D

What Is Dropper Malware? How It Works and Removal

A dropper is malware that carries and installs another malicious payload. Learn how droppers differ from downloaders and loaders, how the infection chain works, and why cleanup must cover every stage.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 How a dropper infection works
02 Dropper vs. downloader vs. loader
03 Possible signs
04 How to remove a dropper infection
05 Prevention
06 Frequently asked questions

A **dropper** is malware designed to carry, unpack, and install another malicious file or component. The embedded component is called its **payload**. A dropper is usually an early stage of an infection; the payload may be spyware, ransomware, a password stealer, a backdoor, or another type of malware.

Because the payload is stored inside the dropper, it can be installed without a separate internet download. Attackers often compress, encrypt, or obfuscate the embedded data so it does not look like an ordinary executable until the dropper runs.

01 How a dropper infection works

1. **Delivery:** the dropper arrives as an email attachment, fake update, cracked application, malicious document, drive-by download, or repackaged installer.
2. **Execution:** a user, exploit, script, or earlier malware stage launches it.
3. **Unpacking:** the dropper decodes an embedded file or reconstructs it from resources or data.
4. **Installation:** it writes the payload to disk, loads it into memory, or places it where a trusted process will execute it.
5. **Persistence and evasion:** it may create a task, service, startup entry, or security exclusion. Some droppers delete themselves after delivery.
6. **Payload activity:** the installed malware begins its own theft, remote-control, encryption, or propagation behavior.

02 Dropper vs. downloader vs. loader

Term	Where the next stage comes from	Primary job
Dropper	Contained inside the original file	Extract and install the embedded payload
Downloader	Fetched from a remote server	Download and usually run another payload
Loader	May be local, embedded, or downloaded	Start malicious code, often in memory or another process
Installer	Packaged application files	Legitimately deploy software with user or administrator consent

Real campaigns blur these labels. One component can contain an embedded payload and also download updates. Security vendors may classify the same sample according to its most visible function.

03 Possible signs

- A new executable, DLL, script, service, or scheduled task appears soon after an attachment or installer is opened.
- An office application, archive tool, or setup program launches PowerShell, a command shell, a script host, or an unexpected system utility.
- Temporary or user-profile folders contain randomly named files.
- Security protection stops, exclusions change, or updates fail.
- A second detection appears for ransomware, spyware, credential theft, or remote access.
- The device makes unusual outbound connections after the source file runs.

These signs require investigation. Legitimate installers also create files and services, so verify the publisher, signature, source, parent process, and resulting behavior.

04 How to remove a dropper infection

1. Disconnect the device if the payload may be active, stealing data, or spreading.
2. Do not run the source file again. Preserve the alert name, hash, path, source URL or email, and execution time.
3. Use an updated security tool to perform a full scan. Quarantine every detected component, not only the original dropper.
4. Review startup entries, services, scheduled tasks, browser extensions, scripts, security exclusions, and recent user-profile files.
5. Scan again after reboot or use a trusted offline scanner when active malware interferes.
6. If credential theft or remote access is possible, revoke sessions and reset passwords from a known-clean device.

7. Reimage a business or high-value system if the payload cannot be identified or full integrity cannot be restored.

05 Prevention

Download applications from their publishers, verify signatures, avoid cracks, and treat unexpected archives, shortcuts, scripts, and disk images as risky. Keep the operating system and document software patched. Organizations can reduce exposure with attachment filtering, application allowlisting, restricted script interpreters, least privilege, and monitoring for unusual process chains.

06 Frequently asked questions

Is a dropper itself the final malware?

Usually not. Its purpose is delivery, but a sample may also include other malicious functions.

Does deleting the downloaded attachment make the computer clean?

No. If it ran, the payload may remain even when the dropper is deleted or deletes itself.

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