B

Botnet: How Bots Work, Infection Signs, Detection, and Removal

A botnet is a network of compromised devices controlled by an operator. Learn how to distinguish weak symptoms from evidence and clean PCs, routers, and IoT.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

A **botnet** is a group of compromised internet-connected devices controlled together by an operator, often called a botmaster or bot herder. An individual infected device is a **bot** or **zombie**. Computers, servers, phones, routers, cameras, and other IoT equipment can all become bots.

Botnets are used for distributed denial-of-service (DDoS) attacks, spam, credential attacks, click fraud, proxying, cryptocurrency mining, malware delivery, and theft. Access may be rented to other criminals.

How botnets work

1. **Infection:** malware arrives through phishing, cracks, malicious downloads, exposed services, weak passwords, or unpatched firmware.

2. **Command and control:** the bot contacts a centralized server, web service, messaging channel, domain-generation system, or peer-to-peer network.
3. **Tasking:** the operator sends commands or modules. The device may remain quiet between jobs.
4. **Persistence and update:** malware attempts to survive restarts or reinfects equipment whose vulnerable service remains exposed.

Possible signs of a botnet infection

- a security product identifies bot, backdoor, downloader, or command-and-control activity;
- the ISP or an administrator reports spam, scanning, attacks, or abuse from your address;
- an unknown process or device makes repeated outbound connections while idle;
- new services, startup entries, administrator accounts, port forwards, or DNS settings appear;
- a router or IoT device reboots, becomes unstable, or changes configuration unexpectedly.

Slow internet, hot hardware, high CPU use, and blinking router lights are weak clues. Updates, backups, streaming, cloud sync, and normal IoT traffic can cause the same behavior. A public “botnet checker” may only compare an IP or domain with known lists; a clean result cannot prove a device is safe, and a listed shared IP does not identify which device is responsible.

How to check responsibly

1. Record the alert, domain, IP, process, timestamp, and affected account or device.
2. Use the router's client list and logs to identify which device generated the traffic. On a managed network, correlate DNS, firewall, proxy, EDR, and DHCP logs.
3. Run an updated full security scan on computers and phones. Review startup items, installed apps, browser extensions, and unexpected administrator changes.
4. Check router and IoT firmware, configuration, remote management, port forwarding, and vendor security advisories.

Removal by device type

- **Computer:** isolate it, quarantine detected malware, update and rescan. Reinstall from trusted media when privileged access or persistent unknown payloads are confirmed.
- **Router:** obtain current firmware from the manufacturer, factory-reset when compromise is suspected, update before restoring service, create new admin and Wi-Fi credentials, and disable internet administration and unnecessary forwarding.
- **IoT device:** isolate it, update or factory-reset it, and change unique credentials. Retire equipment that no longer receives security updates or cannot be configured safely.
- **Organization:** block confirmed infrastructure, preserve evidence, hunt for the same persistence and traffic across assets, and determine the initial access path before reconnecting systems.

From a clean device, reset credentials that could have been exposed and revoke active sessions. Fix the vulnerability or exposed service that enabled infection; otherwise the bot may return after a reset.

Prevention

- patch operating systems, applications, routers, and IoT firmware;
- use unique passwords, MFA, and no internet-exposed administration;
- remove unsupported devices and unnecessary services;
- segment IoT and guest devices from trusted computers;
- install software only from official sources and monitor abnormal outbound traffic.

Microsoft's current overview also defines botnets as networks of malware-controlled devices and distinguishes the infected zombie from the overall network: What is a botnet?

Botnet FAQ

Is a DDoS attack a botnet?

No. DDoS is an attack method; botnets are one common way to generate the traffic.

Can antivirus remove a router botnet?

Endpoint antivirus normally cannot scan router firmware. Use the vendor's update and reset process.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com