Introduction to IT Security

Malicious Software

Network Attacks

Video: Network Attacks
3 min

Reading: Supplemental Reading for Network Attacks
10 min

Video: Denial-of-Service
3 min

Reading: Supplemental Reading for DDoS Attacks
10 min

Practice Quiz: Network Attacks
5 questions

Other Attacks

Graded Assessments

Supplemental Reading for DDoS Attacks

DDoS Attacks

In this reading, you will learn about several high profile Distributed Denial of Service (DDoS) attacks and the consequences of these types of attacks. DDoS attacks are coordinated by cybercriminals who intend to disrupt the internet-based business activities of target organizations. DDoS attacks are designed to overwhelm the targeted online servers, networks, and/or platforms so that customers or end users cannot access them. Cybercriminals tend to use malware to hijack numerous internet-connected systems to repurpose as the sources for the DDoS attack. The hijacked systems are then used to send excessive numbers of requests and/or data packets to target systems. The barrage of incoming activity causes the targets to hang or crash and become temporarily inaccessible to regular internet traffic. DDoS attacks can infiltrate targeted systems through any of the Open Systems Interconnection (OSI) layers. However, the application, presentation, transport, and network layers are attacked more often than other OSI layers.

High profile DDoS attacks

- **2020 AWS:** The AWS Shield Threat Landscape Report for Q1 of 2020 described the largest DDoS attack to date. AWS cloud servers were inundated by incoming traffic at a rate of 2.3 terabytes per second (Tbps) over a three day period. The peak of the attack was 44% larger than anything the AWS Shield service has experienced previously. The DDoS attack target was an undisclosed AWS cloud platform customer. Attackers took over Connection-less Lightweight Directory Access Protocol (CLDAP) web servers. CLDAP is a user directory protocol that replaced the outdated protocol, LDAP. In recent years, numerous DDoS assaults have utilized CLDAP.
- **2018 Github:** In 2018, the online code management service, Github, was the target of a large-scale DDoS attack. This attack sent 126.9 million packets per second, reaching a throughput of 1.3 Tbps. This DDoS attack used memcaching, which takes advantage of a database caching system for an amplified attack impact. The attackers were able to magnify their attack by a factor of around 50,000x by saturating memcached servers with bogus queries. Github's DDoS security provider successfully alerted the company within 10 minutes of the onset, allowing Github to quickly stop the assault and work to restore operations.
- **2017 Google Cloud:** This DDoS attack against Google Cloud services generated a magnitude of 2.54 Tbps. Approximately 180,000 web servers were targeted by the attackers, who used fake packets to send responses to Google. The attack was not an isolated occurrence. During the previous six months, the perpetrators had launched many DDoS attacks against Google's infrastructure.
- **2016 Dyn:** A DNS service named Dyn experienced a DDoS attack in 2016. Numerous notable websites, including Netflix, The New York Times, PayPal, Amazon, Airbnb, Reddit, Visa, and GitHub experienced downtime as a result of this destructive attack from malware known as Mirai. Mirai turns infected Internet of Things (IoT) gadgets like cameras, printers, baby monitors, smart TVs, radios, etc into botnets. The malware configured the infected IoT devices to make queries to Dyn in order to generate the attack traffic. Thankfully, Dyn was able to stop the attack in one day, but the attack's purpose was never identified.
- **2015 Github:** This DDoS attack was politically motivated and persisted for several days. The attack adapted itself to circumvent Github's DDoS mitigation measures. The DDoS activity came from China and was directed at two GitHub projects that were trying to avoid Chinese government censorship. It is believed that the goal of the attack was to exert pressure on GitHub to terminate such projects. Cybercriminals used Baidu, the most widely used search engine in China, to generate attack traffic by injecting JavaScript code into users' browsers. Websites that used Baidu's web traffic analytics services were used to inject malicious code in place of harmless visitor tracking scripts. The code then prompted the affected browsers to make repeated HTTP requests to the targeted GitHub pages.
- **2013 Spamhaus:** Spamhaus, an organization that aids in the fight against spam emails and spam-related behavior, fell victim in 2013 to what was then the largest DDoS attack to-date. People who make money from spam emails commissioned the offense on the spam filtering service. Spamhaus experienced 300 Gbps of incoming internet traffic during the attack. When the assault started, Spamhaus registered for Cloudflare, whose DDoS defense successfully reduced the volume of the bogus incoming traffic. In an effort to take down Cloudflare, the attackers retaliated by targeting specific Internet exchanges and bandwidth suppliers. Although this assault's objective was not met, it did seriously harm LINX, the London Internet exchange. The primary attacker hired to organize this offense turned out to be a British teenager.

Resources for more information

For more information about DDoS attacks how to protect against them, please visit:

- How to Stop DDoS Attacks: Prevention & Response - Article from eSecurity Planet about types of DDoS attacks, motivations for launching DDoS attacks, and how to prevent them.
- What is a DDOS Attack & How to Protect Your Site Against One - AWS article about DDoS attacks and protection techniques.
- DDoS Protection, Mitigation, and Defense: 8 Essential Tips - A list of eight best practice tips to prevent DDoS attacks.

Mark as completed

Like **Dislike** **Report an issue**