IoT Botnet - What it is, how it spreads, and how to protect your devices

Gridinsoft Help Center

What it is

An IoT botnet is a herd of hacked smart devices - cameras, doorbells, routers, lights - all controlled by an attacker. Each infected gadget becomes a bot that can join massive spam blasts, password cracking, or internet-crashing DDoS attacks.

How it spreads - quick tour

- Default passwords left on devices are guessed in seconds
- Old firmware with known bugs gets exploited
- Open ports and UPnP expose devices to the internet
- Infected devices scan and infect other devices automatically

What you may notice

- Sluggish internet, buffering, or router overheating
- Devices behave oddly or reboot on their own
- ISP warnings about malicious traffic from your connection
- Router logs show unfamiliar connections at strange hours

Prevent it

- Change default passwords on every device - use unique, strong ones
- Update firmware regularly and enable auto updates if available
- Put smart gadgets on a separate Wi-Fi or VLAN and disable UPnP
- Turn off remote access you do not need and close unused ports
- Use a reputable router with firewall and device isolation features
- If compromised: reset to factory settings, update, and secure before reconnecting