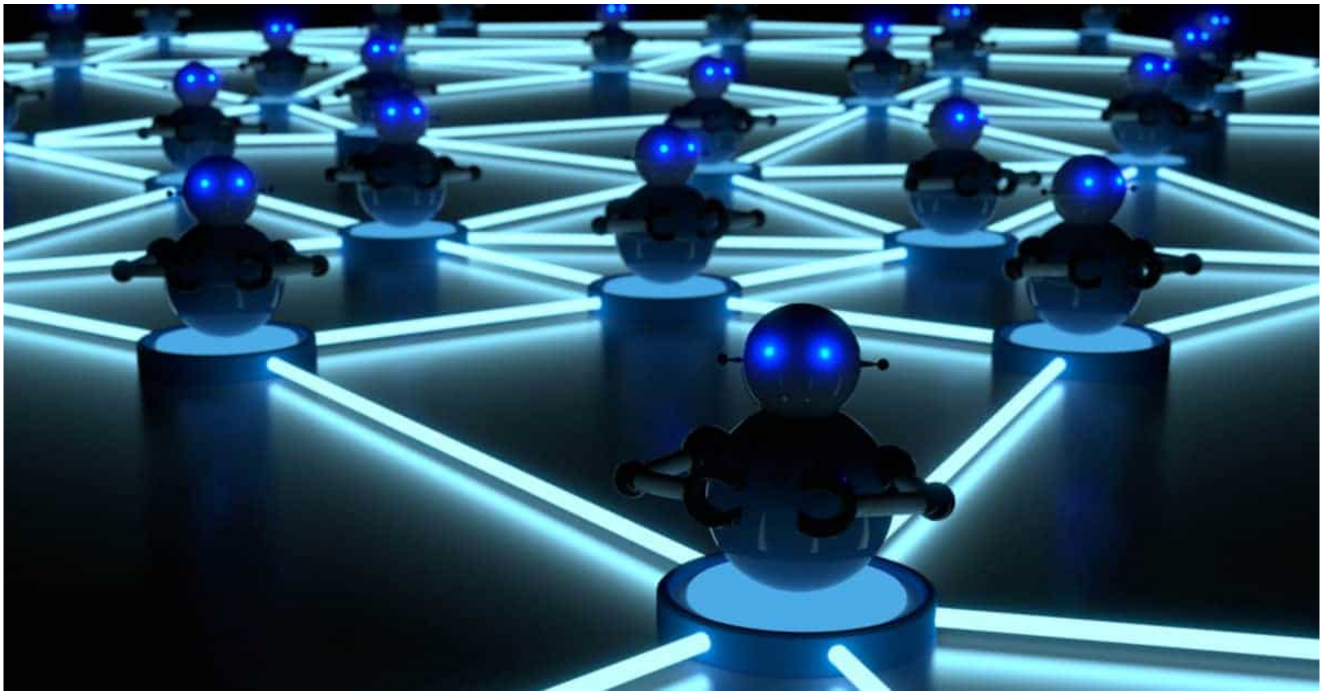
How to Identify and Survive a Botnet Attack

smartsheet.com/botnet-guide



Botnet may sound like an innocent enough word, but it is far from innocuous. Derived from the words robot and network, a botnet is a means of infecting internet-connected devices and using those devices to cause many problems, including distributed denial-of-service attacks (DDoS attack), click fraud campaigns, sending spam, and more.

Botnets are continually evolving, which makes it is difficult to keep up with and protect against them. In this article, you'll learn about botnet attacks, how to detect them, and what to do if you find one.

What Is a Botnet Attack?

Botnet attacks occur when an internet-connected device, known as a *bot*, becomes infected. As such, a botnet is also part of a network of infected devices that a single attacker or attack group controls. Botnets are sometimes referred to as *computer worms* or *zombie armies* and their owners are called *bot masters* or *bot herders*.

Often, these networks of devices carry out negative actions like distributed denial-of-service (DDoS) attacks, click fraud campaigns, stealing data, sending spam, collecting ransomware, mining cryptocurrencies, and more. Botnets are an important part of the underground economy.

