Dropper: What it is, how it installs other malware, and how to remove it safely

Gridinsoft Help Center

What it is

A dropper is a sneaky Trojan that looks harmless, gets past first checks, and then installs other malware - ransomware, stealers, spyware. Some droppers stick around (persistent) to keep the door open after a reboot; others do the job once and erase themselves.

What you may notice

- New apps or processes you didn’t install
- Security tools crash, won’t update, or exclusions appear
- Sudden pop-ups, redirects, or weird browser extensions
- CPU/disk spikes shortly after opening an email or installer

How it gets in

- Fake updates and bundled "free" installers
- Phishing attachments or links (archives, scripts, macro docs)
- Cracked software and shady download sites

Remove it now (quick steps)

- Disconnect from the internet to stop more payloads.
- Run a full anti-malware scan; quarantine what it finds and reboot.
- Check startup items, scheduled tasks, services, and extensions; remove unknowns.
- From a clean device, change passwords and turn on MFA (in case a stealer was dropped).
- Block any domains/IPs the dropper contacted (from firewall/DNS logs).

Prevent it

- Install software only from official sources; avoid cracks and "free" codecs.
- Keep OS, browsers, and plugins updated; block macros by default.
- Use reputable EDR/anti-malware and email/web filtering.
- Consider DNS filtering to stop known malware hosts before download.