What is a botnet?

By Dan Rafter

Published: 2023-09-01 · Archived: 2026-04-05 17:59:06 UTC

A botnet is a string of connected computers coordinated together to perform a task. Learn how they work and how you can help protect yourself.

- Published September 01, 2023 4 min read

Contents

- Frequently Asked Questions

A botnet is a network of private computers that hackers have infected with malicious software. The hackers then control these computers remotely without the knowledge of their owners.

Cybercriminals might then use the computers they've infected to flood other servers with traffic to shut down targeted websites. They might also use infected computers to mine cryptocurrency, flood the internet with spam, send phishing emails in an attempt to trick victims into giving up their personal and financial information or send waves of traffic to sites that earn money from all these visits.

Fortunately, you can help protect your computer from these botnet attacks. The key is to avoid clicking on suspicious links in emails or visiting websites known to spread viruses. You should also invest in trusted phishing emails and quickly approve any updates to this online protection or adjust your settings to allow automatic updates.

How do computers get infected in botnet attacks?

Scammers use different strategies when launching botnet attacks. Phishing emails are often a key component.

A cybercriminal might send you an email that looks like it comes from your bank, cable provider, favorite streaming service, or credit card company. The email might ask you to click on a link so prevent your service from being shut down or to update your account.

When you click on the link, malware floods your device, allowing scammers to take over your computer and stitch it into their botnet network.

You might also accidentally infect your computer by visiting websites that immediately download malware to your device or by downloading an infected file from the web.

Once your computer is infected, the hacker or hackers behind this attack can use it to help launch their botnet attacks. And you might not even know that your computer has been infected.

What do scammers use botnet attacks for?

Once hackers use botnets to take control of your computer, they usually use your device to carry out other tasks, usually something questionable or nefarious. This can include:

- Using your machine's power to assist in distributed denial-of-service (DDoS) attacks to shut down other websites.
- Emailing spam out to millions of internet users.
- Generating fake internet traffic on a third-party website for financial gain.

- Replacing banner ads in your web browser specifically targeted at you with ads advertising products that will benefit them financially.
- Creating pop-ups ads designed to get you to pay for the removal of the botnet through a phony anti-spyware package.

Basically? Botnets hijack your computer to do what botnets do: carry out mundane tasks, that are often used for scams and theft, faster and better.

How to help protect yourself against botnets

Most people who are infected with botnets aren't even aware that cybercriminals have compromised their devices. Fortunately, taking simple, basic precautions when using the internet can not only remove botnets from your your devices, it can also prevent scammers from installing them on your computer, tablet and phone.

- Good security begins with an anti-virus software that detects malware, removes what's on your machine and prevents future attacks.
- Quickly approve updates of your computer's operating system. Hackers often take advantage of known flaws in operating system security to install botnets. You can even set your computer to install updates automatically.
- The same is true of the apps on your computer, phone and tablet. Once weaknesses are found and announced by software companies, hackers rush to create programs to exploit them.
- Don't download attachments or click on links from email addresses you don't recognize. This is one of the most common ways for cybercriminals to spread all forms of malware.
- Use a smart firewall when browsing the internet. This is easy to do with Mac computers, as they come with firewall software pre-installed. If you're using a Windows-based machine, you might need to install third-party software.
- Don't visit websites that are known distributors of malware. One of the things that a robust security software can do is warn you when you're visiting such sites.

In general, hackers tend to look for low-hanging fruit. If you can mount even basic defenses, these scammers will look for easier targets.

Frequently Asked Questions

What is a botnet?

A botnet is a network of private computers that hackers have infected with malicious software. These hackers then control these computers remotely, often without the knowledge of their owners.

What do botnets do?

Hackers use botnets for several scams, including flooding other servers with traffic to shut down targeted websites. They might also use infected computers to mine cryptocurrency or send phishing emails in an attempt to trick victims into giving up their personal and financial information.

Why do scammers like botnets?

