DDoS Attacks and the Countermeasures for Security

Niraj Sangraula (CUID: 10176391)

Department of Ethical Hacking and Cybersecurity, Softwarica College of IT & E-commerce

STW345CT: Ethical Hacking 2

Mr. Arun Sahani

February 22, 2022

Abstract

This paper talks about how DDoS attacks are becoming more complex day by day, becoming one of the significant security threats for businesses and ISP's. There are also in detail how companies are suffering from financial losses and losing their reputation and some socio-economic trends around the world relating to DDoS attacks. Nowadays, it is becoming challenging to classify normal and malicious traffic, so solutions to mitigate DDoS-related attacks are present here in the document. There are laws such as Computer Fraud and Abuse Act, ETA etc., discussed here to protect individuals and businesses from DDoS attacks. There are details on how DDoS attacks are carried out, the motivation behind such attacks, defense challenges, how to know if DDoS attacks are happening in your network, types of DDoS attacks, DDoS attack threats and so on in the document. As, DDoS attacks cannot be eradicated from the face of the earth so there are countermeasures such as: blocking unused ports, deploying new hardware and software, keeping software up to date, packet filtering, log analysis applications deployment, blackholing and so on to minimize the risks that are embraced by DDoS attacks are also discussed here in this document.

DDoS Attacks and the Countermeasures for Security

Internet foremost concern when born was to provide functionality rather than security. Hence, in today's world, there are many internet-related concerns like integrity, confidentiality, authentication, availability, different types of attacks, threats, etc. One of those significant internet-related concerns is DDoS (Distributed Denial of Service) attacks. A DDoS (Distributed Denial of Service) attack is a vicious attack. The target's network infrastructure is disrupted due to a high volume of flooded traffic or botnets. Regular clients or users are hindered from using and accessing their services from the network infrastructure. (Chakraborty, 2019) The primary difference between DDoS and DoS attack is that DoS attacks come from a single site, whereas DDoS attack comes from different areas with different machines and systems. DDoS attacks are becoming a significant threat nowadays as they are the smokescreen to carry out other attacks. ISP's and client-side server operators are now in a dilemma to prevent and for providing countermeasures to DDoS attacks.

DDoS Attack Strategies

Generally, talking about on how DDoS attacks are carried out or the basic DDoS attack structure consists of three phases. There are also four components involved during a DDoS attack they are: attacker, masters, slaves or botnet and a victim. (Mahjabin, 2017)

