INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN : 0975-4520

CaseStudy On DDoS Attacks And Attack TrendsIn Cloud Computing Environments

K.Aparna[1],G.Roopesh Kumar[2],S.Ishar[3],N.Santhosh[4],D.Sreeja[5]

[1-5]JNTUA-CEK university, Andhra Pradesh.

[1]aparna.ece@jntua.ac.in,[2]gandlaroopesh@gmail.com, [3]isharsheik33863@gmail.com,
[4]santhoshnayakanti31@gmail.com,[5]dasarisreeja165@gmail.com

Abstract*—Case studies are primarily used for exploratory based investigations that helps in understanding and explaining phenomenon or construct a theory. These are also used in the validation of Research results. Case studies also demonstrate the capabilities of a new technique,method,tool,process or technology.DDOS attacks causes major threat to cloud security.For these attacks, the Attackers usually create an army of infected computers called 'BotNet' by using the loopholes present in Network protocols used by various organisations for cloud computing. The main objective of this paper is to discuss about various DDoS attacks that occurred recently in the form of case studies.Additionally,this paper also provides insight into details such as by whom this attack started,how many days it lasted and losses that occurred to various companies due to these attacks.

Keywords : DDoS attacks, Cloud security, BotNet, Cloud computing.

I. INTRODUCTION:

Recently there is an escalation in number of security related incidents reported all over the world. The above scenario is also related to the fact that there is an increasing number of mobile devices users as well. Now-a-days cloud computing environment is rapidly growing and trending technology, that implements ubiquitous, effortless access, on-demand network access to joint collection of configurable computing resources and requires less effort to attain maintainability [1].The novel architecture of cloud computing a lot of traditional issueshavebeen effectively countered but its infrastructure and resources sharing has introduced the number of distinctivechallenges. Cloud computing security includes the number of issues primarily in network and access control data, cloud infrastructure and it's not easy to enforce all security measures because of different security demands of different users [2].

Cloud Computing offers ubiquitous, conducive, on demand access to a joint association of customizable computing resources like data-storage systems, network-profiles, oriental-services, high functionality servers and application development field which can be immediately managed, discharged along minimum administration exertion or service provider's cooperation. Cloud technology has four types of deployment-models: Public-cloud, its foundation is contracted to be utilized by the general public and handled by a governmental , intellectual or private company. Private-cloud, its set-up is for an institution that have many users. This type of cloud-model is managed by the institution utilizing its features or by a third-party. Community-cloud, which is mainly built-up for use for many individuals having similar objectives. It is handled by any organization present in that group or by a particular 3rd party. Hybrid-cloud, the foundation of this model structure comprises of different cloud deployment models i.e., private, public, or community model, which assure the mobility of operations and storage functions via a regular technology. This cloud model is highly customizable according to the requirements to be deployed [3].

TheseCloud computing services are often delivered by HTTP protocol giving access and reducing cost at the same time, but these services are vulnerable to HTTP DDoS attacks. DDoS attacks are intentionally performed by the malicious user to disrupt and degrade the service and resources of the legitimate user. In this type of attack, several negotiated computers are used for sole purpose of targeting network resources and servers leading to flooding of messages, malformed packets and connection requests resulting in the denial of service to the legitimate user. DDoS attacks on the cloud are highly sophisticated and request methods are created to find vulnerabilities and perform flooding attacks. The DDoS attacks are classified on the basis of network protocol and application.

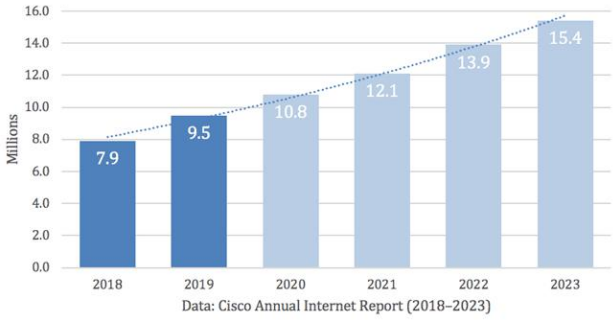
The network or transport level attacks are launched using the UDP, ICMP and TCP protocols. The HTTP DDoS attacks are performed on high and low rates scenarios each of them having a significant impact on the victim. The high rate attack floods the victim with a large number of requests while in the low rate scenario the victim is compromised by slow and

ISSN : 0975-4520

compromised requests which results in the exhaustion of resources [4].