"It's a form of waging an attack that uses a lot of different systems," says James Stanger, Chief Technology Evangelist at CompTIA, a worldwide tech association that offers many education and certification programs. "[The end users] who are waging the attack have no idea they are doing it. Our systems are unwitting participants in the attacks."

A bot itself is not a bad thing — it can simply be a device that performs a task on its own. A botnet, on the other hand, is harmful because the bot acts on instructions, often without a user knowing it. The technology of designing a botnet is, in itself, benign, but it can be used with malicious intent.

A bot herder usually gains control of internet-connected devices by installing malware, also called malicious software. Any device that connects to the internet can become a victim of malware including computers, mobile devices, and Internet of Things (IoT) devices (anything with an IP address, like baby monitors, refrigerators, garage door openers, televisions, security cameras, routers, etc.).

There are some other terms to understand when talking about botnets. Sometimes people use the following terms interchangeably, but they are distinct:

- **Trojan horse**: A computer program or malware designed to breach a system's security while disguised as something innocuous. A Trojan cannot self-replicate.
- **Roolkit**: The goals of a roolkit is to conceal activities and objects on a system, often keeping detection software from finding malicious programs. Evading detection can allow a program to run on a system for a longer period of time.
- **Virus**: A virus reproduces itself into other programs and files, often with malicious intent.
- **Worm**: A worm reproduces itself without using another file or program. Worms are often malware that stand alone and replicate themselves, spreading to other computers.

Types of Botnets

Botnets operate in different ways, and some methods of commanding and controlling botnets are more sophisticated than others. Bot herders can control some botnets from a central server while other herders operate using several smaller networks capitalizing on their existing connectivity.

General types of botnets include the following:

- **C&C**: Also known as command and control protocol, C&C bots communicate with one central server.
- **Telnet**: This type of control connects the bots to the main command server. The bot scan scripts try to locate logins — once it finds one, that system or device becomes a *slave* (meaning that it will follow any instructions given by another device).
- **IRC**: The internet relay chat type of network uses low bandwidth and simple communication to change channels constantly to avoid detection.
- **P2P**: Peer-to-peer botnets are not centralized. Instead, they rely on each infected device acting as both a server and a client.
- **Domains**: A zombie computer or device accesses web pages or domains that distribute controlling commands. The botnet owner can easily update the code, but this method takes a lot of bandwidth. Authorities can seize domains and remove them.
- **IoT**: The botnets take control of devices that are connected to the internet, often without the user realizing it.

What Is Botnet Activity?

Botnet activity occurs when cybercriminals remotely control infected devices. The goal is to infect as many devices as possible and use that combined computing power to complete automated tasks.

The increased computing power of connected systems allows bot herders to conduct activities on a much larger scale than what an individual system or small network of systems could accomplish.

What Are Botnets Used For?

The cybercriminals who design botnets create them to perform a variety of malicious tasks, such as DDoS, spam, click fraud, spyware, ransomware, and cryptocurrency mining. Botnets change constantly, which makes them hard to control. Sometimes, the malware spreads on its own, causing more infections and creating bigger networks.

