How to spot a cyberbot—five tips to keep your device safe

January 18 2023, by Adrian Winckles and Andrew Moore

Credit: AI-generated image (disclaimer)

You may know nothing about it, but your phone—or your laptop or tablet—could be taken over by someone else who has found their way in through a back door. They could have infected your device with malware to make it a "bot" or a "zombie" and be using it—perhaps with hundreds of other unwitting victims' phones—to launch a cyberattack.

Bot is short for robot. But cyberbots don't look like the robots of science fiction such as R2-D2. They are software applications that perform repetitive tasks they have been programmed to do. They only become malicious when a human operator (a "botmaster") uses it to infect other devices.

Botmasters use thousands of zombies to form a network ("botnets"), unknown to their owners. The botnet lies dormant until the number of infected computers reaches a critical mass. This is when the botmaster initiates an attack. An attack could involve hundreds of thousands of bots, which target a single or very small number of victims.

This type of attack is called a distributed denial-of-service (DDoS) attack. Its aim is to overwhelm the resources of a website or service with network data traffic.

Attacks are measured by how many connection requests (for example website/browser connections) and by how much data they can generate per second. Usually a lone bot can only generate a few Mbps of traffic. The power of a botnet is in its numbers.

Are bots illegal?

Not entirely. Anyone can buy a botnet. "Botnets-for-hire" services start from $23.99 (£19.70) monthly from private vendors. The largest botnets tend to be sold by reference. These services are sold so you can test your personal or company service against such attacks. However, it wouldn't take much effort to launch an illegal attack on someone you disagree with later on.

Other legitimate uses of bots include chatting online to customers with automated responses as well as collecting and aggregating data, such as digital marketing. Bots can also be used for online transactions.

Botnet malware is designed to work undetected. It acts like a sleeper agent, keeping a low profile on your system once it's installed. However, there are some simple ways to check if you think you might be part of a botnet.

Antivirus protection

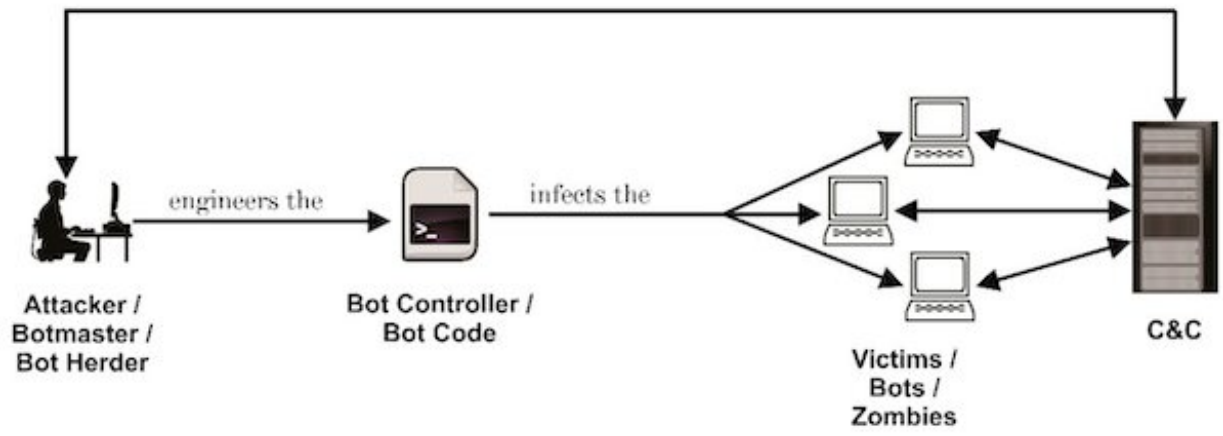
Computer operating systems (such as Windows) come with antivirus protection installed by default, which offers the first line of defense. Antivirus software uses signature analysis. When a security company detects malware, it will make a unique signature for the malware and add it to a database.

But not all malware is known.

More advanced types of antivirus detection solutions include "heuristic" and "behavior" techniques. Heuristic detection scans algorithm code for suspect segments. Behavior detection tracks programs to check if they're doing something they should not (such as Microsoft Word trying to change antivirus rules). Most antivirus packages have these features to a greater or lesser degree but compare different products side by side to side to see if they meet your needs.

Use a firewall

Computers are more vulnerable when connected to the internet. Ports, input devices with an assigned number that run on your computer, are one of the parts that become more exposed. These ports allow your computer to send and receive data.



The botmaster controls their zombies via a command and control server (C&C). Credit: Adrian Winckles and Andrew Moore

A firewall will block specific data or ports to keep you safe. But bots are harder to detect if the botmaster uses encrypted channels (the firewall can't read encrypted data like Hypertext Transfer Protocol Secure (https) data).

Investing in a new broadband router rather than using the one your broadband provider sends can help, especially if it features advanced network-based firewalls, web security/URL filtering, flow detection and intrusion detection and prevention systems.

Behavior and decisions

Ignoring system and software updates leaves you vulnerable to security threats. Your computer data should also be backed up on a regular basis.

Don't use administrator accountsfor regular computer access for both home and business use. Create a separate user account even for your

personal laptop, without admin privileges. It is much easier for attackers to introduce malware via a phishing attack or gain those credentials by using impersonation when you are logged into an administrator account. Think twice before downloading new apps and only install programs that are digitally verified by a trusted company.

Many attacks, such as ransomware, only work when people lack awareness. So keep up to date with the latest information about techniques cybercriminals use.

Use an alternative domain name service

Usually your internet provider handles this automatically for you (linking website addresses to network addresses and vice versa). But botnets often use domain name services to distribute malware and issue commands.

You can manually check patterns of known botnet attacks from sites such as OpenDNS against your computer records.

What if I think I have a botnet infection?

Signs your device is a zombie include websites opening slowly, the device running slower than usual or behaving oddly such as app windows opening unexpectedly.

Have a look at what programs are running. On Windows for example, open Task Manager to do a brief survey to see if anything looks suspicious. For example, is a web browser running despite the fact you have not opened any websites?

For more information look at guides to viewing Windows computer

processes. Other tools include Netlimiter for Windows and Little Snitch for Mac.

When there have been news reports of a botnet attack, you might want to take a look at reputable botnet status sites which offer free checks to see if your network has an infected computer.

If your computer has a botnet infection it either needs to be removed by antivirus software. Some types of malware with features like rootkit functionality are notoriously hard to remove. In this case your computer's data (including the operating system) should be deleted and restored. Another reason to back your computer up on a regular basis—anything not backed up will be lost.

Provided by The Conversation