II. RELATED WORK:

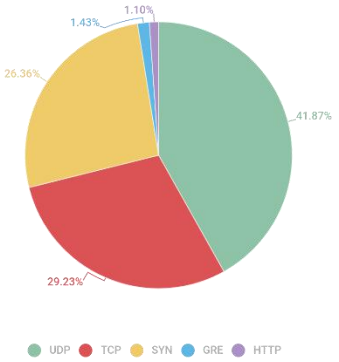
The first known Distributed Denial of Service attack occurred in 1996 when Panix, now one among the oldest internet service providers, was knocked offline for several days by a SYN flood, a way that has become a classic DDoS attack. Over subsequent few years DDoS attacks became common and Cisco predicts that the entire number of DDoS attacks will double from the 7.9 million seen in 2018 to something over 15 million by 2023.\But it's not just the amount of DDoS attacks that are increasing. The bad guys are creating ever bigger botnets – the armies of hacked devices that are wont to generate DDoS traffic. As the botnets get bigger, the size of DDoS attacks is additionally increasing. A Distributed Denial of Service attack of 1 gigabit per second is enough to knock most organizations off the web but we're now seeing peak attack sizes in excess of one terabit per second generated by many thousands or maybe many suborned devices. For more background about what's technically involved during a Distributed Denial of Service attack, see our post what's a DDoS Attacks.



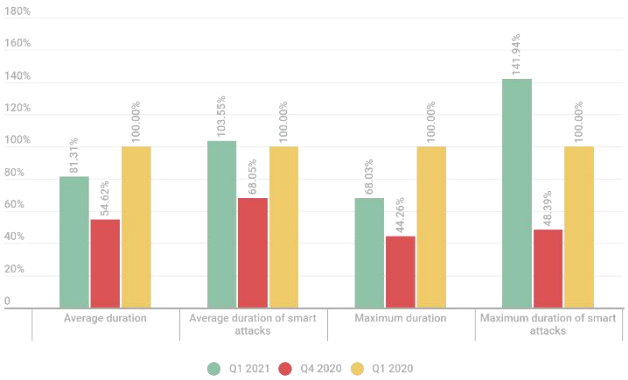
1. The Top Cyber Attack Statistics:

TYPES OF DDoS ATTACKS IN Q1 OF 2021:

In Q1 2021, the seemingly unassailable leader, SYN flooding (26.36%), lost its grip on the ranking. This DDoS type shed 51.92 p.p. and finished third. Meanwhile, UDP (41.87%) and TCP flooding (29.23%) gained in popularity among attackers. GRE (1.43%) and HTTP flooding (1.10%), which round out the ranking, also posted modest growth. [5]



we noted a downward trend in the duration of short attacks and an upward one in the duration of long attacks. This trend continued this quarter as well, which is clearly seen from the duration data compared to Q4 of the previous year