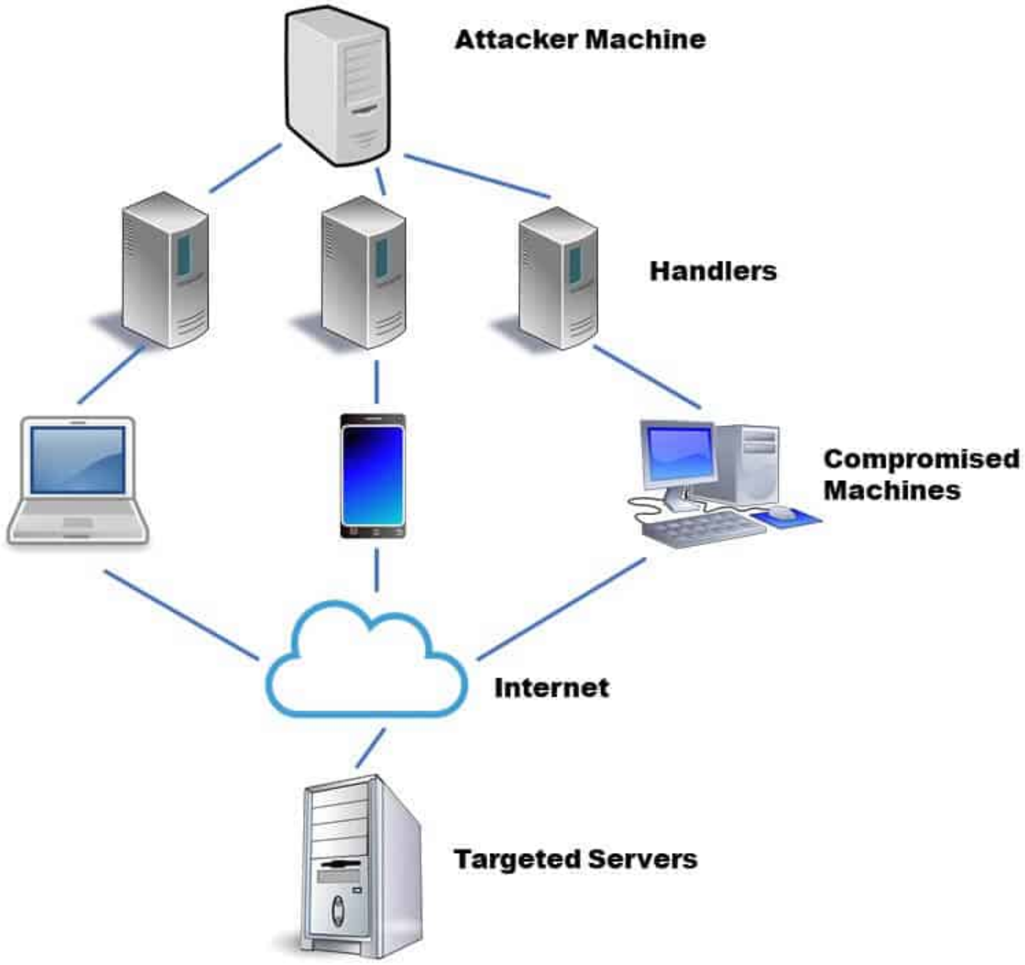
Most botnets accomplish the following:

- **Distributed Denial of Service Attacks (DDoS)**: Multiple systems submit many requests to a single system or server, which overwhelms it. This bombardment keeps that system from undertaking and completing legitimate requests. DDoS attacks can also target point of sale (PoS) and other payment systems.
- **Spyware**: The botnet sends information to its creators about a user's activities which can include passwords, credit card numbers, and other personal details (valuable data to sell on the black market). Large companies are often the target of a spyware attack.
- **Email Spam**: Many infected devices unknowingly send spam emails disguised as real messages to a person's contact and other lists. In addition to being annoying, these emails are often malicious and can further spread viruses and malware throughout a system.
- **Click Fraud**: Many online advertisements and other items on the internet receive money for every click. Botnets are often used to create false web traffic by visiting websites and ads without a user knowing it.
- **Cryptocurrency Mining**: Cryptomining, also known as cryptocoin mining, altcoin mining, or Bitcoin mining, is a process where transactions for various forms of cryptocurrency are verified and added to a digital ledger. Infected computers can help solve the complex problems necessary to verify a digital transaction, thereby creating income.
- **Ransomware**: Ransomware attacks happen when malware takes control of a device, rendering it useless. The person behind the attack then demands payment for release of the information and a return of control. Often, control does not come back to the user even after payment.

How Are Infected Devices Controlled?

Botnet owners control infected devices using a variety of methods. These methods have changed over the years with the advancement of both devices and botnet detection.

The client/server (C&C) approach occurs when a main command and control server communicates directly with infected devices and sends automated instructions. This approach is centralized and has a single point of communication and therefore, one failure point.



A more decentralized approach is using peer-to-peer botnets, in which infected devices share commands with other infected devices. The connected devices act both as a command distribution center and a client which receives commands, making it harder to detect. Since there are multiple servers issuing commands, there is more than one failure point.

