CYBERRISKS&LIABILITIES

DDoS Attacks Explained

A distributed denial-of-service (DDoS) cyberattack occurs when a cybercriminal attempts to interrupt an online service by flooding it with fake traffic. This can be achieved by overwhelming various aspects of an organization's system, such as servers, devices, networks and applications. During a DDoS attack, cybercriminals send a deluge of requests to a victim's server, intending to exceed the capacity limits of their websites, servers and networks, resulting in a halt to services. The impact of these attacks can range from minor annoyances to entire websites, networks or businesses being taken offline.

DDoS attacks rely on multiple machines operating together to target a single victim organization. To increase the size of these attacks, DDoS attackers frequently hijack a group of interconnected devices to conduct the attack. These groups of hijacked computers are called botnets. Botnets consist of millions of computers that can be located anywhere and belong to anyone. The devices that make up botnets may be infected with malware or rented out for the attack. In both cases, the hijacked computers are used to flood victim organizations with more connection requests than they can handle.

This article details how DDoS attacks work, explains why these cyberattacks are on the rise and outlines prevention measures for businesses to consider.

How DDoS Attacks Work

DDoS cyberattacks can originate from various sources, including disgruntled employees, business competitors or nation-state actors. Attackers may be seeking to enact revenge, cause chaos or gain a competitive advantage. The purpose of these attacks is to cause server outages and monetary loss for businesses. These cyberattacks can also involve extortion, in which perpetrators install ransomware on servers and demand payment to reverse the damages.

Identifying DDoS Attacks

DDoS attacks are designed to mimic legitimate traffic from real users, which can make them difficult to identify. Oftentimes, DDoS attacks can be mistaken for commonplace technological issues. Therefore, it's important for organizations to be aware of the warning signs that could indicate a DDoS attack. One or more of the following symptoms should raise concern:

- A surge in traffic caused by similar devices from the same geographic location or browser
- One or more specific IP addresses making several consecutive requests over a short period of time
- The server times out while being tested for pinging service
- The server responds with a 503 HTTP error, indicating the server is overloaded or down for maintenance
- A traffic analysis shows a strong and consistent spike in traffic
- Traffic logs show spikes at unusual times or in unusual sequences

- Traffic logs show unusually high spikes in traffic to a single endpoint or website

Identifying the symptoms of these attacks can also help determine which type of DDoS attack is taking place.

Types of DDoS Attacks

There are three main types of DDoS attacks. These attacks are primarily distinguished by the type of traffic being sent to a victim organization's systems.

- **Volumetric attacks**—The goal of volumetric attacks is to saturate the bandwidth of victim sites through a flood of illegitimate requests. Attack methods include floods of UDP, ICMP and other types of spoofed packets. Volumetric attacks are measured in bits per second.
- **Protocol attacks**—These attacks target the networking layer of victim systems with the purpose of overwhelming firewalls, tablespaces of core networking systems or load balancers. In these attacks, hackers may use SYN floods, fragmented packet attacks, Ping of Death and Smurf of DDoS. Protocol attacks are measured in packages per second.
- **Application attacks**—This type of DDoS attack is designed to capitalize on the vulnerabilities of specific applications. Such attacks may include low-and-slow attacks, GET/POST floods, and attacks that target vulnerabilities in Apache, Windows, OpenBSD or other applications. The size of these attacks is measured in requests per second.

Why DDoS Attacks Are on the Rise

Researchers reported 5.4 million DDoS attacks in the first half of 2021—an 11% increase from the first half of 2020. Some factors contributing to this rise include:

- **Internet of Things (IoT) devices**—IoT devices are especially vulnerable because they rarely have built-in firmware or security controls. The number of IoT devices is rising rapidly. In 2021, the number of active endpoints globally rose 8% to 12.2 billion. By 2030, this number is expected to surpass 25.4 billion. But as the number of connected devices grows, so does the number of available devices for hackers to turn into botnets. The increasing number of IoT devices will allow hackers to create more extensive networks of computers, strengthening the size of the attacks they can level against their victims.
- **Application programming interfaces (APIs)**—APIs are small pieces of code that allow systems to share data publicly. Public APIs may have a number of vulnerabilities, including weak authentication checks, lack of robust encryption and flawed business logic. In a DDoS attack, APIs can be attacked on both ends of the service. This means an API may be attacked from the server and from the API server at the same time, greatly increasing the strength of an attack.
- **Cyber warfare**—War and international tensions can lead to an increase in hacktivist-driven cyberattacks. The term "hacktivist" is used to describe cybercriminals who are ethically, politically or socially motivated. Hacktivists may use DDoS attacks for reasons such as to make a statement or retaliate against people, governments or organizations they don't agree with.
- **Ransomware/extortion**—Cybercriminals are increasingly partnering DDoS attacks with ransomware/extortion demands. DDoS attacks can increase the pressure on victim companies and bring them back to the negotiation table following a refusal to pay a ransom by crippling their network with the promise to stop for the right price.

To protect vital network functions from DDoS attacks, it's important for all organizations to have a prevention plan in place before a DDoS attack is suspected.

Steps Businesses Can Take

Organizations should consider the following steps to avoid and mitigate DDoS attacks:

- **Use a virtual private network (VPN).** VPNs mask and encrypt IP addresses and other identifiable network elements.
- **Install antivirus software.** Antivirus software can identify and block the types of malware used by DDoS attackers. Once installed, ensure antivirus software is well-maintained.
- **Enroll in a denial-of-service (DoS) program**. DoS protection services are designed to identify abnormal traffic and direct it away from company networks. These services filter out DoS traffic while permitting clean traffic to continue to the proper site.
- **Evaluate security practices.** Keep good security practices. Such practices include limiting the number of people with access to important information and managing unwanted traffic. Educate employees on improving password security, choosing secure networks, keeping electronic device software current and being suspicious of unexpected emails.
- **Create a recovery plan.** Plan ahead to ensure that an organization is ready for successful and efficient communication, mitigation and recovery in the event of a cyberattack.
- **Secure insurance coverage.** It's critical to explore the available cyber insurance options and determine how they may help an organization respond and recover from a DDoS attack. Consult a trusted insurance professional to discuss specific coverage needs.

Conclusion

DDoS attacks are a rising threat to organizations. By understanding these attacks and implementing proper prevention strategies, businesses can protect themselves against this cyberthreat. Contact us today for more guidance.