M

Malware: Types, Warning Signs, Removal, and Recovery

Malware is malicious code that steals data, disrupts systems, or gives attackers control. Learn the main types, stronger and weaker warning signs, safe removal, account recovery, and prevention.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
7 min

CONTENTS

In this guide

01 What is malware?

02 Malware types and what they mean

03 How malware reaches a device

04 What happens during a malware infection?

05 Signs of a possible malware infection

06 How to remove malware safely

07 When a factory reset or reinstall is appropriate

08 How to prevent malware

09 Frequently asked questions

10 References

01 What is malware?

Malware is software or code designed to act against the interests of a device, data, network, or user. It may steal information, spy on activity, encrypt or destroy files, display unwanted content, use computing resources, or give an attacker remote control. The word is short for **malicious software**.

Some related labels describe a different dimension of an incident: crimeware emphasizes criminal use, while a blended threat combines several delivery or attack techniques. These descriptions can overlap with the malware types below rather than replace them.

Malware is an umbrella term, not one specific threat. A single infection can be described in several ways: a trojan explains how it was disguised, an information stealer explains what it collects, and a botnet agent explains how an operator controls it.

02 Malware types and what they mean

Type	Defining behavior	Typical impact
Virus	Attaches to a file or program and spreads when the infected host is run	Changes files and may carry another malicious payload
Worm	Self-replicates and spreads between systems, often through a vulnerability or network service	Rapid propagation, disruption, and delivery of other malware
Trojan	Pretends to be legitimate or useful so a person installs or runs it	Data theft, remote access, or installation of a second stage
Ransomware	Denies access to data or systems, commonly through encryption	Extortion, downtime, data loss, and possible data exposure
Spyware or infostealer	Collects credentials, session tokens, documents, browsing data, screenshots, or other information	Account takeover, fraud, and privacy loss

Type	Defining behavior	Typical impact
Keylogger	Records keyboard input and sometimes forms, clipboard, or screen activity	Stolen passwords, messages, and financial details
Remote access trojan or backdoor	Lets an unauthorized operator control the device or run commands	Persistent access, surveillance, lateral movement, and additional payloads
Rootkit or bootkit	Hides or persists deep in the operating system, boot process, or firmware	Stealthy control and reduced trust in local security checks
Botnet agent	Enrolls the device in a remotely controlled group	DDoS, spam, proxying, credential attacks, or malware distribution
Cryptominer	Uses CPU, GPU, or cloud resources to mine cryptocurrency without approval	High resource use, cost, heat, and reduced performance
Wiper	Deletes, overwrites, or corrupts data and system components	Destructive loss and operational disruption
Potentially unwanted application	Shows undesirable behavior but may not meet the malware definition	Bundling, aggressive ads, tracking, or unwanted configuration changes

"Fileless" describes a technique rather than a single purpose: malicious code may run in memory or abuse trusted system tools with limited files on disk. Likewise, a loader or dropper exists mainly to install another payload.

03 How malware reaches a device

- Phishing or malspam links, attachments, QR codes, and fake shared documents.
- Cracked software, fake updates, malicious ads, and trojanized installers.
- Unpatched internet-facing services, browsers, plugins, or applications.
- Compromised websites, browser extensions, software updates, or suppliers.

- Stolen credentials used to log in and deploy tools remotely.
- Exposed remote access, weak cloud permissions, or abused management software.
- Removable media and unauthorized physical access.
- Malicious mobile apps or abuse of accessibility, device-admin, and sideloading permissions.

04 What happens during a malware infection?

1. **Delivery or access:** a file arrives, a vulnerability is exploited, or an attacker signs in.
2. **Execution:** code runs through an application, script, service, scheduled task, macro, or trusted system tool.
3. **Persistence and evasion:** the malware tries to survive restarts, hide, disable defenses, or blend with normal activity.
4. **Command and control:** some malware contacts external infrastructure for instructions or additional tools.
5. **Actions on objectives:** it steals data, encrypts files, spreads, monitors the user, disrupts services, or consumes resources.

Not every sample performs every stage, and multiple tools may divide the work. Removing the initially detected file does not prove that persistence, stolen credentials, or later payloads are gone.

05 Signs of a possible malware infection

Stronger signs

- A trusted security product reports malicious behavior or a confirmed threat.
- Files are unexpectedly encrypted, renamed, deleted, or accompanied by a ransom note.
- Security tools, updates, backups, or logging are disabled without authorization.
- An unknown process creates persistence, launches scripts, injects into another process, or contacts a suspicious destination.

