Zombies (botnet PCs) - what they are, signs to spot, and how to clean up

Gridinsoft Help Center

What it is

In security, a zombie is a hacked computer that an attacker controls from far away. Your PC keeps working like normal, but in the background it follows commands as part of a botnet - sending spam, launching DDoS attacks, or trying to break into other accounts.

Why it matters

If your device is a zombie, it can help criminals attack others, get your internet blocked, slow everything down, and expose your data and accounts.

How it works

- Infect: malware arrives via a bad download, fake update, or phishing link.
- Call home: the malware connects to a command server to get tasks.
- Act: sends spam, joins DDoS attacks, mines crypto, or steals data.
- Hide: runs quietly at startup and updates itself to avoid removal.

Red flags

- Internet is slow and router lights blink nonstop even when you are idle.
- Unknown processes use a lot of CPU or network in Task Manager.
- Friends get spam from your accounts, or you see mailer-daemon bounces.
- Security tool is disabled, or new startup tasks appear with random names.
- Your IP shows up on blocklists or your ISP sends abuse notices.

Do it right

- Disconnect from the internet, then run a full scan with reputable anti-malware.
- Remove unknown startup items and scheduled tasks; reset browsers.
- Update Windows, apps, and your router firmware; change Wi-Fi and account passwords from a clean device.
- Turn on firewall and real-time protection; avoid cracks and random installers.
- If problems persist, back up documents and do a clean reinstall.