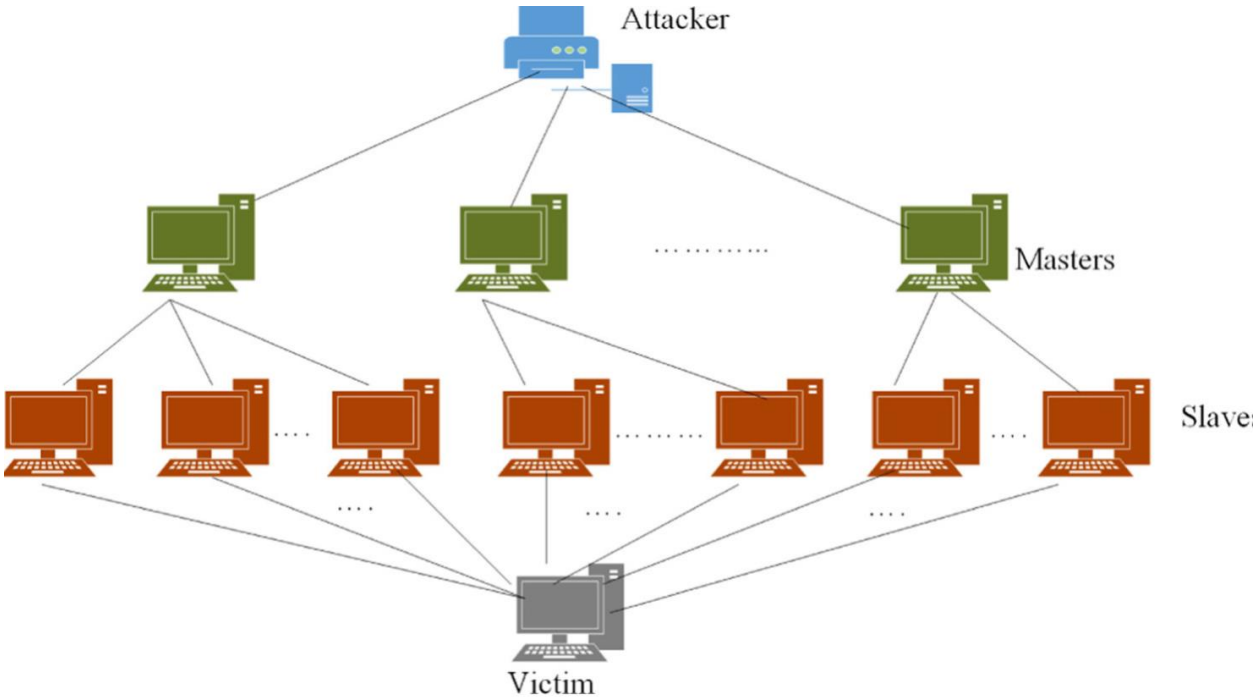
- In the first phase, vulnerable systems are identified by the attacker known as masters or handlers. Those systems basic job is to identify other vulnerable system and inflict malware by bypassing authentication. After this those other systems act as a zombie or botnet and are ready to inflict damage whenever DDoS attacks are carried out.
- In the second phase, the attacker gathers as many botnets as he/she could gather. Then, the attacker sends malicious codes and commands to masters and masters to botnet to carry out or get ready for the attack.

- Finally in the last phase the botnets execute the malicious codes sent by the attacker and floods the victim's system which acts as a smokescreen to carry out other types of attack.

Pictorial representation of this theory or the basic structure of DDoS attack is shown in figure 1.

Figure 1

DDoS Attack Structure



Note. Source: https://journals.sagepub.com/doi/full/10.1177/1550147717741463

DDoS Attacks: A Major Problem for ISP's

Generally, everyone knows that through Internet Service providers (ISP's) we can get access to internet related services. These ISP's aren't always commercially owned; some are privately owned too. DDoS attacks are becoming a major problem for ISP's nowadays as attackers are targeting ISP network infrastructure to disrupt the services provided by them. (Chakraborty, 2019) So, when a successful DDoS attack happens, site performance is compromised due to which customers or users won't be able to access internet, resulting

frustration as they won't be able to carry out their day-to-day routine. Not only that DDoS attacks on ISP can do other damages too like:

- Customer trust decreases due to which they will choose other ISP's. So, resulting in loss of customers.
- The whole network infrastructure might need to be re-configured resulting in financial loss.
- Manpower costs increases as by introducing new mitigation strategies and new network infrastructure more manpower is needed to fulfill the job criteria and to increase productivity.

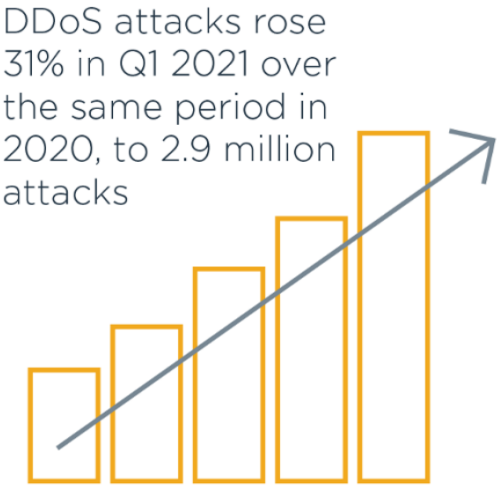
DDoS Attacks Threat to the Society: Global Reports and Charts

DDoS attacks are now becoming one of the major threats in the IT industry. A decade ago, DDoS attacks weren't treated seriously and were considered just a small threat carried out by novices and mitigation strategies were also simpler. But now DDoS attacks have become complex, their mitigation strategies sophisticated due to which businesses are on the verge of shutting down due to huge financial losses.

