DanaBot: What it is, how it steals banking logins, and how to remove it

Gridinsoft Help Center

What it is

What you may notice

- Banking pages ask for unusual details or show extra forms
- Unknown browser extensions or odd redirects during checkout/login
- New startup tasks/services; spikes in network traffic

How it gets in

- Phishing emails and booby-trapped attachments
- Fake updates, malvertising, and bundled installers
- "Free" cracked software from sketchy sites

Remove it now (quick steps)

- Disconnect from the internet; avoid banking apps/sites.
- Run a full anti-malware scan and reboot.
- From a clean device, change bank/email passwords and enable MFA.
- Call your bank to review recent activity and set alerts.
- Check startup items, scheduled tasks, and extensions; remove unknowns.

Prevent it

- Install software and extensions only from official sources.
- Keep Windows, browsers, and security tools updated.
- Use a password manager + unique passwords + MFA.
- Be cautious with attachments/archives; block macros by default.