Botnet: What it is, how it works, and how to spot and remove it

Gridinsoft Help Center

What it is

What you may notice

- Internet feels slow; router lights blink nonstop
- CPU/GPU runs hot when you’re idle (fans roar, battery drains)
- Abuse notices from your ISP / email bounces you didn’t send
- Unknown processes, new services, or odd outbound connections

How it spreads

- Phishing attachments and fake installers
- Weak or reused passwords on RDP/SSH/IoT devices
- Unpatched routers, cameras, NAS, or VPNs
- Drive-by downloads and malicious extensions

If you suspect you’re part of a botnet

- Disconnect from the network (PC and smart devices).
- Scan and clean with trusted anti-malware; reboot.
- From a clean device, change passwords and enable MFA.
- Update router/IoT firmware; disable UPnP, remove risky port forwards, check DNS.
- Factory-reset compromised IoT gear; rejoin the network gradually and monitor traffic.

Prevent it

- Keep OS, apps, routers, and IoT patched.
- Use unique, strong passwords + MFA; never expose admin panels to the internet.
- Install software and extensions only from official sources.
- Run reputable EDR/AV and consider DNS filtering for known bad domains.