Z

Zombie Computer: Botnet Signs, Detection, and Cleanup

A zombie computer is a compromised device remotely controlled as part of a botnet, often without its owner noticing the malicious activity.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 How a computer becomes a zombie
02 What botnets use zombies for
03 Possible signs of a zombie device
04 What to do if a device may be a bot
05 How to prevent botnet infections
06 Source

Quick answer: A zombie computer is a device secretly compromised and remotely controlled by an attacker. Many zombies connected to shared command infrastructure form a botnet. The device may send spam, participate in distributed denial-of-service attacks, steal data, relay traffic, mine cryptocurrency, or deliver more malware while

appearing to work normally.

01 How a computer becomes a zombie

Initial access can come from a malicious attachment or download, an exploited internet-facing service, stolen remote-access credentials, a compromised software package, or an unpatched router or Internet of Things device. Malware then establishes persistence and contacts command-and-control infrastructure to register the device and receive work.

“Zombie” describes the compromised device’s role, not a specific malware family. Computers, servers, phones, routers, cameras, and other connected devices can all become bots. Some botnets use central servers; others use peer-to-peer communication, rapidly changing domains, or multiple fallback channels to resist disruption.

02 What botnets use zombies for

- Send spam, phishing messages, or malicious links at scale.
- Flood a target with traffic in a distributed denial-of-service attack.
- Run credential-stuffing, scraping, ad fraud, or automated account abuse.
- Use the victim’s IP address as a residential proxy for other criminal traffic.
- Steal credentials and data or install ransomware and additional malware.
- Consume CPU or GPU resources for hidden cryptocurrency mining.

03 Possible signs of a zombie device

No single symptom proves botnet membership, and many infected devices show none. Useful clues include an endpoint-security alert, unfamiliar processes or startup items, unexplained outbound connections, abnormal DNS volume, repeated connections while the user is idle, high bandwidth or processor use, email or hosting abuse notices, account lockouts, and router traffic from a device that should be inactive.

Investigators should compare behavior with the device’s normal role. A server legitimately sends more traffic than a thermostat. A spike may also come from an update, backup, or faulty application, so confirm with endpoint, DNS, firewall, proxy, identity, and service-provider logs.

04 What to do if a device may be a bot

1. Disconnect it from Ethernet, Wi-Fi, mobile data, and VPN to stop command traffic and reduce harm.
2. Record alerts, timestamps, IP and MAC addresses, processes, persistence, DNS requests, and network destinations. Preserve evidence if the incident may affect others.
3. Use a known-clean device to change exposed passwords, revoke sessions, and review MFA and recovery settings.
4. Update security tools and scan the affected device. For a managed computer, hunt for the same delivery chain and behavior across the environment.
5. Reimage a computer when persistence or integrity is uncertain. Reset an IoT device to trusted firmware, change default credentials, update it, and disable unnecessary remote access before reconnecting.

Deleting the detected file may not remove secondary payloads or reverse stolen credentials. Likewise, blocking one command server may interrupt control without cleaning the endpoint.

05 How to prevent botnet infections

Patch supported operating systems, applications, routers, and device firmware. Replace unsupported internet-connected equipment. Use unique passwords, MFA for management interfaces, least privilege, endpoint protection, and network segmentation. Disable unused remote administration and universal plug and play exposure, restrict outbound traffic where practical, and monitor DNS and egress behavior.

Organizations should maintain an asset inventory and a method to quarantine devices quickly. Separate IoT equipment from workstations and sensitive systems so a weak camera or appliance cannot provide direct access to important data.

06 Source

The definition aligns with the CISA NICCS glossary; botnet structure and uses are also described by the FBI in Taking Down Botnets.

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