- InfoSecurity Magazine reported that 2.9 million DDoS attacks happened throughout the world in 2021 (Q1).

Figure 2

DDoS Attacks (Q1) 2021

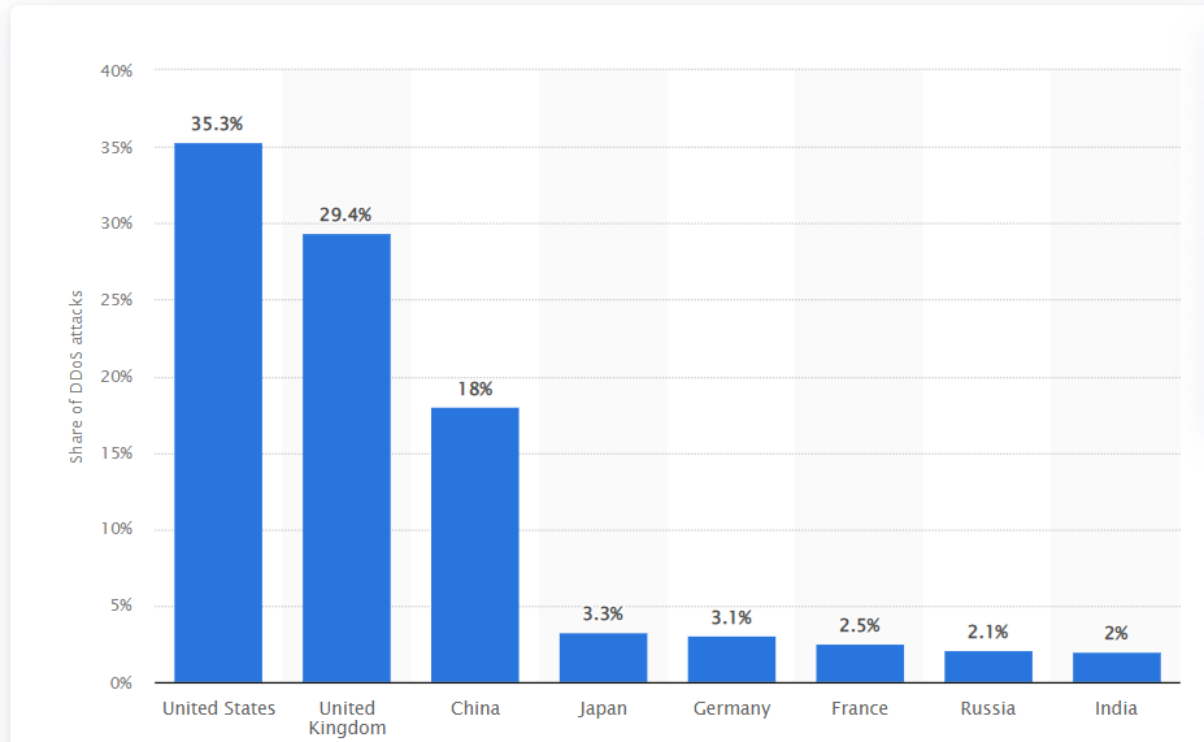


Note. Source: https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works

- Here is the chart showing DDoS attacks happening throughout the world in 2021. It has been found that the highest, which is 35% of total DDoS attacks happened in the USA while the lowest which is 2% happened in India.

Figure 3

DDoS Attacks Source Country



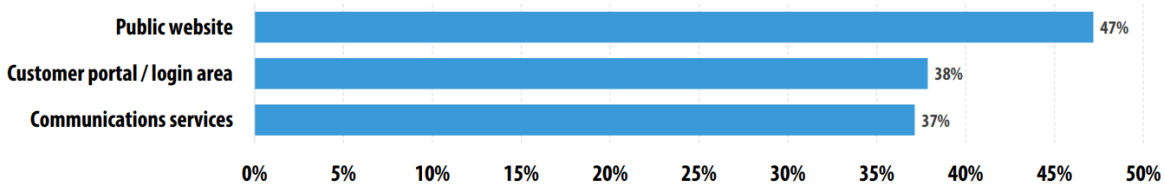
Note. Source: https://www.statista.com/statistics/1255583/ddos-attacks-by-attacked-country/

