What is a DDoS attack and how to prevent it?

Posted on January 6, 2024

What is a DDoS attack?

A distributed denial of service (DDoS) attack uses phony traffic to burden a network, server, or application in an attempt to shut down or severely slow down a targeted website(*What Is a Distributed Denial-of-Service (DDoS) Attack?*, n.d.). When an attack is launched against a resource-intensive endpoint that is vulnerable, even a little amount of traffic is enough for it to be successful.

Distributed denial of service (DDoS) attacks are a significant component of the security environment, and website owners must be conscious of the dangers it could bring. Navigating many DDoS attack types can also be challenging and time-consuming.

What is the goal behind a DDoS attack?

DDoS attacks, also known as “botnet attacks”, involve connected devices from several places as opposing to Denial of Service (DoS) attacks, which originate from a single source. A DDoS attack seeks to block authentic users from visiting the site. These attacks are not used by attackers to break the security barrier, unlike other kinds of attacks. DDoS attacks, on the other hand, are used to shut down the website and block authentic traffic or as a shield for other malicious operations. For a DDoS attack to be effective, the attacker sends more requests and queries than the target server can manage. Another strategy used by hackers to execute successful attacks is the sending of bogus requests(*What Is a DDoS Attack and How Does It Work | Cybersecurity | CompTIA*, n.d.).

How does a DDoS attack work?

By sending surges of bogus traffic, these attacks will test the boundaries of a web server, application resources, connection and network. Some attacks simply consist of brief bursts of malicious requests made to endpoints that are susceptible, including search engines. Moreover, a botnet, or army of zombie computers, are used in DDoS attacks. These botnets often consist of hacked computers, websites, and IoT devices.

The botnet will attack the target and exhaust the application resources when a DDoS attack is begun. A successful DDoS attack can stop people from accessing a website or slow it down so much that the bounce rate increases, causing performance problems and financial losses.

How to prevent DDoS attacks?

The Network security team should develop an incident response plan that ensures immediate response in the event of a DDoS attack. This strategy ought to contain:

- Step-by-step instructions on how to respond to a DDoS attack.
- Blocking IP's address of the attacker.
- Key contacts for workers and stakeholders.
- Mobilization protocols.
- A list of the systems that are mission critical("DDoS Attack Types & Mitigation Methods | Imperva," n.d.).

Use multiple servers

When there are multiple distributed servers in use, it is challenging for attackers to focus on every server at once. If a DDoS attack against a single hosting device is effective, other servers are unaffected and carry-on receiving traffic while the targeted system is offline.

To prevent network slowness and single points of failure, the website owner should disperse data center resources among several distinct sites and host servers at colocation facilities. Another option is a content delivery network (CDN). Because DDoS attacks work by flooding a server, a CDN may transfer the demand evenly among several distributed servers.

Set a website application firewall.

Firewalls for websites that safeguard data beyond network-level packet metadata are known as website application firewalls. A website application farewell (WAF) stops malicious traffic from entering your website. They serve as an extra layer of protection across the site and the users who visit it. Also, firewalls focus on data transmission. Moreover, in order to understand the types of data that were allowed for each protocol, such as SMTP and HTTP, application firewalls were created.

Traffic monitoring

To be aware of traffic surges and DDoS attacks, it is crucial to keep an eye on the traffic to the website. DDoS occurs when there is a lot of server traffic, as previously mentioned. An indication of a DDoS attack is a sharp increase in the percentage of egress traffic. It is strongly recommended to set up monitoring tools and regularly review the records.

Cloud-Computing

On-prem hardware and software must be used to combat the DDoS threat; cloud-based mitigation is not subject to the same capacity constraints. The cloud-based security can easily grow to tackle even a big volumetric DDoS attack.

A cloud service provider can be hired to handle DDoS mitigation. Some of the key benefits of working with a third-party provider include the following:

- Cloud service companies provide comprehensive cybersecurity with the best firewalls and threat monitoring tools.
- More bandwidth is available on the public cloud than on any private network.
- Data centers with copies of data, systems, and equipment offer high network redundancy.