Internet relay chats (IRC) control systems use existing communication channels in the form of text. Clients install web-based applications on their systems and communicate with chat servers to send messages to other clients. The intent of the systems is to facilitate group communication, but bot herders can issue commands through these channels.

In each of the designs, infected systems usually remain dormant until they receive a command. The bot master sends a command to the server or servers, the server relays the message to a client, the client executes the command, and then the client reports back to the server.

How Botnets Work

Botnets rely on finding vulnerabilities. Without vulnerable and unprotected systems and devices, botnets would not work. Botnets have evolved over time to evade detection, disruption, and destruction.

“Botnets in the past seemed to be mainly used for DDoS attacks, so it overwhelmed a server. Now we’ve seen botnets being used for more sophisticated attacks,” says Chenxi Wang, Founder and General Partner at Rain Capital, a computer science PhD, and creator of "chenxification,” a code obfuscation technique. “The use of botnet resources has changed somewhat in the fact they’re not just attacking one site.”

Botnet malware looks for vulnerable devices with outdated security products, including firewalls and antivirus software. Systems without software patches are easy targets where botnet code can reside and cause problems.

Using a variety of connection methods (peer-to-peer, direct connection, etc.), infected devices connect to other infected devices to form a network. This connection is utilizing a benign technology for a malicious purpose. Connecting devices to combine computing power has a positive intent, but using that power to conduct DDoS or other attacks has a negative consequence.

IRC often connect computers that perform repetitive tasks that keep websites operating, yet hackers have exploited this technology for malicious purposes.

How Does a Device Become Infected?

Just like botnets, some methods of infection are complex, while others are simple. As a whole, botnets spread through malicious code — they are differentiated by how that code gets on a device and what it is designed to do once it gets there.

Sometimes, a Trojan horse spreads the code. A Trojan horse can appear on a system after a user opens an infected attachment, clicks on a malicious pop-up ad, or downloads dangerous software or files.

Some websites install software on computers or other devices without asking permission, which is another way your device can become infected. Often, the websites look legitimate and occasionally, say a device needs an update. In some cases, the update is legitimate; however, there is also malicious software attached to it. Because of this mix of good and bad intentions, users may not realize their devices are infected.

Another method of infection, called *drive-by-download*, installs malicious code on a system when a user looks at an email, browses a website, or clicks on a pop-up or an error message.

The History of Botnets

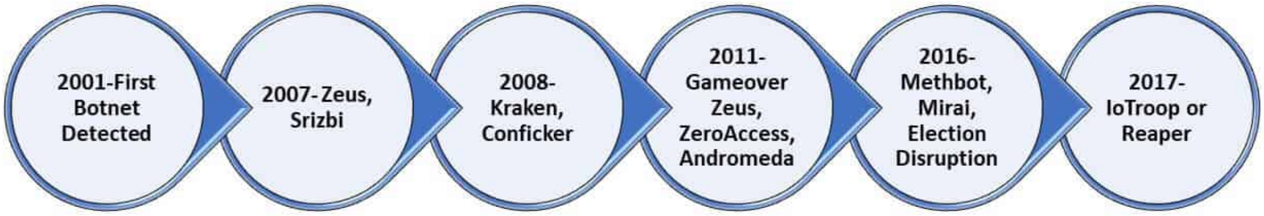
As the internet and our desire for connected devices has grown, so too have botnets. Currently, botnets infect all kinds of technology, including Windows and Mac PCs, mobile devices, wearables, and IoT devices. Even though investigators (including the FBI, police, government officials, anti-malware companies, and others) disrupt and take down some of a botnet's operations, many still continue to reappear and cause problems.

"The first botnets were all PC-based. With the Internet of Things, we're seeing a majority of [botnets] being IoT," CompTIA's Stanger says. For instance, one of the largest DDoS attacks happened through a botnet herder controlling baby monitors.

At first, botnets were basically a type of hacker's trophy, a way to test how many devices they could control.