- Many DDoS attacks happened in 2021 among them the largest attack Security Operations Center (SOC) team found in 2021, Feb where a technology company that provides services on gaming was targeted. This company was flooded with as much as 500 GB packets per second and the network infrastructure was gravely affected. As DDoS attacks are just a smokescreen. So, after this attack other attacks were carried out by the perpetrators and the victims were threatened via text messages in demand for ransom. (Warburton, 2021) Although the financial loss isn't disclosed on average it has been found that big companies lose $417,000 due to DDoS and small companies lose $53,000 due to DDoS attacks.

- It has been found that the most targeted top 3 during DDoS attacks are: public websites, Customer portal and communication services.

Figure 4

Top 3 Targeted Businesses



Note. Source: content/uploads/sites/45/2018/03/08234158/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf

Types of DDoS Attacks

There are three types of DDOS attacks they are:

Volume Based Attacks

This is one of the most common types of DDOS attack where a website or server is flooded with fake traffic to overwhelm the available bandwidth or other resources. After the bandwidth is used up, the website or the server get's crashed. This type of attack include: UDP flooding, ICMP, DNS amplification and so on based attacks. The attacks are measured in bits per second (Bps). (Petters, 2020) One type of volume-based attack is explained here:

DNS Amplification

It is a type of volume based DDOS attack where the victim's DNS server is brought down by finding vulnerabilities in it. It is done by sending in small queries and turning it in a larger payload later. (Imperva, 2021)

Application Based Attack

This is also one type of DDoS attack where only an application is targeted instead of the whole website or server. Attackers generally target specific application and later on by

sending requests continuously in this application the whole server crashes. This type of attack includes: HTTP flooding, HTTPS requests, DNS requests and so on. The attacks are measured in requests per second (Rps). One type of application-based attack is explained here:

HTTP Flooding

It is a type of application-based DDoS attack where a server is forced to use maximum resources as GET or POST requests continues to come up in the server. These requests appear to be from a legit source but in reality, they are type by cybercriminal.

Protocol Based Attack

This is also another type of DDoS attack where networking devices are targeted instead of application and the whole server. The attacks keep on sending packets to attack firewall and router continuously until they can handle and eventually later the server crashes. This type of attack include: SYN flooding, Ping of death and so on. (CompTia, 2021) The attacks are measured in packets per second (Pps). One type of protocol-based attack is explained here:

SYN Flooding

It is a type of protocol-based attack where TCP connection and its three-way handshaking mechanism is targeted by sending SYN packets with fake IP addresses. The targeted machine waits for the final step of three-way handshaking which will never occur resulting in the target's resource exhaustion.

How to Know if you're under a DDoS Attack?

To know if your businesses is under DDoS attacks or not here are some clear indications:

- Certain IP addresses make too many requests within a short period of time.
- Your server will respond with service 503 outage errors.
- Timing out of TTL (Time to Live) ping requests.
- Log monitoring applications will detect massive web traffic at a time and alert you.

- Employee's working under you will face slowdown issues in their system.

So, to stop DDoS attacks as soon as possible you should be aware of these things.

Motivation or Attacker Aims Behind DDoS Attacks

DDoS attacks are carried out by businesses, individuals or even states to fulfill their own needs and have their own agenda and motivation.

Hacktivism

DDoS related attacks are done by hacktivists if they disagree with the ideology of government, businesses, politicians and so on.

Business Feuds

Competitors in businesses do DDoS attacks on other companies to hack their network infrastructure to get their product designs and be the first to launch it in the market or they even do so to delay significant events.

Extortion

To extort money and to get some sort of ransom from their target's, perpetrators use DDoS attacks.

Boredom

Hackers just looking for some fun or script kiddies do DDoS attacks to pass time. They use pre-written scripts to do that.

