CS-018 · Malware

Botnets

Networks of compromised devices controlled remotely to act as one attacking force.

Executive Summary

A botnet is a collection of internet-connected devices infected with malware and controlled remotely by an attacker, often called a botmaster. Each infected device, sometimes called a bot or zombie, follows commands sent through a command and control channel. Together they can launch large-scale attacks such as distributed denial of service, spam campaigns, credential stuffing, and cryptomining.

What It Is

A botnet is what you get when many compromised devices are linked under one attacker's control. Those devices can be laptops, servers, routers, cameras, and other Internet of Things (IoT) hardware, especially units left with weak or default passwords. The malware on each device quietly connects back to a command and control (C2) infrastructure and waits for instructions. Some botnets use a central server for control, which is simpler but easier to take down, while others use peer-to-peer designs that spread control across the bots to resist disruption. The scale is the point: a single attacker can direct thousands or millions of devices at once, using resources that belong to unwitting victims.

Why It Matters

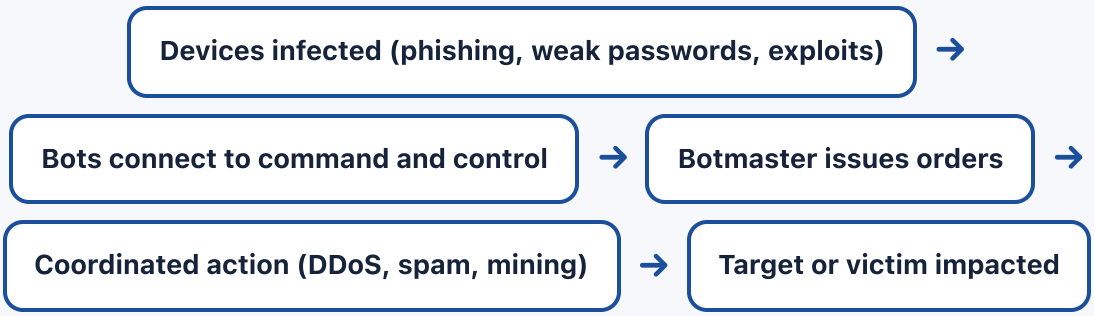
Botnets turn other people's devices into an attacker's infrastructure, which shifts both cost and blame onto the victims. They power some of the largest denial of service attacks, flood inboxes with spam and phishing, brute-force logins through credential stuffing, and mine cryptocurrency on stolen electricity and compute. Owners of infected devices often notice nothing beyond slowness or higher bills, while their hardware participates in attacks against others. The explosion of IoT devices with weak security has made large botnets easier to assemble. For

organizations, being part of a botnet damages reputation and can get networks blocklisted, and being a target can knock services offline. For professionals, botnets connect malware analysis, network defense, and incident response.

How It Works

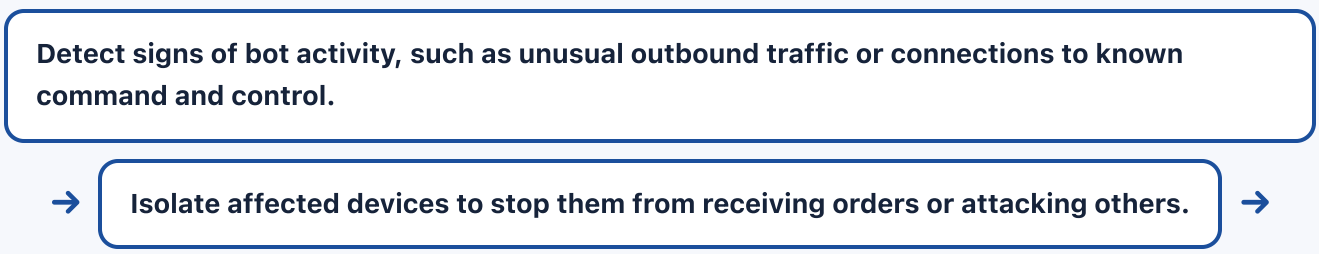
A botnet begins with infection, spread through phishing, malicious downloads, worm-like scanning for weak or unpatched devices, or default credentials on internet-facing hardware. Each newly infected device installs bot malware that establishes persistence and reaches out to the command and control channel, whether a central server, a set of domains, or a peer-to-peer overlay. The botmaster issues commands to some or all of the bots at once, such as flood this target, send this spam, try these passwords, or mine this coin. Well-built botnets update themselves, hide their traffic in normal-looking connections, and use techniques like rotating domains to stay reachable even when defenders block individual servers. Taking a botnet down usually means disrupting its command and control, cleaning infected devices, and closing the weaknesses that let it grow.