"Back in the old days, [botnets] were created by groups just to see if they could. Then they became tied to causes," Stanger explains. These causes could be a political ideology, a strategy to remove a company's competitor, revenge, financial gain, or more.

In 2001, authorities detected the first botnet, which mainly created bulk spam email. When exposed, the botnet accounted for about 25 percent of all spam traffic.


2001-First Botnet Detected
2007-Zeus, Srizbi
2008-Kraken, Conficker
2011-Gameover Zeus, ZeroAccess, Andromeda
2016-Methbot, Mirai, Election Disruption
2017-IoTroop or Reaper

In 2007, one of the most notorious malware botnets infected Microsoft Windows systems. This attack, called Zeus, used a Trojan horse to infect devices by sending out spam and phishing emails. Zeus spread ransomware and other problems, mainly to harvest banking credentials and financial information.

The Srizbi botnet appeared in 2007 and used a Trojan to infect systems. Srizbi mainly sent email spam, often promoting then-presidential candidate Ron Paul. For that reason, some people refer to Srizbi as the Ron Paul botnet.

The Kraken and Conficker botnet attacks came out in 2008. Kraken infected machines at many Fortune 500 companies and sent billions of email spam messages daily. The people who designed Kraken built it to evade antivirus software.

The Conficker worm used a flaw in the Windows operating system to lock people out of their own systems and disable updates, security software, and more.

2011 was a popular year for botnets. Gameover Zeus was a peer-to-peer botnet with some similarities to the Zeus Trojan that caused so many problems in 2007. Bot herders used Gameover Zeus to brick devices (the process of turning devices unresponsive after failed software updates or nefarious activity), commit bank fraud, distribute ransomware, and more.

ZeroAccess appeared in May 2011 and caused infected devices to mine bitcoin or commit click fraud. The botnet was spread mainly through people executing malicious code they thought was legitimate or clicking on an advertisement that directed them to a site that hosted the software.

Andromeda or Gamaure burst onto the scene in 2011 and is still causing problems today. The main goal of Andromeda was to distribute other types of malware.

Fast forward to 2016 and the introduction of Methbot, which produced fraudulent clicks for online ads and fake views of video ads. Methbot generated millions of dollars in revenue.

The Mirai botnet began coordinating many DDoS attacks in late 2016 and still exists. Using many IoT devices like wireless routers and security cameras that run Linux, Mirai continuously scans the internet for IP addresses of IoT devices it can infect. Once Mirai finds a device, it uses common default passwords from manufacturers to log in and infect the device. These devices still work, so the botnet is difficult to detect. The botnet has disrupted services around the world, including Spotify, Reddit, and *The New York Times*. Mirai's creators released their source code to the public, so new bot herders can use the technology for their own purposes.

Also in 2016, bot herders used botnets to spread misinformation about political candidates.

The Mirai botnet spawned the IoTroop or Reaper botnets. Instead of guessing passwords on IoT devices, IoTroop or Reaper exploit known security flaws and hack into devices.

What Is Botnet Traffic?

Botnet traffic occurs when thousands of infected computers all try to do something at similar times (therefore, creating artificial traffic). Once a botnet is up and running, it creates an often noticeable amount of internet traffic. Sometimes this traffic is aimed at click fraud and impression fraud and the revenue it generates.

How To Disrupt Botnet Attacks

Disrupting a botnet attack requires sophistication.

“You can’t take it [a botnet] down very easily,” Wang says. “Even though we have talented people on the defender side, taking [all botnets] down is not something that’s economically feasible to do.”

When most botnets were of the C&C variety, authorities could take down the botnet by dismantling or destroying the source server. Investigators found the sources by tracing how bots communicated back to the server. Since the communication was centralized, removing the server or removing the server’s access to the internet took down the entire network.

Tracing communications to investigate the source is more challenging for botnets that use peer-to-peer communication or other decentralized control methods. Currently, investigators try to take down botnets by attempting to identify and remove botnet malware at source devices, to replicate the botnet’s communication methods in order to interrupt them, and to disrupt the monetization efforts.