Attack geography

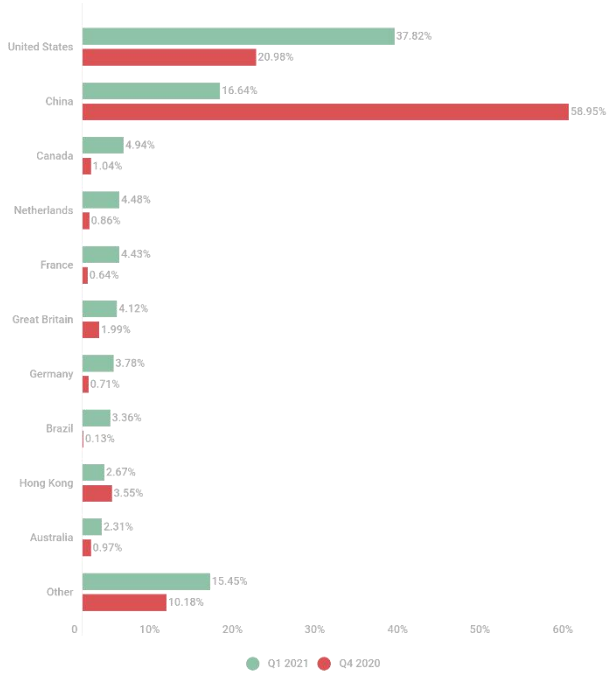
In Q1 2021, the perennial leaders by number of DDoS attacks swapped places: the US (37.82%) added 16.84 p.p. to top the leaderboard, nudging aside China (16.64%), which lost 42.31 p.p. against the previous reporting period. The Hong Kong Special Administrative Region (2.67%), which had long occupied third position, this time dropped to ninth, with Canada (4.94%) moving into the Top 3.

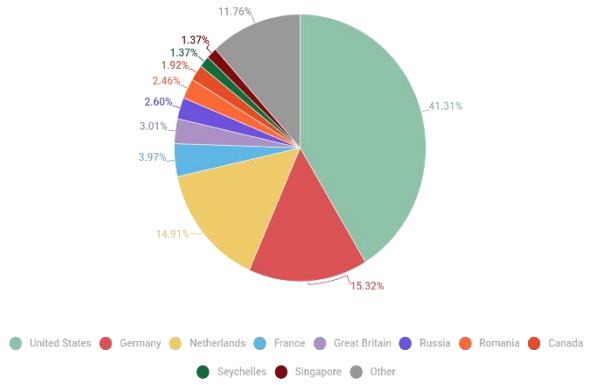
The UK (4.12%) also lost ground, falling from fourth to sixth place, despite its share increasing by 2.13 p.p., behind the Netherlands (4.48%) and France (4.43%). South Africa, which had fifth place last quarter, dropped out of the Top 10.

Germany (3.78%) moved up to seventh place, displacing Australia (2.31%), which rounds out the ranking this quarter. Eighth place was taken by Brazil (3.36%), having rarely climbed higher than eleventh before.

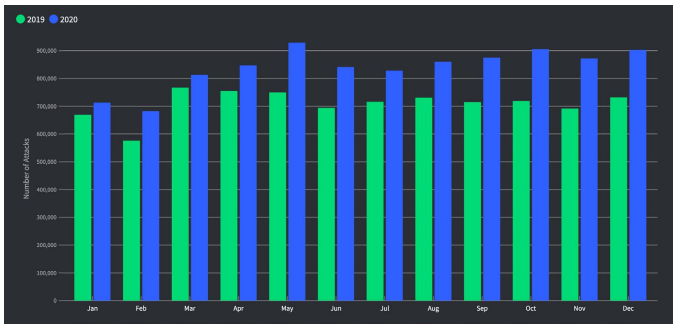
INTERNATIONAL JOURNAL OF TECHO-ENGINEERING

ISSN : 0975-4520





Monthly DDoS attacks frequency 2020[7]



The blight of cyber attacks, data breaches, phishing attacks and more appeared to make headlines almost a day in and virtually nobody was safe. Businessmen, governments, schools, and healthcare organizations have experienced the wrath of these hackers through malware and ransomware attacks, and their attacks cost billions globally. In fact, dozens of cities within the U.S., South Africa , and other locations round the world have found themselves the targets of such attacks within the last year.

Here are a number of the highest cyber attack statistics of 2019:

- **$26 Billion Lost to BEC/EAC Scams**

The FBI's IC3 estimates that quite $26 billion dollars was lost between June 2016 and July 2019 thanks to business email compromise/email account compromise scams.