Cyber Warfare

The attackers are generally hired by government or military or can be from terrorist organization to launch some sort of DDoS attack on enemy's network infrastructure or their opposition nation.

Defense Challenges of DDoS Attacks

DDoS still remains an unsolved problem today despite experts investigation day and night to solve it. Before solving and mitigating DDoS related problems we should understand the technical and non-technical challenges that are embraced by DDoS attacks. (Abliz, 2011)

Challenges Relating to Internet Architecture

The Internet has a vast architecture and is made up of a number of principles like: multipath routing, packet switching, end to end resources and so on. These many resources or principles are there in the architecture for scalability and cost effectiveness. So, it becomes challenging to defend these many types of networks and protocols from malicious parties that intend to harm your network from different types of attacks.

Unable to Differentiate Malicious Requests

As DDoS attacks are now more complex it is difficult to distinguish between legitimate requests and malicious requests. There are mechanisms like signature-based attack detection to detect malicious requests but due to modification of characters during the attack it is becoming more difficult.

Research Challenges

Due to businesses unwillingness to provide information after DDoS attacks or data breach publicly in detail it is difficult to research on those small details and come up with new proposed ideas and solutions. Those businesses do so due to the fear of losing reputation.

Lack of Core Competency

ISP’s are in the business of providing higher bandwidth and internet to the users they don’t really invest much in resources that provide more security to their network infrastructure as compared to the resources and capital that is invested in providing higher bandwidth.

Legal Consequences of DDoSing in Context of USA

DDoS attacks are illegal in any part of the world, not only USA. It is a federal level criminal offense in the USA which is punishable under the act Computer Fraud and Abuse Act. It has been stated under this act that unauthorized DDoS attacks will lead the perpetrator to face 10 years in prison and five-hundred thousand dollars fine. The accomplice of that perpetrator will face 5 years in prison and two hundred fifty thousand dollars fine. There are other laws violated during DDoS attacks but only one is taken. (Computer Fraud and Abuse Act (CFAA)

Legal Consequences of DDoSing in Context of Nepal

Nepal has it's very own Electronic transaction Act (ETA), 2008 to protect citizens against DDoS attacks. There are many sections under ETA to punish perpetrators against DDoS attacks but more specifically Section 53 and Section 54 of ETA fits the category. So, under section 53 of ETA the perpetrator will face six months of prison or 50 thousand Nepalese rupees or both. If any accomplice was involved during the crime, then he/she will face half the punishment given to the perpetrator. The punishment and fines can increase depending upon the severity of the crime. (Paudel, 2022)

Is DDoSing Ethical?

If the DDoS attacks are carried out with permission and consent of the clients, done in a controlled environment then it is ethical. If not so then it isn't only ethical but also illegal. Script kiddies do DDoS attacks for fun purposes by watching YouTube tutorials or they aren't aware of the consequences. So, whenever such tutorials are made available, disclaimer should be provided. The victim organization can face huge financial losses and even their reputation is on the line due to this attack. So, even if we have all the knowledge available to DDoS, we should only carry out this attack by bounding ourselves in the ethical and legal realm.

Proposed Countermeasures for Security

Doing something like blocking unused ports, deploying new hardware and software, keeping software up to date and so on can mitigate DDoS attacks. But here, in a more detailed way, countermeasures to stop DDoS attacks are provided, which can be seen below:

Spoofed Packets Filtering

For hiding, the origin of the attack perpetrators relies on IP address spoofing. But with the help of mechanisms like spoofed packets filtering, it will be easy to drop packets with false IP addresses before reaching the target and stop DDoS attacks from happening.

Ingress/Egress Filtering

With the help of Ingress/Egress filtering, only IP addresses within the listed range can enter the network. When traffic comes into a network, it is handled by ingress filtering, whereas when traffic leaves the network, it is dealt with by egress filtering. So, it is a filtering one's network must-have. (Albiz, 2011)

Monitoring

There are many solutions, such as Comodo cWatch, Loggly etc., to monitor the web traffic and provide detailed analysis and statistics in real-time to the admin. This type of solution monitors and sends quick solutions to mitigate the ongoing risk in the network, troubleshoot, generate errors with possible solutions, and send it to the admin.

