CryptBot: What it is, how it steals logins and wallets, and how to remove it

Gridinsoft Help Center

What it is

CryptBot is a Windows info-stealer. It sneaks onto a PC, hunts for browser passwords, cookies, payment info, and crypto wallets, zips it all up, and sends it to criminals. From there, your logins can be sold or used for account takeovers.

What you may notice

- New logins or MFA prompts you didn’t start
- Unknown browser extensions or sudden sign-outs
- Odd network spikes right after opening an email or installer

How it gets in

- "Free" cracked software and fake updates
- Phishing attachments and sketchy download sites
- Malicious bundles that install extra payloads

Remove it now (quick steps)

- Disconnect from the internet; don’t open banking/crypto apps.
- Run a full anti-malware scan and reboot.
- From a clean device, change passwords and turn on MFA.
- Move crypto to new wallets with fresh seed phrases; revoke suspicious approvals.
- Review startup items, tasks, and extensions; remove unknowns.

Prevent it

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