Detection of Distributed Denial of Service Attack via Machine Learning

Mudit Rathore
ICM 2015 502

What are Cyber Attacks ?

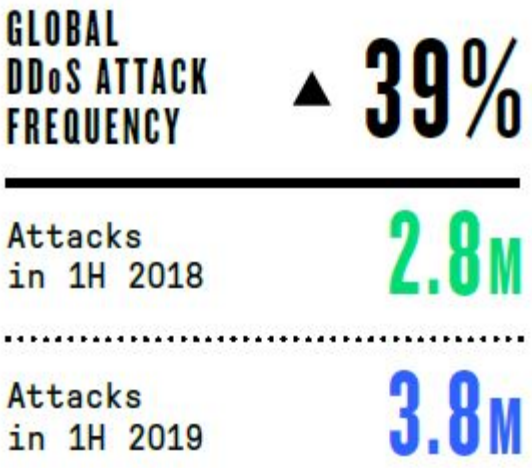
- Cyberattacks use malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes.
- For the scope of our study, we will be focusing on a specific type of cyber attack called Denial of Service attacks (DoS).
- DDoS Attacks are a specific type of DoS attack where the attacker coordinates the use of hundreds or thousands of devices across the internet for the attack.

What is DDoS ?

- DDoS stands for Distributed Denial of Service.
- It is a type of cyberattack that tries to make a website or network resource unavailable by taking advantage of the specific capacity limits that apply to any network resource.
- The attack can orginate from multiple sources which makes filtering of the attack traffic extremely difficult.
- Almost any type of internet-facing connected device could be a potential DDoS attack source: Internet of Things (IoT) devices, smartphones, personal computers, and powerful servers.

Why DDoS ?

- The goal of this attack is to decline the availability of services to legitimate users.
- The targeted services may include general services like DNS, HTTP, and FTP or specific services by organizations.
- DDoS attacks have become more powerful and more sophisticated over time.



Problem Background

Center for Strategic and International Studies (CSIS), in partnership with McAfee, published a global report discussing the impact of cybercrime on economies worldwide.

It concludes that close to $600 billion, i.e. nearly one percent of global GDP, is lost to cybercrime each year, which is up from a 2014 study that put global losses at about $445 billion.

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

NETSCOUT Threat Intelligence

Top Verticals Targeted by DDoS Attacks

1H 2018

RANK	VERTICAL	ATTACKS FREQUENCY	MAX ATTACK	CLASSIFICATION
1	Wired Telecommunications Carriers	793,778	1.7 Tbps	Information
2	Telecommunications	491,314	302.0 Gbps	Information
3	Data Processing, Hosting + Related Services	316,395	316.9 Gbps	Information
4	Wireless Telecommunications Carriers	157,388	327.5 Gbps	Information
5	Software Publishers	44,724	170.6 Gbps	Information
6	International Affairs	40,711	34.3 Gbps	Public Administration
7	Electronic Shopping + Mail-Order Houses	39,493	170.6 Gbps	Retail Trade
8	Other Telecommunications	39,004	600.0 Gbps	Information
9	Custom Computer Programming Services	31,837	170.6 Gbps	Professional, Scientific + Technical Services
10	Educational Services	27,164	96.8 Gbps	Educational Services

1H 2019

RANK	VERTICAL	ATTACK FREQUENCY	MAX ATTACK	CLASSIFICATION	
1	Wired Telecommunications Carriers	1,048,579	472.9 Gbps	Information	– 0
2	Telecommunications	591,033	634.3 Gbps	Information	– 0
3	Wireless Telecommunications Carriers	460,682	301.8 Gbps	Information	▲ 1
4	Data Processing, Hosting + Related Services	312,377	330.4 Gbps	Information	▼ 1
5	Custom Computer Programming Services	34,139	146.4 Gbps	Professional, Scientific + Technical Services	▲ 4
6	Satellite Telecommunications	30,563	54.1 Gbps	Professional, Scientific + Technical Services	NEW
7	Educational Services	24,564	68.3 Gbps	Educational Services	▲ 3
8	Professional, Scientific + Technical Services	22,098	71.6 Gbps	Professional, Scientific + Technical Services	NEW
9	Colleges, Universities + Professional Schools	20,188	176.4 Gbps	Educational Services	NEW
10	Software Publishers	13,368	78.8 Gbps	Professional, Scientific + Technical Services	▼ 5

DDoS attacks

- The largest DDoS attack that has observed and mitigated by prolexic, one of the leading companies in the DDoS attack detection and mitigation was peaked at 1.3 Tbps.

- There were nearly four million DDoS attacks around the world in the last six months.

- Almost any type of internet-facing connected device could be a potential DDoS resource: Internet of Things (IoT) devices, smartphones, personal computers, and powerful servers, and on average, 7.7 million IoT devices are connected to the internet every day around the globe.

Research Objectives

- Our objective is to develop a machine learning based distributed denial of service detection system.
- We will be developing a detection system using Ensemble Learning based on base learners and meta learners.
- Principal Component Analysis, Neural networks, and Random Forest Classifiers are good contenders for a base learner in our ensemble model.
- We will be using CIC-IDS-2017 dataset. CICIDS2017 dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data.

Challenges

- Detection of DDoS attack is a very challenging task because of the nature of a DDoS attack, it is very hard to mitigate as it penetrates right through the open ports on the firewall.
- Attributes such as source IP address, destination IP address, and packet rate are generally very good measures of detecting a DDoS attack, but, these attacks are often sourced from virtual machines in the cloud, rather than from the attacker's own machine, to achieve anonymity and higher network bandwidth; thus traceability and identification becomes very difficult.

Challenges

- Encryption of network data packets are also major challenges in this field as the defense can only access the metadata of the packet i.e., the information provided in the header and not the information provided as the content of the data packets.
- The wide variety of network protocols means difference in the header profile and the information carried by packets, it becomes quite difficult to design a system to monitor all these packets with their different feature vectors and information analysis requirements.
- This is especially critical because a DDoS attack does not necessarily have a single type of packet.

Expected Outcomes

The primary outcome of this study is to be able to classify incoming network traffic packets into legitimate and DDoS attack packets .

The secondary outcome of the study is to be able to identify the nature of DDoS attack, categorization of the network packets and, building a detection system which can identify a wide variety of attack packets from the incoming network traffic.

Thank You !!