Black Holing

ISPs can use an anti-spam technique like blackholing to block upcoming network traffic so that the traffic won't reach the destination. More specifically, RTBH (remotely triggered blackholing) should be used to ask their upcoming network to block. (Chakraborty, 2019)

Scrubbing

DDoS scrubbing center is where ISP’s can send malicious traffic for cleansing and analysis purposes to find vulnerabilities. After this is done, the traffic is routed back to the host network.

Conclusion

DDoS attacks are becoming more complex day-by-day due to which it is becoming one of the significant security threats for businesses and ISP's. They are now in a dilemma to prevent and provide countermeasures to DDoS attacks. Attackers are finding new ways to exploit businesses' network infrastructure vulnerabilities by creating botnets and bypassing their authentication. DDoS attacks are also becoming the new choice for attackers to use as a smokescreen to carry out other attacks. Businesses are suffering from financial losses and losing their reputation. It has indeed become difficult to classify between normal and malicious traffic.

There are solutions too to mitigate DDoS-related attacks. There are laws such as Computer Fraud and Abuse Act, ETA etc., to protect individuals and businesses from DDoS attacks. It is impossible to eradicate DDoS attacks from the face of the earth. Still, there are countermeasures such as: blocking unused ports, deploying new hardware and software, keeping software up to date, packet filtering, log analysis applications deployment, blackholing and so on to minimize the risks embraced by DDoS attacks.

References

Abliz, M. (2011). Internet denial of service attacks and defense mechanisms [Review of *Internet denial of service attacks and defense mechanisms*]. *Department of Computer Science, University of Pittsburgh*, *3*, 1–50. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=S3iaj3kAAAAJ&citation_for_view=S3iaj3kAAAAJ:u-x6o8ySG0sC

(PDF) An Introduction to DDoS Attacks and Defense Mechanisms: An Analyst's Handbook. (n.d.). ResearchGate. Retrieved February 16, 2022, from https://www.researchgate.net/publication/216573214_An_Introduction_to_DDoS_Attacks_and_Defense_Mechanisms_An_Analyst

Chakraborty, S., Kumar, P., & Sinha, B. (2019). A STUDY ON DDOS ATTACKS, DANGER AND ITS PREVENTION [Review of *A STUDY ON DDOS ATTACKS, DANGER AND ITS PREVENTION*]. *ResearchGate*, 1–15. https://doi.org/10.1729/Journal.20847

Computer Fraud and Abuse Act (CFAA) | Practical Law. (n.d.). Content.next.westlaw.com. https://content.next.westlaw.com/Document/I210618b5ef0811e28578f7ccc38dcbee/View/FullText.html?originationContext=document&transitionType=DocumentItem&ppcid=5251ba51a0ad4300addd0ce209332a3a&contextData=(sc.Default)&firstPage=true

DDoS attacks by attacked country worldwide 2021. (n.d.). Statista. Retrieved February 16, 2022, from https://www.statista.com/statistics/1255583/ddos-attacks-by-attacked-country/

Mahajan, D., & Sachdeva, M. (2013). DDoS Attack Prevention and Mitigation Techniques - A Review. *International Journal of Computer Applications*, *67*(19), 21–24. https://doi.org/10.5120/11504-7221

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12), 155014771774146. https://doi.org/10.1177/1550147717741463

Paudel, N. (n.d.). cyber law. *Www.academia.edu*. Retrieved February 16, 2022, from https://www.academia.edu/5497117/cyber_law

Petters, J. (2020, March 29). *What is a DDoS Attack? Identifying Denial-of-Service Attacks* [Review of *What is a DDoS Attack? Identifying Denial-of-Service Attacks*]. Varonis; Inside Out Security Blog. https://www.varonis.com/blog/what-is-a-ddos-attack

Warburton, D. (2021, May 7). *DDoS Attack Trends for 2020*. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020

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