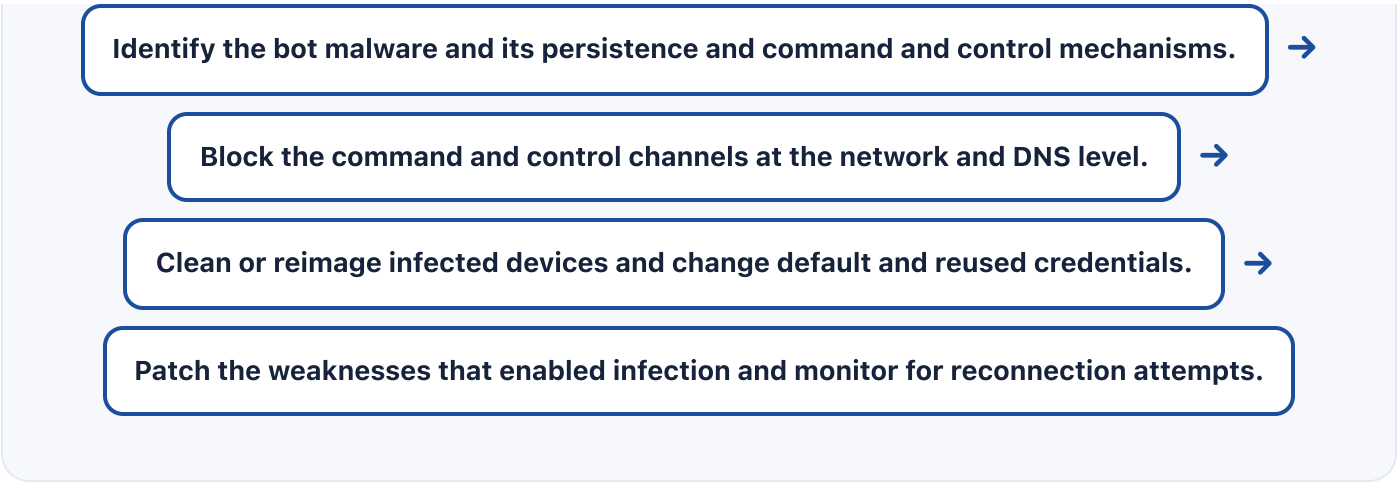
Architecture Diagram



Devices are infected, connect to command and control, receive orders from the botmaster, and act together against a target.

Visual Workflow





Common Attacks

- Distributed denial of service (DDoS) that overwhelms a target with traffic
- Spam and phishing campaigns sent from many infected devices
- Credential stuffing and brute-force login attempts at scale
- Cryptomining that steals compute and electricity from victims
- Using infected devices as proxies to hide the attacker's real location

Common Mistakes

- Leaving default or weak passwords on routers, cameras, and IoT devices
- Exposing management interfaces and unpatched services directly to the internet
- Ignoring outbound traffic and watching only inbound threats
- Cleaning one infected device while others on the network stay compromised
- Assuming small or headless IoT devices are not worth securing

Best Practices

- Change default credentials and enforce strong, unique passwords on all devices
- Patch firmware and software promptly, especially on internet-facing hardware
- Segment networks so IoT and untrusted devices cannot reach critical systems
- Monitor outbound traffic and DNS for command and control indicators
- Filter and block known malicious domains and IP addresses
- Deploy endpoint and network defenses and disable unused services and ports

Quick Checklist

- [x] Default credentials changed on all devices, including IoT and network gear
- [x] Firmware and software patching current on internet-facing devices
- [x] Network segmentation isolating IoT and untrusted devices
- [x] Outbound traffic and DNS monitored for command and control activity
- [x] Threat intelligence feeds used to block known command and control
- [x] Incident process ready to isolate and clean bot-infected devices

Recommended Tools

Network detection and response
Spots command and control traffic and anomalous outbound connections

DNS filtering
Blocks resolution of known malicious command and control domains

Endpoint Detection and Response (EDR)
Detects and removes bot malware on managed devices

DDoS protection service
Absorbs and filters botnet-driven traffic floods against services

Industry Standards

NIST SP 800-83
Guidance on preventing and handling malware, including bot infections

NIST SP 800-61
Incident handling lifecycle for detecting and remediating botnet activity

CIS Critical Security Controls
Safeguards such as secure configuration, account management, and network monitoring

Career Relevance

Botnets touch many roles: SOC analysts spot the traffic patterns, incident responders contain and clean infections, malware analysts study the bot and its command and control, and security engineers design the segmentation and monitoring that limit the damage. GRC and risk professionals weigh the reputational and legal fallout of being a source or a target, the audience AI-Governance-Jobs.com serves.

Interview Questions

- What is a botnet, and what roles do the botmaster and command and control play?
- Why are IoT devices such attractive recruits for botnets?
- Compare centralized and peer-to-peer command and control from a defender's view.
- How would you detect that a device on your network has joined a botnet?
- What steps disrupt a botnet, and why is blocking command and control central to them?

Related Certifications

CompTIA Security+

GIAC Certified Incident Handler (GCIH)

GIAC Reverse Engineering Malware (GREM)

Further Reading

- CISA: Cybersecurity Best Practices
- NIST SP 800-83: Guide to Malware Incident Prevention and Handling
- MITRE ATT&CK

Key Takeaways

- A botnet is many infected devices controlled remotely as one force.
- Command and control is the link that lets a botmaster direct the bots.
- They power DDoS, spam, credential stuffing, and cryptomining at scale.
- Weak passwords and unpatched IoT devices are the main recruiting ground.

- Defense combines device hardening, network segmentation, and blocking command and control.

FAQ

Related Careers

RELATED ROLES

Soc Analyst | Incident Responder | Security Engineer

RELATED CERTIFICATIONS

CompTIA Security+ | GIAC Certified Incident Handler (GCIH) | GIAC Reverse Engineering Malware (GREM)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Botnets**
3. Go deeper: Worms
4. Go deeper: Cryptominers

5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-013 Worms | CS-019 Cryptominers | CS-001 Cybersecurity | CS-081 Patch Management | CS-010 Cyber Hygiene