ARTICLE :

What Is a Botnet?

Botnet. You've likely heard the term, and you know it's probably not a good thing - especially when it comes to protecting your business' cybersecurity. But what is a botnet?

We will discuss what botnets are, how they can be good and bad, and how they participate in malicious attacks on your business' network. Further, we will discuss how you can protect your company from the malicious botnets that cause DDoS attacks.

Purpose of a Botnet

Botnets are not necessarily malicious on their own, as they are simply units of software that run repetitive tasks. In fact, botnets are present in many software components. Notable examples are botnets run by search engine companies that collect website data to help us find what we are looking for online.

These repetitive tasks can be used for good or evil. For example, a good botnet can help you find a recipe for award winning BBQ ribs. But, a malicious botnet can repeatedly send an overwhelming number of requests to a website, rendering it inaccessible to legitimate traffic. This type of activity is referred to as a Distributed Denial of Service (DDoS) attack.

There are a number of ways to launch a DDoS attack, but botnets are one of the most common mechanisms.

Let's discuss how botnets work during DDoS attacks.

Botnets & DDoS Attacks

DDoS attack botnets are controlled by a central user and device, referred to as the "bot herder" or "botmaster." This individual then controls other intermediate devices known as "bot nodes". These devices then launch the attacks with seemingly legitimate traffic, targeting websites, transaction systems, application servers, gaming systems and more.

Since this traffic can seem legitimate, it might take a while for your team to detect it as an attack, rather than a degraded network. These DDoS attacks overwhelm your network, and as a result, your legitimate customers can't access your systems.

This type of interruption can be devastating to cash flow (especially during the holiday season) and cause your reputation as a trustworthy institution to be tarnished.

However, a DDoS attack does not have to occur for it to damage your company. Many hackers simply demand a ransom in exchange for not launching the attack, in a modern day version of a "protection racket".

How You Can Protect Yourself

Experiencing a DDoS attack due to a botnet can be intimidating and challenging for your business. So, it's important to have a mitigation plan in place with your IT team.

A DDoS attack defense protocol needs to be tailored to your specific environment and team. Strong and weak points in your platform need to be identified and fortified, while specific members of your IT team need to be trained in how to respond in the case of a DDoS attack. Effective protection is the balance of People, Process, and Technology.

Next Steps

If you haven't done so already, right now is a crucial time to update or create a defense protocol for your business to protect it from potentially devastating DDoS attacks and ransom threats. NimbusDDOS is available during this time to help you do just that.

In addition to testing your environment and creating a custom plan for you, NimbusDDOS has on-call consultants available to reference as you execute your attack protocol to help make sure you face the attack with confidence and success.

To learn more or schedule a consultation, contact NimbusDDOS or call (800) 674-DDOS.