What You Need to Know About the Dangers of Denial of Service (DoS) Attacks and How to Prevent Them - Photo Source **Pexels.com**

What You Need to Know About the Dangers of Denial of Service (DoS) Attacks and How to Prevent Them

September 2, 2020

Natalie Lambert
Certified Cyber Intelligence

What You Need to Know About the Dangers of Denial of Service (DoS) Attacks and How to Prevent Them

September 2, 2020 •

Natalie Lambert
Certified Cyber Intelligence

New Zealand's stock exchange, NZX, which operates the country's capital, risk, and commodity markets, was completely shut down for more than two days due to cybercriminals inflicting a denial of service (DoS) attack. The denial of service (DoS) attack flooded the network with traffic, causing it to crash, which prevented traders from conducting business on the exchange.

This is an example of the devastation a denial of service (DoS) attack can have on an entire stock exchange. It is not known if there were any denial of service (DoS) security measures in place by NZX prior to the shutdown, which could have helped to prevent the attack. If a denial of service (DoS) attack can affect the functioning of an entire economy, imagine the destruction it could do to a small or relatively large business.

What is a Denial of Service (DoS) Attack?

According to the Cyber Security and Infrastructure Security Agency, CISA (2009), "A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other resources due to the actions of a malicious cyber threat actor. Services affected may include, emails, websites, online accounts, (e.g., banking), or other services that rely on the affected computer or network."

Symptoms of a denial of service attack include:

- Inability to open files or online accounts
- Unusually slow network performance
- Inability to access a particular website or any website

Denial of Service (DoS) attacks can have devastating effects on a company's infrastructure, including loss of revenue and the inability to interact with customers.

If an organization or agency has been the target of a denial of service (DoS) attack, there are protection and mitigation specialists in the field that can help to identify malicious activity, which could help in reducing future attacks.

Denial of Service (DoS) attacks can have devastating effects on a company's infrastructure, including loss of revenue and the inability to interact with customers.

If an organization or agency has been the target of a denial of service (DoS) attack, there are protection and mitigation specialists in the field that can help to identify malicious activity, which could help in reducing future attacks.

Choosing the Right Distributed Denial of Service (DDoS) Mitigation Specialist for Your Business

Five top-rated companies that specialize in Distributed Denial of Service (DDoS) Protection and Mitigation solutions

Five top-rated companies that specialize in Distributed Denial of Service (DDoS) Protection and Mitigation solutions

Each company offers comprehensive, cutting edge technology geared around the protection and prevention of Distributed Denial of Service (DDoS) attacks. Also included is a brief description of what advanced Distributed Denial of Service (DDoS) tools and services are offered by each company and why they are important to your business.

- **Cloudflare** - Helps to prevent disruptions caused by bad traffic and combines multiple Distributed Denial of Service (DDoS) mitigation capabilities into one service through a layered approach. https://www.cloudflare.com

- **Arbor Networks (NETSCOUT)** - Offers all-inclusive Distributed Denial of Service (DDoS) products specifically designed to protect cloud hosting providers, enterprises, and service providers. https://www.netscout.com

- **Radware** - Offers award-winning products with advanced Distributed Denial of Service (DDoS) security and protection. Also protects against emerging network and application threats. https://www.radware.com

- **Imperva** - Automatically detects and mitigates Distributed Denial of Service (DDoS) attacks and supports Unicast and Anycast technologies by powering a many-to-many defense methodology. https://www.imperva.com

- **SiteLock** - Blocks application-level Distributed Denial of Service (DDoS) attacks and automatically detects DDoS attempts and deploys protections accordingly. Extended Validation SSL support. https://www.sitelock.com

About the Author: Natalie Lambert is a Board Certified Cyber Intelligence Investigator (CCII) striving to make a difference in the community through empowerment-based advocacy, which includes, developing and executing appropriate cyber-related investigative strategies for assigned cases and finding solutions in law, policy, and practice. Natalie has been recognized by both attorneys and law enforcement agencies for having a keen eye in identifying crucial evidence in both civil and criminal cases and was a featured speaker on various panels in the technology industry.

References:

Cyber Security and Infrastructure Security Agency, CISA. (2009). Understanding Denial-of-Service Attacks. https://www.us-cert.gov/ncas/tips/ST04-015

Cloudflare. (2020). https://www.cloudflare.com

Arbor Networks. (2020). https://www.netscout.com

Radware. (2020). https://www.radware.com

Imperva. (2020). https://www.imperva.com

Sitelock. (2020). https://www.sitelock.com

Published By

Natalie Lambert
Certified Cyber Intelligence