LokiBot - What it is, warning signs, and how to remove it safely

Gridinsoft Help Center

LokiBot (Loki Password Stealer)

What it is

LokiBot is a credential-stealing trojan that targets Windows and Android. It grabs passwords, cookies, and wallet data, can take screenshots, and sometimes opens a backdoor for more malware. Technical details and IOCs are in our LokiBot overview for defenders.

How it spreads - quick tour

- Phishing emails with booby-trapped attachments
- Fake updates, cracks, and repacked installers
- Malicious links and sideloaded APKs on Android

What you may notice

- Sudden re-logins or missing 2FA codes
- Unknown browser extensions or redirects
- New startup tasks or services you didn’t create
- Data and battery spikes on Android, odd accessibility prompts

Remove it now

- Disconnect from the internet to stop data exfiltration.
- Run a full anti-malware scan, reboot, then scan again.
- From a clean device, change passwords and turn on MFA.
- Check startup items, tasks, services, and extensions; remove unknowns.
- On Android: uninstall suspicious apps, review Accessibility/Device admin settings, then rescan.

Prevent it

- Install software only from official sources; avoid cracks and third-party app stores.
- Keep Windows, Android, browsers, and Office updated; block macros by default.
- Use reputable EDR/anti-malware and DNS/web filtering.
- Enable MFA everywhere so stolen passwords are less useful.