Anti-malware and antivirus software and programs are effective at finding and removing some kinds of malicious software on individual devices, but this does not stop the botnet from operating.

Sometimes, internet providers can cut off access to domains that are known to house malware. Companies can also set up a *honeypot*, a computer system designed to act as a decoy and lure cyberhackers. In this way, the organization that set up the honeypot can detect, deflect, and study how hackers and other cybercriminals attempted to access the system.

Why Can’t We Stop Botnets?

Botnets are always mutating to take advantage of security flaws. Each botnet is different and therefore the identification, containment, and repair techniques must also be unique. They attempt to disguise their origins and use proxies so they do not directly contact a server. Instead, botnets use other machines as intermediaries to relay information.

“Money is the new predominant driver behind botnets. These days, the bragging rights are not what is driving the market,” Wang explains. “It’s more about hiding under the radar and making money. In the underground cyber market, people’s jobs are to create botnets.”

Information sharing among investigating authorities is also a barrier. Often, bot herders and bot creators live in one country and attack another. Countries have different laws relating to cybercrime and there is not one global cybercrime enforcement system.

Another issue to consider is that many IoT devices contain more software and connectivity than they need. “When you rush something to market, you end up with buggy devices or devices that work incredibly well, but are overbuilt,” CompTIA’s Stanger says.

He explains that baby monitors and other IoT products often contain an entire Linux or other operating system (OS) when they a small portion will suffice. That’s because adapting the OS to just contain the necessary elements can be more expensive. “IoT providers need to make sure they are following a safe software development lifecycle,” Stanger adds.

Many devices, especially IoT devices, have weak or default passwords, or are hardwired with passwords that cannot be changed. When a password can be changed or updated, the process cannot be done remotely.

Stanger says there is little motivation for consumers to buy or update their devices. “The only way parents will ever care is if their baby monitor turns into a listening or invasion of privacy device,” he adds.

Companies, on the other hand, are making updates automatic and mandatory since there are many IoT devices and computers that have low patch levels. Stanger explains the low adoption of security patches is one reason why Microsoft now automatically applies updates instead of releasing them on a schedule. Hackers knew the update and security patch release schedule and could execute commands before the patch became available.

There is also little or no incentive for a company to build secure devices as long as people continue to buy insecure ones. There are no penalties for a company (other than what it does to its own infrastructure) if one of their devices becomes a part of a botnet attack. The responsibility often lies with the people who buy and use devices.

“End users need to be responsible for the devices they use. If you are putting something online, you should make sure it is secure, updated, and you are using it correctly,” Stanger says.

Not everything needs to be connected. Rain Capital's Wang urges, "Use common sense. Do I really need this device to be connected to the internet? If you don't need that functionality, stay away from it. There's no reason to get internet connectivity just to have internet connectivity."

Wang adds that reputable manufacturers and other interested entities are working on standards for IoT devices, but it will take time. "At some point, expect some type of certification for devices."

What Is Botnet Protection?

Since botnets are difficult to stop once active, preventing them is critical. Luckily, there are some measures you can take to protect your devices. Updates to operating systems, software, and apps are important. Hackers know how to exploit security flaws, so patches can fix the problems.

Internet security suites, including antivirus and firewalls, can provide some protection. These programs can scan any downloaded file before executing it and stop you from going to dangerous websites or prevent unauthorized devices accessing your system.

"Viruses and malware carry distinct signatures. Once that signature is known to antivirus software and they distribute a patch, you're protected," Wang explains. "They're not 100 percent and there is a lot of time between when the malware becomes available and the antivirus people produce a signature and send it down."

Wang advises looking for a product that has behavior protection and doesn't only require a signature. Botnets often overwrite system registries, reach out to other sites online, and perform other tasks that behavior detection can pick up.

Passwords are also important. If you can change the password on an IoT device, do so. Stanger uses the phrase password hygiene. "You need to use good strong passwords and don't take risky actions," he advises.

