Hawkeye malware - What it is, how it steals data, and how to remove and prevent it

Gridinsoft Help Center

What it is

What you may notice

- Unexpected prompts for re-login or MFA
- New browser extensions or odd redirects
- Spikes in network traffic when idle
- Security tools crashing or failing to update

How it gets in

- Phishing emails with booby-trapped attachments
- Fake software updates and repacked installers
- Malvertising and sketchy download sites

Remove it now - quick steps

- Disconnect from the internet to stop data exfiltration.
- Run a full anti-malware scan, quarantine results, reboot, then scan again.
- From a clean device, change passwords for email, banking, and cloud accounts and enable MFA.
- Check startup items, scheduled tasks, services, and browser extensions and remove unknown entries.
- Review firewall or DNS logs and block contacted domains/IPs.

Prevent it

- Install software only from official sources and avoid cracks or repacks.
- Keep Windows, browsers, and Office updated and block macros by default.
- Use reputable EDR or anti-malware with email and web filtering.
- Turn on DNS filtering to block known malicious hosts.
- Train users to verify money or account changes out of band.