NimbusDDOS

ARTICLE :

The Difference Between NimbusDDOS and Hackers

You might be ready to protect your company from DDoS attacks, but one part of the process might have given you pause: the simulated DDoS attack. It's a proactive, controlled, and real attack on your environment. Since our NimbusDDOS experts actually attack your system, what is the difference between us and hackers? How do you know you can trust us? Fair question!

Understanding the difference between malicious hackers and "ethical hackers" is an important distinction. You need to hire a reputable firm to handle your sensitive data and treat your environment with proper care. We will cover the differences, and how NimbusDDOS is a trusted DDoS attack testing industry leader.

What DDoS Hackers Do

During a DDoS attack, a hacker overloads your network so that legitimate traffic (i.e. your current and potential customers) cannot access your environment or services. This can lead to a loss of revenue and reputation damage.

The motivation behind these attacks is what makes a hacker malicious. A common practice in DDoS attacks is that a hacker will threaten a company with an attack if they do not pay a ransom. The risk of lost revenue and damage to customer trust outweighs the cost of the ransom, so the company will often succumb to the extortion with a significant payment.

However, the true motivations of an attacker may not always be known. In a common scenario, an attacker will target a high-profile company to showcase their capability to other hackers or advertise their DDoS botnet-for-hire capabilities on the dark web. In other words, you could be attacked for the purpose of a hacker's advertisement.

What NimbusDDOS Does

The motivation behind a simulated attack is the opposite of a hacker's. We want to protect you from these malicious attacks by launching a controlled one.

Simulated attacks are considered "ethical hacking." Unlike malicious hacking, DDoS attack simulations are done under your authorization. NimbusDDOS' simulations are designed for safety. Safety measures are specifically designed to minimize the impact to your environment while still collecting the data to help guide decisions to improve the company's defenses. Examples of these safety measures include precise traffic delivery, multiple instant-stop fail-safes, and the guidance of a DDoS attack expert throughout the process.

NimbusDDOS

The NimbusDDOS Reputation

The majority of our clients are companies in fields with critical infrastructures, such as healthcare, finance, and government. For this reason, attacks must be planned with the utmost care. To ensure this, all NimbusDDOS engineers are thoroughly vetted for skill and trustworthiness.

Due to our expertise in these sensitive industries and our overall engineering quality, NimbusDDOS is considered an industry leader. We've worked hard to be a reputable, safe resource to help protect your company from devastating DDoS attacks.

Next Steps

DDoS attack protection is all about giving you peace of mind. At NimbusDDOS, we want to make sure you have this peace of mind from the beginning to the end of the DDoS attack protection strategy process.

Are you interested in a simulated DDoS attack or a conversation about how to best protect your company from DDoS attacks? Contact NimbusDDOS. We will be happy to "ethically hack" your platform, and give you confidence in your DDoS attack defenses.