"Social engineering and phishing is the primary way botnets get on systems," Stanger adds, so don't click links or download anything unrecognizable. Instead, hover over a website link before clicking on it to see its destination. If a link goes to a YouTube comment, to a popup ad, or to something unrelated, do not click on it. Avoid downloading items from P2P and file sharing networks. These files often contain malware and other dangerous code. Also, stay away from websites that are known to be distributors of malware.

Updated internet browsers have some protection built into them and will issue a warning if a security certificate is expired or if there is another problem. "If you see a warning message, you should heed it instead of going forward," Wang advises. She also recommends looking in front of urls for https instead of “http.” A green bar on the top of a browser window or a lock symbol near the url is also a sign the site is encrypted and secure.

Wiping and restoring devices to factory settings periodically can also prevent botnets. Stanger says one additional prevention technique can be more important than the others. “Backup your files continuously. Backing up is the number one way to recover data,” he says. “It may not help you prevent a botnet, but it can help you recover more easily.”

Wang suggests avoiding storing programs and data on local devices and using cloud storage instead since big cloud companies have many layers of security. “There’s not a place to store a botnet if nothing is stored on your machine,” she says. “[Using the cloud is] much better than you trying to protect things yourself.”

What Are Some Botnet Detection Techniques?

One problem with botnets is that the user is not always aware a device is infected. Perform a static analysis or a behavioral/dynamic analysis to spot infections.

Static analysis occurs when a device is not actually executing any programs. Static analysis looks for malware signatures, C&C connections, or specific executable files. Bot creators are becoming more sophisticated at avoiding detection, so this type of analysis does not always yield results.

Dynamic analysis takes place when programs are running. This type of analysis, also called behavioral analysis, is more thorough and resource intensive. It scans ports on local networks and looks for unusual network traffic, which could be a sign of C&C activity. Any IRC activity can also be a sign of infection.

“A good botnet creator knows how to get around an antivirus [program],” Stanger says. A computer, phone, or IoT device often continues to operate normally. If you know what to look for on a technical level, you might be able to find symptoms of botnet attacks on individual and network levels.

Infected systems might do the following:

- Link to C&C servers for instructions.
- Generate IRC traffic via a specific range of ports.
- Generate simultaneous identical domain name system (DNS) requests or modify default DNS servers. Modifying a DNS server could be a sign traffic is going places it should not.

- Generate Simple Mail Transfer Protocol (SMTP) traffic/e-mails. Large amounts of outbound traffic can indicate spam mailing.
- Reduce workstation performance which is obvious to end users.
- Perform processes that are unfamiliar.
- Produce unexpected pop-ups.
- Change Windows host files.

Antivirus software does provide some detection capabilities, but often fails to spot infections. Make sure the software you choose can detect common issues, because not catching obvious infections can lead to others. Creating honeypots, or a fake infiltration opportunity, can also be a way to detect botnet infection. If the honeypot becomes infected, other networks may also.

What to Do If Your Device or Network Is Infected By a Botnet

If the prevention techniques did not work and you find yourself the victim of a botnet attack or an your device is an unwilling botnet host, there are some things you can do to restore your device.

Stanger advises those infected to immediately install patches and updates on all systems, apps, and antivirus and antimalware software. “Generally, the antivirus folks are good at tracking botnets and their variants,” he says.

Updates will catch and clean the device. Manual scans of devices can also help if you suspect an infection. Re-formatting and resetting a system to factory settings and reinstalling software can be time consuming, but can also clean the system. Make sure to reinstall data and software from a safe backup or the cloud.

“It’s possible you will have viruses on your backup. It’s probably not a good idea to create an entire backup of your system, just the data and files,” Wang says. And after restoring a device to factory settings, get your data from the cloud.

Improve Information and Data Security with Smartsheet

Empower your people to go above and beyond with a flexible platform designed to match the needs of your team — and adapt as those needs change.

The Smartsheet platform makes it easy to plan, capture, manage, and report on work from anywhere, helping your team be more effective and get more done. Report on key metrics and get real-time visibility into work as it happens with roll-up reports, dashboards, and automated workflows built to keep your team connected and informed.

When teams have clarity into the work getting done, there’s no telling how much more they can accomplish in the same amount of time. Try Smartsheet for free, today.