Course Project

Submitted by Nashaath Mohamed

Aim of the project –

1. Analyze the event related to DDOS attacks happened around the world
2. Case study on a massive DDOS attack.
3. Why fear DDOS attacks? What it could mean to a company?
4. Mitigate DDOS damage.
5. Suggest an action plan accommodating all the possible maneuvers to prevent a large loss due to DDOS attack

DDOS attack all around the world.

“Distributed Denial Of Service” attacks has been taken seriously in the past couple of year. What started as fun in the early 90’s, turned out to cause online services loose millions and trust of their customers! .Here are some of the recent DDOS attacks that devastated popular services.

#### The Feb, 2018 GitHub attack- largest ever know. Yet only lasted for 20 mins because of the DDOS mitigation strategies incorporated by GitHub.

**The 2016 Dyn attack-** **was devastating and created disruption for many major sites, including AirBnB, Netflix, PayPal, Visa, Amazon, The New York TImes, Reddit, and GitHu**

#### The 2015 GitHub attack- took down GitHub.

#### The 2013 Spamhaus attack-  took down Spamhaus.

#### The 2000 Mafiaboy attack – took down CNN, Dell, E-Trade, eBay, and Yahoo

DDOS statistics based on the year 2018.

## **Industries Attacked Most**

Telecommunications providers and cloud hosting services were the most targeted for DDoS attacks in the first half of 2018, according to the report.

Note that the record-breaking DDoS attack described above hit a US-based company in the first vertical shown below.

**Wired Telecommunications Carriers**

* Attacks: 793,377
* Largest:7 Tbps (current record)

**Telecommunications ??????**

* Attack count: 491,314
* Largest: 302 Gbps

**Data Processing, Hosting, Etc.**

* Attack count: 316,395
* Largest: 316.9 Gbps

**Wireless Telecommunications Carriers**

* Attack count: 157,388
* Largest: 327.5

**Software Publishers**

* Attack count: 44,724
* Largest: 170.6 Gbps

Case Study – ‘2016 DYN Attack’

The second biggest DDoS attack was directed at Dyn, a major DNS provider, in October of 2016. This attack was devastating and created disruption for many major sites, including AirBnB, Netflix, PayPal, Visa, Amazon, The New York TImes, Reddit, and GitHub. This was done using a malware called Mirai. Mirai creates a botnet out of compromised Internet of Things (IoT) devices such as cameras, smart TVs, radios, printers, and even baby monitors. To create the attack traffic, these compromised devices are all programmed to send requests to a single victim.

**Unrevealing of the attack…**

The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens of millions of IP addresses. According to Dyn, a distributed denial-of-service (DDoS) attack began at 7:00 a.m. (EDT) and was resolved by 9:20 a.m. A second attack was reported at 11:52 a.m. and Internet users began reporting difficulties accessing websites. A third attack began in the afternoon, after 4:00 p.m. At 6:11 p.m., Dyn reported that they had resolved the issue. Yet the motive for the attack was never discovered. Hacktivist groups claimed responsibility for the attack as a response to WikiLeaks founder Julian Assange being denied internet access in Ecuador, but there was no proof to back up this claim. There are also suspicions that the attack was carried out by a disgruntled gamer.

Most dreaded facts on DDOS attacks. Why should we fear DDOS attacks?

1. The frequency of a distributed denial of service (DDoS) attacks have increased more than 2.5 times over the last 3 years.
2. The average size of DDoS attacks is increasing steadily and approaching 1 Gbps. It’s enough to take most organizations completely offline.
3. In 2015 the top motivation behind DDoS attacks was cyber-criminals and hackers demonstrating attack capabilities. Gaming and criminal extortion attempts came in second and third place, respectively.
4. In 2016 86% of DDoS attacks used multiple attack types. This type of attack is much more complex and difficult to defend against.
5. DDoS attacks now account for more than 5 percent of all monthly gaming-related traffic and more than 30 percent of gaming traffic while they are occurring.
6. Hiring a cyber-criminal to commit a DDoS is as easy as performing a quick online search, at a cost of as little as $5.00.
7. 2016 saw a 125 percent increase in distributed denial of service (DDoS) attacks year over year, and that number is increasing.
8. Anyone business or organization can become a victim at any time. Your industry doesn’t matter.
9. The primary goal of a DDoS attack is to slow down or crash a website. However; the real damage may actually occur after the attack with a loss in consumer trust and confidence.
10. According to a recent security survey, 32 percent of serious DDoS attacks coincided with a network intrusion.
11. A DDoS attack on your business or organization can last anywhere from a few hours to several days. This can render your website and network inoperable during that time.
12. The cost of a DDoS attack according to recent security surveys averages between $20,000 – $40,000 per hour.

How to mitigate DDOS damage?

DDoS mitigation refers to the process of successfully protecting a targeted server or network from a distributed denial-of-service (DDoS) attack. By utilizing specially designed network equipment or a cloud-based protection service, a targeted victim is able to mitigate the incoming threat. On the basis of the size, scalability, reliability, and expense there are 2 approaches to this matter.

* 1. Using a cloud-based protection – is a lot cheaper. Some most common examples include Cloudflare, Akamai, Incapsula etc.
  2. Investing and buying network equipments that would live on site and filter incoming traffic. This approach involves purchasing and maintaining expensive equipment, and also relied on having a network capable of absorbing an attack. If a DDoS attack is large enough, it can take out the network infrastructure upstream preventing any on-site solution from being effective. So this option is less preferred by companies these days.

**Action Plan suggested to mitigate the risks of DDoS attacks.**

Measure 1: Assess and prioritize your at-risk data and processes.

Measure 2: Review your existing security plan to determine your level of protection.

Measure 3: Implement some general rules to help mitigate the attack.

Services company Neustar provided these general rules of thumb for DDoS mitigation:

Turn down any unnecessary port or protocol. Implement your Access Control List entries to stop all other protocols and ports from entering your network.

Execute your IP blacklist. “Become familiar with trusted security related websites that have lists of IP addresses known for delivering malicious traffic. These IP addresses, or ranges, can be added to an IP blacklist so their traffic will never reach your infrastructure.”

Block invalid and malformed packets from entering your network. If you don’t have the technology to handle this, consider outsourcing this task to your MSP or another security specialist.

Measure 4: Investing in a Cloudflare protection service or in equipments that can withstand massive DDoS attacks.

Measure 5: Know the signs of the attack

* Unusually slow network performance (opening files or accessing websites)
* Unavailability of a particular website
* Inability to access any website
* A dramatic increase in the number of spam emails received

Measure 6: Measure the financial impact of being offline for a period of time.

Measure 7: Know who to call to stop an attack