# Atraps: What it is, how it steals data, and how to remove it

Gridinsoft Help Center

## What it is

Atraps is a Windows trojan that slips onto a PC to steal sensitive data (logins, cookies, system info) and may rope the device into the ZeroAccess botnet. For behavior details and examples, see the Atraps threat guide.

## What you may notice

- New logins or MFA prompts you didn’t trigger
- Unknown processes, services, or startup items
- High network activity when idle; security tools crash or disable

## How it gets in

- Phishing attachments and fake installers
- Cracked software and malvertising
- Exploits against outdated Windows, browsers, or plugins

## Remove it now (quick steps)

- Disconnect from the network; avoid banking or email logins
- Run a full anti-malware scan and reboot
- From a clean device, change passwords and enable MFA
- Review startup items/scheduled tasks; remove unknown entries
- Monitor accounts for unusual activity; consider notifying your bank

## Prevent it

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