- **Nearly 1 Billion Web-Based Cyber Attacks Repelled**

Kaspersky reports that 975,491,360 browser-based attacks from round the world were halted by their products. This same data also indicates that 273,782,113 unique URLs were discovered to be malicious URLS.

- **quite $675 Million Stolen by North Korean Nation-State Actors**

In March 2019, the UN Security Council reported quite $678 million in foreign currency and cryptocurrency theft by North Korea between 2015 and 2018. These nation-state actors attempted to steal $1 billion via state-sponsored hacking of companies and cryptocurrency exchanges from companies around the world.

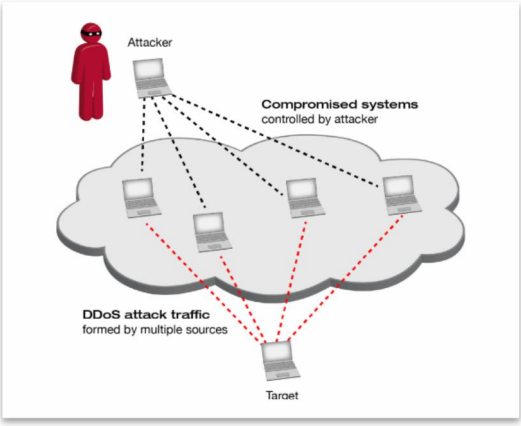
ISSN : 0975-4520

- **400% Increase in Threats to Mac Devices**

In its 2020 State of Malware Report, Malwarebytes reports that the amount of threats against Mac devices increased by 40% from 2018 to 2019. They report a mean of 11 threats per Mac device, which is almost double the 5.8 threat average on Windows endpoint devices.

A. Attack Generation:

In a secure Environment using Tor Hammer tool, the DDoS attack was generated. Kali 2018.2 OS with kernel 4.15.0,GNOME 3.28.0 are present in the attacking machine During the process of execution of DDoS attack, traffic is generated at sink node for the specified program and also Rachael, traffic protocol analyser records both suspicious and normal traffic during this process. This recorded traffic was then given to the server.



B. Attack detection and Data set Collection :

An input files were given to Intrusion Detection System SNORT, which were taken from server. It is used to detect all those attacks but to identify the DDoS attacks the default rules were changed. By defining the required topless, the output from the SNORT were directed.

III. THE ATTACKER'S INCENTIVE

DDoS attackers are usually motivated by various justifications. Analysing the attacker's incentives helped in responding to these attacks [32].

- Economical/Financial gain: A major part of attacks are generally performed by frustrated people, possibly with lower technical skills.
- Intellectual Challenge: The attackers are usually young hacking enthusiasts wanting to show off their capabilities to experiment and launching various attacks.
- Cyber warfare:The Attackers are usually motivated to attack a wide range of critical sections of other countries.
- Ideological belief: Attackers in this category are motivated because of their ideological beliefs to attack their targets and political incentives have led to recent sabotages.

IV. ANALYSIS:

DDoS Attacks Are Forecasted to get Double by 2022

We'll likely need to wait some time to see a slowdown in global DDoS attack numbers. Globally, the total number of DDoS attacks is expected to reach double to 15.4 million by 2023, according to the Cisco Visual Networking Index (VNI).

DDoS Protection & Mitigation Market will Get twice market by 2024

The remarkable upsurge in DDoS attacks is expected to coincide Without a surprise, rise in the DDoS protection and mitigation market. Another research firm estimated that the DDoS protection and mitigation market to get double market to$4.7 billion by 2024, showing a compound annual growth rate (CAGR) of 14%.

V.CASE STUDY

February 28th DDoS Incident Report on GitHub

BACKGROUND

Cloudflare named an amplification vector using memcached over UDP in their blog post in the week , "Memcrashed–Major amplification attacks from UDP port 11211". The attack works by targeting memcached instances that are inadvertently accessible on the overall public internet with UDP support enabled. Spoofing of IP addresses allows

memcached's responses to be targeted against another address, like ones won't to serve GitHub.com, and send more data toward the target than must be sent by the unspoofed source. The vulnerability caused because of misconfiguration described within the post is somewhat unique amongst that class of attacks because the amplification factor is up to 51,000, meaning that for each byte sent by the attacker, up to 51KB is shipped toward the target.

