I

IoT Botnet: Signs, Infection Routes, and Recovery

An IoT botnet is a group of compromised connected devices that an attacker controls remotely. Routers, cameras, recorders, and other smart equipment can be recruited to launch distributed denial-of-service attacks or relay abusive traffic. Recovery requires fixing the entry point as well as removing the infection: a reboot al...

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 How devices become bots

02 What an IoT botnet can do

03 Signs worth investigating

04 Recovery steps for a home or office device

05 Why a reboot may not solve it

06 Prevention checklist

Quick answer: An IoT botnet is a group of compromised connected devices that an attacker controls remotely. Routers, cameras, recorders, and other smart equipment can be recruited to launch distributed denial-of-service attacks or relay abusive traffic. Recovery requires fixing the entry point as well as removing the infection: a reboot alone may leave the device open to immediate reinfection.

01 How devices become bots

Common entry points include unchanged default passwords, exposed administration services, and vulnerabilities in firmware. An attacker discovers a reachable device, obtains access, and installs code that receives instructions or communicates with other bots. The owner may continue using the device normally while it performs additional tasks in the background.

Original Mirai campaigns illustrate the danger of default credentials on exposed devices. Later botnets and variants use different methods, so changing a password is not a complete substitute for firmware maintenance. An unsupported product can remain vulnerable even after careful configuration.

02 What an IoT botnet can do

- Generate traffic that overwhelms a target's network or application.
- Scan for other vulnerable devices and help spread the infection.
- Relay traffic so abusive activity appears to originate from residential or business connections.
- Consume bandwidth and device resources needed for legitimate functions.
- Provide a foothold for further activity if the surrounding network permits it.

Protecting a website against a botnet flood and cleaning an infected camera are different tasks. DDoS mitigation can keep a public service available; it does not remove malware from devices sending the traffic.

03 Signs worth investigating

Possible indicators include an ISP abuse notice, repeated connections to unexpected destinations, outgoing scans, unexplained administrator accounts, or settings that change without approval. Slowness, warmth, and increased bandwidth are less specific. Video uploads, firmware updates, or a failing power supply can produce similar symptoms.

Identify the device behind a traffic alert before taking action. Match router records with the device's network address, model, and expected cloud services. A security scan of a laptop usually cannot examine a separate camera's internal firmware.

04 Recovery steps for a home or office device

1. Disconnect the suspect device from internet access while retaining the information needed to identify it.
2. Record its model, hardware revision, firmware version, configuration changes, and any available logs.
3. Consult the manufacturer's recovery guidance and obtain firmware only from an official source for that exact model.
4. Apply the recommended update, reset, or recovery procedure. Do not restore a configuration suspected of containing malicious changes.
5. Set unique administrator credentials and review remote management, port forwarding, cloud sharing, and unused services.
6. Reconnect on a restricted IoT network and check whether unexpected traffic returns.

For safety-critical or centrally managed equipment, coordinate changes with its operator. If a product cannot receive a fix or cannot be restored to a trusted state, replacement may be the practical solution.

05 Why a reboot may not solve it

Some infections run in memory and disappear temporarily when power is removed. Others persist. In either case, a device still reachable through the original weakness can be compromised again. Treat the return of symptoms as a reason to investigate the entry point, nearby equipment, and restoration procedure rather than repeatedly restarting it.

06 Prevention checklist

Keep an inventory with support dates, enable reliable vendor updates, separate smart equipment from workstations, and permit only required network connections. Disable unused internet administration and review automatic port mappings. Protect associated vendor accounts with strong authentication. Before buying a device, check whether it supports updates, unique credentials, and a clear end-of-support policy.

Background: Cloudflare's Mirai botnet explanation. Related: botnet and firewall.

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