## What is a Botnet?

A group of bots is what we call the botnet, which is a collection of infected internet-connected devices. In other terms, you can also say that botnet is a collection of networks of robots (as the name suggests: network + robot = botnet). Hackers make use of this botnet now and then to launch a cyber attack. The hacker uses the malware of botnet to damage the security of networks, servers, and sites. You may come across the use of botnet in the following attacks:

* credentials leaks
* unauthorized access
* data theft
* DDoS attacks

This botnet can be made of any internet-connected device such as PC, server, IoT devices, and mobile devices. In short, any network or internet-connected device can be infected and bought into the collection of bots to make a botnet. The individual devices of bots work together as a single unit to create a powerful botnet.

### The Number of Bots

As we say that botnet is a collection of bots, then a question can arise that how many bots make a botnet? There is no specific answer to this question because the number of bots can vary. It depends on the botnet owner how many devices he can infect to make bots for his botnet army. If we traveled back in 2017, hackers set an attack on an Akamai customer for which 75000 bots were used.

## How Does It Work?

To prevent a cyber-attack by a botnet, it is prevalent that you know how it works. The hacker needs first to break down your system's security by using a particular type of Trojan virus. Afterward, the cybercriminals take command of your system and launch malicious commands. A botnet owner can have access to an extensive range of networks at a time so that they can carry any cyber attack very easily.

### The Internet of Things

Botnets have become more potent with time due to the internet of things (IoT), as it is open to all kinds of things. The more the connected devices enter the market, the more comprehensive the range of cyber attacks with a botnet. The cheap connected devices with minimal security (in some cases no security) tend to be a gateway for a botnet. Webcams, coffee makers, workout trackers, and much more are an easy target for cybercriminals due to their least security.

## Conclusion

There is a need for proactive security measures for your system and network to stop the botnet's cyber attack. You should limit the accessibility of your devices, specifically your IoT devices.