Over the past year GitHub deployed additional transit to their facilities. They've quite doubled their transit capacity during thatpoint , which has allowed them to face up to certain volumetric attacks without impact to users. They are continuing to deploy additional transit capacity and develop robust peering relationships across a various set of exchanges. Even still, attacks like this sometimes require the assistance of partners with larger transit networks to supply blocking and filtering.

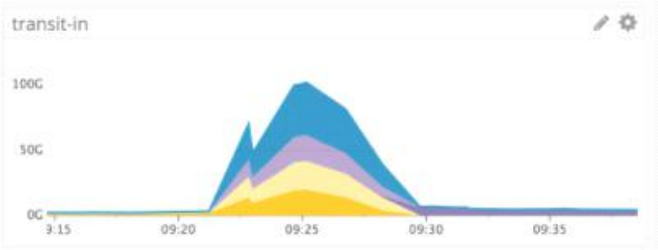
THE INCIDENT

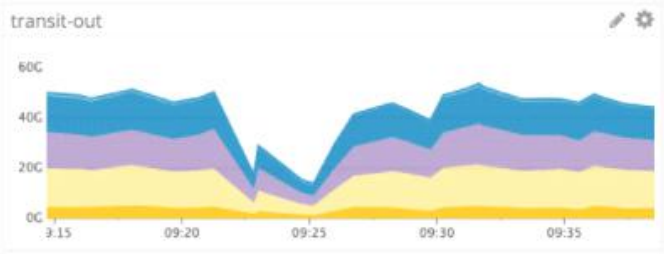
ISSN : 0975-4520

Between 17:21 and 17:30 UTC on February 28th GitHub identified and mitigated an enormous volumetric DDoS attack. Theattack arised from over thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints.

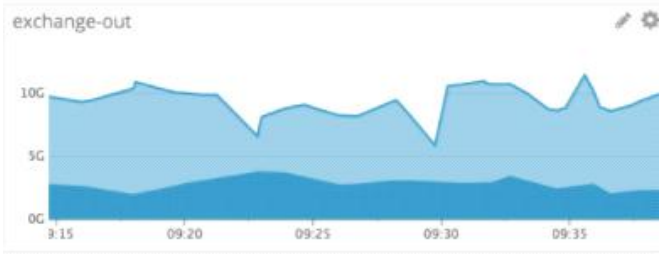
It was an amplification attack by using the memcachedbased approach described above that peaked at 1.35Tbps via126.9 million packets per second.

At 17:21 UTC GitHub's network monitoring system detected an anomaly within the ratio of ingress to egress traffic andnotified the oncall engineer et al. in their chat system. The graph shows both inbound versus outbound throughput overtransit links:

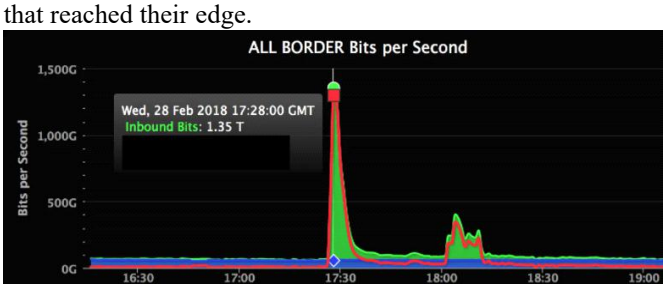




Given the rise in inbound transit bandwidth to over 100Gbps in one among their facilities, the choice was made tomaneuver traffic to Akamai, who could help provide additional edge network capacity. At 17:26 UTC the command wasinitiated with theirChatOps tooling to withdraw BGP announcements over transit providers and announce AS36459exclusively over their links to Akamai. Routes reconverged within the next jiffy and access control lists mitigated theattack at their border. Monitoring of transit bandwidth levels and cargo balancer response codes indicated a fullrecovery at 17:30 UTC. At 17:34 UTC routes to internet exchanges were withdrawn as a followup to shift a further 40Gbps faraway from our edge.



