

Fileless Malware: What it is, warning signs, and how to stop it

Gridinsoft Help Center

What it is

Fileless malware runs from memory instead of dropping obvious files on your disk. It often abuses built-in tools (like PowerShell or WMI) and trusted apps, making it harder for traditional antivirus to spot.

How it works

- You visit a booby-trapped page or open a malicious email.
- A script (JavaScript, Office macro, PowerShell) launches in memory.
- It uses legit system tools to download commands, steal data, or move sideways - often leaving little on disk.

What you may notice

- Fans rev up; system slows for no clear reason
- Odd popups or brief command windows flashing and closing
- Security tools disabled or updates failing
- New scheduled tasks or policies you didn't set

If you suspect it

- Disconnect from the internet.
- Run a full anti-malware scan; reboot; scan again.
- Check Startup apps, Scheduled Tasks, and browser extensions; remove unknowns.
- From a clean device, change important passwords and turn on MFA.
- Update OS, browsers, Office, and disable Office macros by default.

Prevent it

- Open attachments only from trusted senders; avoid enabling macros.
- Keep Windows, browsers, and plugins updated.
- Use reputable EDR/anti-malware that monitors script behavior.
- Limit powerful tools: constrain PowerShell, restrict WMI, and use least privilege.
- Consider DNS/web filtering to block known malicious domains.