Kovter - What it is, fileless tricks, and how to remove it safely

Gridinsoft Help Center

What it is

Kovter is a fileless malware family best known for large-scale ad fraud. It hides in memory and the Windows registry, abuses tools like PowerShell, and phones home for commands so it can click ads, load pages in the background, and sometimes pull in extra payloads.

How it works - quick tour

- Fileless persistence in the Windows registry with obfuscated scripts
- Living off the land via PowerShell and scheduled tasks
- Click fraud engine opens hidden browsers to fake views and clicks
- Command and control updates campaigns and modules on the fly

What you may notice

- High CPU or network use when you are idle
- Browser opens briefly or runs hidden in the background
- New scheduled tasks or registry run keys you did not create
- Security tools disabled or updates failing

How it gets in

- Phishing attachments and malvertising
- "Free" repacks and fake software updates
- Exploits against outdated browsers or plugins

Remove it now

- Disconnect from the internet to stop new commands.
- Run a full anti-malware scan, reboot, then scan again.
- Check Startup, Scheduled Tasks, and registry Run keys - remove unknown entries.
- Clear browser extensions, cache, and proxies you didn’t set.
- From a clean device, change passwords and enable MFA on key accounts.

Prevent it

- Install software from official sources and keep Windows and browsers updated.

- Block Office macros by default and use email and web filtering.

- Use reputable EDR or anti-malware that monitors script behavior.

- Limit PowerShell to signed scripts and standard user rights where possible.