- New administrators, remote-access tools, browser extensions, device profiles, or accessibility permissions appear.
- Accounts show stolen-session activity soon after the device was used.

Possible but weak signs

- Slow performance, crashes, overheating, high battery use, or low storage.
- Unexpected ads, browser redirects, homepage changes, or notifications.
- Unexplained network traffic, fan activity, or CPU/GPU use while idle.
- Apps open or close unexpectedly, or settings change.

Weak signs also have ordinary causes such as failing hardware, legitimate updates, browser settings, or resource-heavy applications. Investigate several signals together instead of assuming one symptom proves malware.

06 How to remove malware safely

1. **Stop sensitive activity.** Do not type new passwords, make payments, or access important accounts on the suspected device.
2. **Isolate the device.** Disconnect it from networks if active theft, remote control, encryption, or spread is likely. In a business, use the approved isolation process and notify security before destroying evidence.
3. **Preserve useful details.** Record alerts, filenames, timestamps, symptoms, messages, and recent downloads. Responders may need logs or a forensic image.
4. **Scan with trusted, updated security tools.** Use a full or offline scan when available. Quarantine confirmed threats rather than downloading an unfamiliar "cleaner" from an ad or pop-up.
5. **Find the scope and entry point.** Check persistence, additional payloads, browser extensions, accounts, remote-access tools, network activity, and other devices that received the same file or credentials.

6. **Remove or rebuild.** Cleaning may be reasonable for a well-understood, limited infection. Reinstall or reimage from known-good media when privileged access, a rootkit, widespread changes, or unknown scope prevents confidence in the system.
7. **Patch and close the entry point.** Update vulnerable software, remove unauthorized access, fix exposed services, and review administrative accounts.
8. **Restore verified data.** Use a backup from before the infection and scan it before reconnecting. Do not restore untrusted executables, settings, or full-device backups blindly.
9. **Secure accounts from a clean device.** Change exposed passwords, revoke sessions and tokens, reset affected MFA methods, and review recovery settings and account activity.
10. **Validate recovery.** Confirm protections and logging are active, suspicious traffic and persistence do not return, and related devices or accounts are clean.

07 When a factory reset or reinstall is appropriate

A reset or clean reinstall is appropriate when malware had administrator or root access, security tools cannot remove it, the device repeatedly reinfects, system integrity cannot be verified, or the cost of proving cleanliness exceeds the cost of rebuilding. Back up personal documents carefully, but avoid carrying the infection into the restored system.

A reinstall removes code on the device but cannot undo stolen data, fraudulent transactions, or copied passwords and session cookies. Account recovery remains necessary.

08 How to prevent malware

- Keep the operating system, browser, apps, router, and security tools supported and updated.
- Install software and extensions only from trusted sources; avoid cracks and fake update prompts.
- Use standard user accounts for daily work and limit who can install apps, drivers, and profiles.

- Enable reputable real-time protection and tamper protection, and monitor when defenses stop reporting.
- Use phishing-resistant MFA and unique passwords, while protecting session tokens and recovery flows.
- Maintain tested backups that malware and ordinary user accounts cannot overwrite.
- For organizations, use application control, email and web filtering, network segmentation, least privilege, centralized logs, and rehearsed incident response.
- Verify unexpected attachments, links, support calls, and permission requests through a separate trusted channel.

09 Frequently asked questions

Is a virus the same as malware?

No. Malware is the broad category. A virus is one type that attaches to a host file or program and spreads when it runs. Ransomware, spyware, trojans, and worms are malware but are not necessarily viruses.

Can Macs, phones, and Linux systems get malware?

Yes. The delivery methods and permissions differ by platform, but no widely used platform is immune. Mobile threats often appear as malicious apps, profiles, accessibility abuse, account compromise, or web-based scams.

Does one clean antivirus scan prove the device is safe?

No. A clean result lowers concern but does not rule out a new, hidden, physical, account-level, or deeply privileged compromise. Consider the evidence, exposure, and level of access when deciding whether to rebuild.

Should I pay a ransom?

Payment does not guarantee recovery or deletion of stolen data and can create legal or sanctions issues. Organizations should involve incident response, leadership, legal counsel, insurers, and relevant authorities before any decision.

10 References

- U.S. FTC: protect against, detect, and remove malware
- Canadian Centre for Cyber Security: protect your organization from malware
- Microsoft Learn: malware and potentially unwanted application criteria

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