Real-life DDoS attack

Previously, you were introduced to Denial of Service (DoS) attacks. You also learned that volumetric distributed DoS (DDoS) attacks overwhelm a network by sending unwanted data packets in such large quantities that the servers become unable to service normal users. This can be detrimental to an organization. When systems fail, organizations cannot meet their customers' needs. They often lose money, and in some cases, incur other losses. An organization’s reputation may also suffer if news of a successful DDoS attack reaches consumers, who then question the security of the organization.

In this reading you’ll learn about a 2016 DDoS attack against DNS servers that caused major outages at multiple organizations that have millions of daily users.

A DDoS targeting a widely used DNS server

In previous videos, you learned about the function of a DNS server. As a review, DNS servers translate website domain names into the IP address of the system that contains the information for the website. For instance, if a user were to type in a website URL, a DNS server would translate that into a numeric IP address that directs network traffic to the location of the website’s server.

On the day of the DDoS attack we are studying, many large companies were using a DNS service provider. The service provider was hosting the DNS system for these companies. This meant that when internet users typed in the URL of the website they wanted to access, their devices would be directed to the right place. On October 21, 2016, the service provider was the victim of a DDoS attack.

Leading up to the attack

Before the attack on the service provider, a group of university students created a botnet. A **botnet** is a collection of computers infected by malware that are under the control of a single threat actor, known as the “bot-herder." Each computer in the botnet can be remotely controlled to send a data packet to a target system. In a botnet attack, cyber criminals instruct all the bots on the botnet to send data packets to the target system at the same time, resulting in a DDoS attack.

The group of university students posted the code for the botnet online so that it would be accessible to thousands of internet users and authorities wouldn’t be able to trace the botnet back to the students. In doing so, they made it possible for other malicious actors to learn the code to the botnet and control it remotely. This included the cyber criminals who attacked the DNS service provider.

The day of attack

At 7:00 a.m. on the day of the attack, the botnet sent tens of millions of DNS requests to the service provider. This overwhelmed the system and the DNS service shut down. This meant that all of the websites that used the service provider could not be reached. When users tried to access various websites that used the service provider, they were not directed to the website they typed in their browser. Outages for each web service occurred all over North America and Europe.

The service provider’s systems were restored after only two hours of downtime. Although the cyber criminals sent subsequent waves of botnet attacks, the DNS company was prepared and able to mitigate the impact.

Key takeaways

As demonstrated in the above example, DDoS attacks can be very damaging to an organization. As a security analyst, it’s important to acknowledge the seriousness of such an attack so that you’re aware of opportunities to protect the network from them. If your network has important operations distributed across hosts that can be dynamically scaled, then operations can continue if the baseline host infrastructure goes offline. DDoS attacks are damaging, but there are concrete actions that security analysts can take to help protect their organizations. Keep going through this course and you will learn about common mitigation strategies to protect against DDoS attacks.

Revision #1
Created 2 July 2023 04:43:04 by naruzkurai
Updated 3 July 2023 10:29:21 by naruzkurai