The first part of the attack peaked at 1.35Tbps and there was a second 400Gbps spike slightly after 18:00 UTC. The graph provided by Akamai shows inbound traffic in bits per second that reached their edge.



NEXT STEPS

Making GitHub's edge infrastructure more characterized tocurrent and future conditions of the internet and lessdependent upon human involvement requires better automated intervention. GitHub is investigating the use of their monitoring infrastructure to automate enabling DDoS mitigation providers and will continue to measure their responsetimes to incidents like this with a goal of reducing mean time to recovery (MTTR). They are going to continue to expand their edge network and endeavor to identify and mitigate new attack vectors before they affect peoples' workflow on GitHub.com. They know what proportion we believe GitHub for our projects and businesses to succeed. They will continue to analyze this and other events that effects their availability, build better detection systems, and streamline response.

VI .RESULT AND DISCUSSION:

- DDoS Attacks Are Forecasted to get Double by 2022

ISSN : 0975-4520

We'll likely need to wait some time to see a slowdown in global DDoS attack numbers. Globally, the total number of DDoS attacks is expected to reach double to 15.4 million by 2023, according to the Cisco Visual Networking Index (VNI).[6]

- DDoS Protection & Mitigation Market will Get twice market by 2024

The remarkable upsurge in DDoS attacks is expected to coincide Without a surprise, rise in the DDoS protection and mitigation market. Another research firm estimated that the DDoS protection and mitigation market to get double market to $4.7 billion by 2024, showing a compound annual growth rate (CAGR) of 14%[6].

VII .CONCLUSION:

In this paper, we discussed about the dangers of DDoS attacks and how the attack trends are happening in the real time. We also made a case study about the attack on github which shook the world. Given how malicious these attacks are the necessary measures must be taken in order to minimise the damage and to avoid future encounters.

ACKNOWLEDGMENT

The authors are grateful to the Faculty of JNTUACEKand our friends for their patronage and assistance throughout the formulating of this paper

REFERENCES

[1] P. Mell and T. Grance, "*The NIST Definition of Cloud Computing NIST Special Publication 800-145 (SP800-145)*," National Institute of Standards and Technology, Gaithersburg, September 2011

[2] Wani, Abdul Raoof, Q. P. Rana, and Nitin Pandey. "*Analysis and Countermeasures for Security and Privacy Issues in Cloud Computing*." System Performance and Management Analytics. Springer, Singapore, 2019. 47-54.

[3] Bohn, R & Messina, John & Liu, Fang & Tong, Jin& Mao, Jian. (2011). NIST Cloud Computing Reference Architecture. 594-596. 10.1109/SERVICES.2011.105**.**

[4] E.Cambiaso, G. Papaleo, and M. Aiello, "*Taxonomy of Slow DoSAttacks to Web Applications," in Recent Trends in Computer Networks and Distributed Systems Security*, vol. 335 of *Communications in Computer and Information Science,* pp. 195–204, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[5] DDoS attacks in Q1 2021 | Securelist

[6] https://securelist.com/ddos-attacks-in-q1-2021/102166

[7] https://www.netscout.com/sites/default/files/2021-04/ThreatReport_2H2020_FINAL_0

[8] https://sectigostore.com/blog/ddos-attack-statistics-a-look-at-the-most-recent-and-largest-ddos-attacks

[9] F. N. Hamdani and F. Siddiqui, "Detection of DDoS Attacks in Cloud Computing Environment," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), 2019, pp. 83-87, doi: 10.1109/ICCS45141.2019.9065429.

[10] M. Zekri, S. E. Kafhali, N. Aboutabit and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 2017, pp. 1-7, doi: 10.1109/CloudTech.2017.8284731.