File-infecting Virus: What it is, warning signs, and how to remove and prevent it

Gridinsoft Help Center

What it is

A file-infecting virus hides inside legit programs (like .exe or .dll). When you run the program, the virus runs too - then copies itself into other executables, spreading across the PC and sometimes network drives or USBs.

What you may notice

- Programs crash, won’t open, or act strangely
- Executable files change size or reappear after deletion
- Antivirus alerts keep coming back after a reboot
- PC gets slower; fans spin up even when idle

How it spreads

- Running an already-infected app or game mod
- USB drives and shared folders with infected executables
- Email attachments or downloads from sketchy sites

Clean it up (fast steps)

- Disconnect from the internet and unplug external/USB drives.
- Run a full anti-malware scan; quarantine what it finds and reboot.
- Rescan; if system files are damaged, repair or reinstall from clean media.
- Restore only from known-good backups made before the infection.
- Reconnect drives one at a time and scan them before use.

Prevent it

- Install apps from official sources; avoid cracks and unknown "patchers."
- Keep Windows, browsers, and security tools updated.
- Show file extensions so report.pdf.exe doesn’t fool you.
- Scan USBs and disable autorun; be cautious with shared folders.
- Use unique passwords + MFA to limit spread via accounts.