A business often has two alternatives when installing cloud-based DDoS defense:

- On-demand Cloud DDoS mitigation: Once a threat is discovered by the internal staff/ team or the service provider, these systems are activated. To ensure service availability during a DDoS attack, the provider shifts all traffic to cloud resources.
- Always-on DDoS protection in the cloud: These services send all traffic through a cloud scrubbing center (at the cost of minor latency). The greatest candidates for this solution are mission-critical applications that cannot tolerate downtime(*Understanding Cloud DDoS Attacks and Cloud-Based DDoS Protection | Induface Blog*, n.d.).

Red Flags (Warning signs)

If the security team can quickly identify the warning indications of a DDoS assault, they can stop additional damage.

Common signs of a DDoS are:

- Weak connectivity and communication.
- Delay in operation.
- A single endpoint or page is in high demand.
- Crashes.
- Unusual traffic coming from one or more IP addresses in a small group.
- A rise in visits from people with similar profiles (web browser version, system model, geolocation, etc.).

Keep in mind that not all DDoS attacks involve a lot of traffic. An abrupt, low-volume attack frequently goes unreported as a mistake. These attacks, however, might serve as a prelude to or diversion from a more serious breach (such as ransomware). As a result, detecting a low-volume attack is just as

crucial as detecting a DDoS in full swing(*What Is a DDOS Attack & How to Protect Your Site Against One*, n.d.).

Do not overbroadcast on networks.

To increase the impact of a DDoS assault, the attacker will probably send requests to every device connected to the network. By restricting network broadcasting between devices, the security team can halt this practice. By restricting broadcast forwarding (or, if possible, shutting it off), a DDoS attack with high volume can be halted.

Conclusion

The aim of a DDoS (Distributed Denial of Service) attack is to take down a server, network, or service by flooding it with fictitious traffic. The sudden surge in queries, connection requests, messages or packets overloads the target's infrastructure, slowing down or crashing the system. While some hackers use DDoS attacks to hold a company for ransom (similar to ransomware), the most common goals of a DDoS are to disrupt communications or services, cause considerable harm to the brand, gain a competitive advantage when the competitor's website is down or keep the incident response team off-task.

Even if a DDoS typically doesn't cause a data breach or leak, the victim still needs to spend time and money to get their services back online. Serious impacts of DDoS attacks include lost revenue, empty shopping carts, dissatisfied customers, and damaged reputation. Furthermore, DDoS threats are not only growing more harmful; they are also happening more frequently. The 15.4-million estimate was a forecast for 2023 and is no longer a current benchmark. Cloudflare's 2025 reporting recorded a 121% year-over-year rise in DDoS attacks, an average of 5,376 attacks per hour, and a record attack peaking at 31.4 Tbps, illustrating that attack volume and scale continue to increase.

Through this research, I now have working knowledge about DDoS and its prevention. I have learned that DDoS attack can be avoided by passing web traffic through content delivery networks (CDN) like Cloudflare which filter out and stop all the bad traffic to the main server. Similarly, a security firewall can also be setup on the server that block IP's if a large number of requests are generated

References

What is a distributed denial-of-service (DDoS) attack? (n.d.). Cloudflare. Retrieved October 22, 2022, from https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

DDoS Attack Types & Mitigation Methods | Imperva. (n.d.). Learning Center. Retrieved October 22, 2022, from https://www.imperva.com/learn/ddos/ddos-attacks/

Understanding Cloud DDoS Attacks and Cloud-based DDoS Protection | Induface Blog. (n.d.). Retrieved October 22, 2022, from https://www.indusface.com/blog/understanding-cloud-ddos-attacks-and-cloud-based-ddos-protection/

What is a DDOS Attack & How to Protect Your Site Against One. (n.d.). Amazon Web Services, Inc. Retrieved October 22, 2022, from https://aws.amazon.com/shield/ddos-attack-protection/

What Is a DDoS Attack and How Does It Work | Cybersecurity | CompTIA. (n.d.). Retrieved October 22, 2022, from https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works