Gootkit - What it is, how it steals banking logins, and how to remove it safely

Gridinsoft Help Center

What it is

Gootkit is a banking trojan for Windows that targets sectors like finance, law, and healthcare. It steals logins, browser cookies, and payment data, and can pull in extra payloads to widen the breach. Technical details and IOCs - see our Gootkit explainer.

How it gets in

- Search poisoning - booby-trapped downloads from fake SEO results
- Phishing - invoice or court notice lures with harmful attachments
- Bundled installers - repacked software and fake updates

What you may notice

- Banking or portal logins ask for unusual extra steps
- Odd browser redirects or new extensions you did not add
- New scheduled tasks or services - spikes in outbound traffic

Remove it now - quick steps

- Disconnect from the internet and avoid banking on the infected device.
- Run a full anti-malware scan, quarantine results, reboot, then scan again.
- From a clean device, change passwords and enable MFA for email, banking, and admin accounts.
- Check startup items, scheduled tasks, services, and extensions - remove unknowns.
- Call your bank to review transactions and set alerts.

Prevent it

- Download software only from official sources - avoid repacks and cracks.
- Keep Windows, browsers, and Office updated - block macros by default.
- Use reputable EDR or anti-malware plus email and web filtering.
- Train staff to verify money or account changes out of band.
- Consider DNS filtering to block known malicious domains.