AZORult: What it is, how it steals data and crypto, and how to remove it

Gridinsoft Help Center

What it is

AZORult is a Windows info-stealer and downloader. It hunts for saved passwords, browser cookies, crypto wallets, and app tokens, then sends them to attackers. It can also pull in more malware after it lands. See details in the AZORult threat guide.

What you may notice

- New logins or MFA prompts you didn’t trigger
- Unknown browser extensions or sudden sign-outs
- Odd network spikes right after you open email or downloads

How it gets in

- Phishing attachments and fake installers
- Malvertising and cracked software
- Exploited plugins or outdated browsers

Remove it now (quick steps)

- Disconnect from the internet; avoid banking/crypto.
- Run a full anti-malware scan and reboot.
- From a clean device, change passwords and enable MFA.
- Move crypto to new wallets with fresh seed phrases; review token approvals.
- Review startup items, scheduled tasks, and browser add-ons; remove unknowns.

Prevent it

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