojan virus?

“Trojan virus” normally means Trojan malware: malicious code delivered under a believable name or purpose. The deception may be a document, installer, update, browser extension, mobile app, or remote-support tool. Once run, the Trojan can steal information, open remote access, or install other payloads; it does not need to attach itself to other files.

02 Common types of Trojans

- **Downloader:** retrieves additional malware.
- **Dropper:** contains and installs another payload.
- **Backdoor or remote-access Trojan:** provides unauthorized control.
- **Banking Trojan:** targets financial credentials and transactions.
- **Information stealer:** collects passwords, cookies, wallets, and documents.
- **Proxy Trojan:** routes attacker traffic through the victim.
- **Fake security tool:** displays deceptive warnings and demands payment.

03 How Trojans reach devices

Attackers use email attachments, fake updates, search ads, unofficial installers, peer-to-peer downloads, poisoned repositories, and social-engineering messages. A Trojan may also be installed after exploitation or by another compromised account, so user deception is common but not required in every case.

04 Warning signs

Possible signs include unexpected child processes, new startup entries, disabled security tools, unfamiliar browser sessions, unusual outbound traffic, credential alerts, remote-control behavior, or a program requesting permissions unrelated to its purpose. Sophisticated Trojans may remain quiet.

05 Trojan vs. virus vs. worm

A virus inserts itself into other files or system areas and spreads when infected content runs. A worm spreads automatically between systems. A Trojan relies on disguise or another delivery mechanism and does not replicate itself. One malware campaign can use components from several categories.

06 What to do after suspected infection

1. Disconnect the device when credential theft or remote control is possible.
2. Preserve alerts, files, URLs, messages, process details, and timestamps.
3. Use a known-clean device to secure primary email and sensitive accounts.
4. Revoke sessions and tokens, change exposed passwords, and enable MFA.
5. Run approved full or offline security scans.
6. Search for persistence and additional payloads.

07 Removal and recovery

Quarantine detected files, remove scheduled tasks, services, extensions, accounts, and unauthorized remote tools, then patch the initial access path. If the Trojan ran with high privileges or system integrity cannot be established, rebuild from known-good installation media. Restore only verified data.

08 Why deleting the original installer is insufficient

A dropper or downloader may have placed payloads elsewhere, stolen browser sessions, or created cloud persistence. Review identity, email forwarding, OAuth grants, API keys, and network activity. Determine what the Trojan could access before declaring the incident closed.

09 Prevention

Use official download sources, keep systems updated, block risky attachments, use least privilege, and maintain endpoint and web protection. Avoid cracks and unsolicited support tools. Verify unusual requests through a separate channel and keep tested backups that malware cannot modify.

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