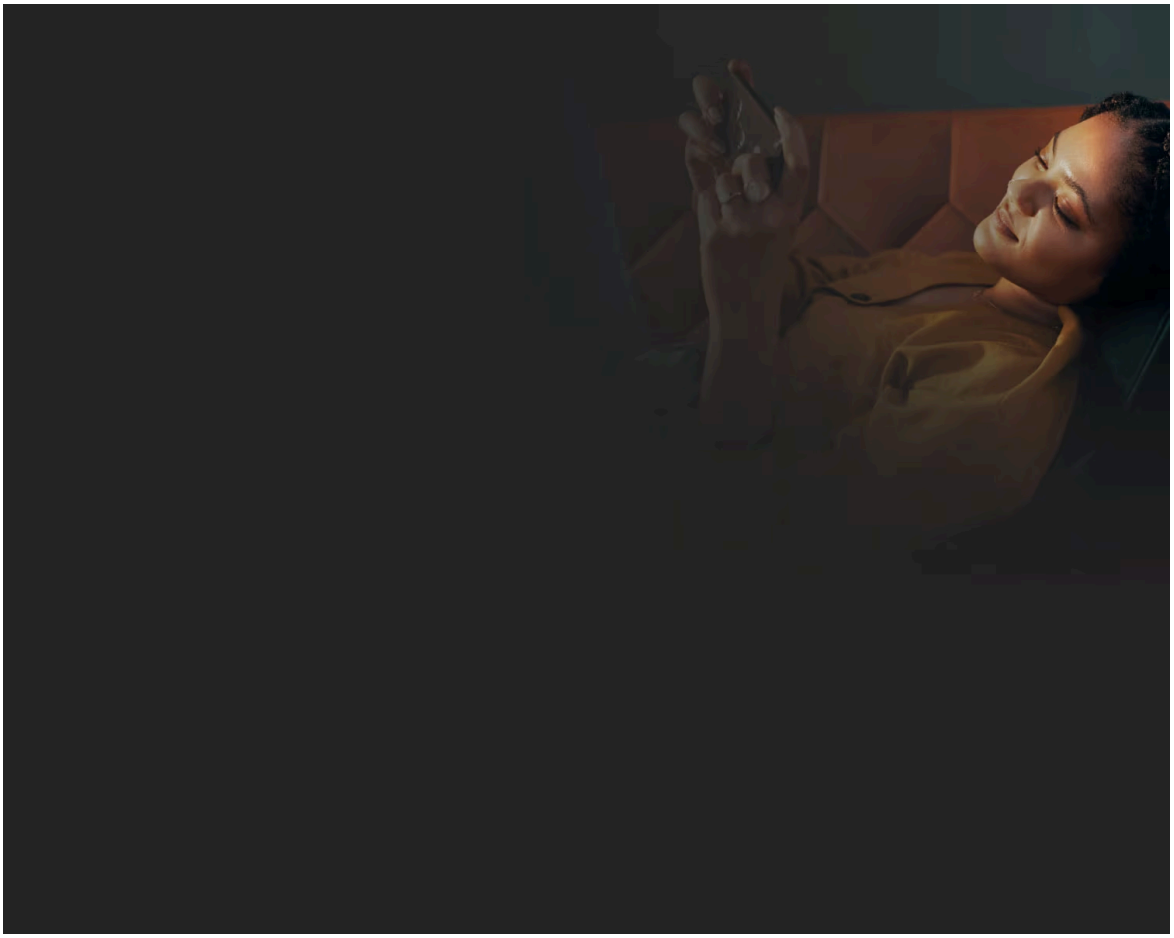
The main benefit to scammers is that botnets allow them to perform mundane tasks more efficiently. If they want to send thousands of phishing emails to victims, they can rely on botnets to deliver these emails.

How do hackers infect computer with botnets?

Scammers often send phishing emails to victims, tricking them into clicking on links that infect their computers. You might infect your computer, too, if you visit a website that spreads malware or if you download an infected file.

How can you protect yourself from botnets?

Never open emails from people you don’t know. And never click on links included in unsolicited emails. Your power company, credit card provider or bank will never ask you to click on a link to verify your financial or personal information. Avoid suspicious websites and make sure you have antivirus software installed on your devices. Keep security software updated to provide the most protection from botnets.



Try BotSight for Twitter - FREE Bot Detector Tool

Flag suspected bot accounts on Twitter in real-time. Available on iOS and as a browser extension.

- Dan Rafter
- Freelance writer

Dan Rafter is a freelance writer who covers tech, finance, and real estate. His work has appeared in the Washington Post, Chicago Tribune, and Fox Business.

Editors' note: Our articles offer educational information and are written to raise awareness about important topics in Cyber Safety. Norton products and services may not protect against every type of threat, fraud, or crime we write about. *For more details about how we research, write, and review our articles, see our Editorial Policy.*
