**Part B**

**A GitHub leading software development platform hit by a massive DDOS attack [2018]**


**Abstract**

The DDoS attack is intended to disrupt normal business function by overwhelming and amplify the internet traffic using fraudulent request which causes a denial of service to legitimate traffic. Feb 28, 2018, the largest and leading software development platform GitHub faced DDoS attack which Peaked at 1.35 Terabits per second and it is highest recorded traffic in terms of DDoS attack history, which made the GitHub service unavailable worldwide. unlike the other attacks which are design for the financial gain but DDoS attack does not bring any financial gain to an attacker, however, it gives the satisfaction to the attacker if business resource belongs to a competitor are become inoperative, the analysis of DDoS attack pattern done by referring journal article which aim to create the awareness among Policy Maker and IT professionals to combat against the threats and make the Business to Achieve the Highest Goal By providing High Availability model to business


**Introduction**

The DDoS attack mostly targeted to the centralized system or service and it is impossible to capture the origin of the attack as the attack are done by millions compromised botnet network which controlled by the attacker, hence it is a difficult task for the IT professional to distinguish between fraudulent request and legitimate traffic. Unless and until any serious, any major service disruption occurred

The GitHub is not the only platform that faced the DDoS attack there are Plenty of other services such as Dyn, Cloudflare respectively experienced major service outage in the year 2016 and 2014,

**Distributed Denial of Service (DDoS) attack**

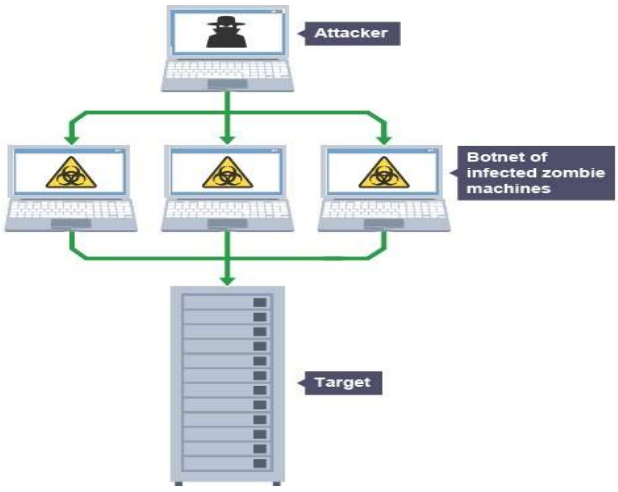



**Figure 1 DoS attack, taken From the BBC.co.uk**
(Denial of Service (DoS) attacks, n.d.)

According to the Scenario, Attacker Gather his Army of network computers by infecting multiple computers through malicious software or code which are known as zombie machines and once all machine becomes part of the common botnet network then attacker send the fraudulent request to the target server through zombie machine, hence the zombie machine innocently send the traffic to target server as it Directed by the attacker which block down the legitimate network request and make the service unavailable for the genuine user

**Most Common Type of Dos Attack**

Over the Last Decade, Plenty of DoS attack evolved and the number of attack vector mechanism discovered and implemented by the hacker

**According to Rapid7** Team. DoS attack Categorised as under (Team, n.d.)

1. *System-Targeted Denial-of-Service*
2. *Application-Targeted Denial-of-Service*
3. *Network-Targeted Denial-of-Service*

1 System-Targeted Denial-of-Service

The attacker asses the system resource such as CPU memory, disk space and afterwards they send SYN

flooding packet to the system which will make the congestion in the network hence the legitimate user can't make any new network connection so it will slow down the service delivery

2 Application Targeted Denial of service

The Application vulnerability can be exploited by the attacker to accomplish such type of attack, for Example, An Attacker bombarding on MySQL Central Database which has a vulnerability and made the service un-operational to the genuine user, and the same attack executed on GitHub application layer

3 *Network-Targeted Denial-of-Service*

In the Network DoS approach, attacker gather the power of millions of zombie machine and send the fake request to target system which will consume all the available bandwidth which will result to a service outage for the genuine user

**Symptoms and Impact of Denial of Service experienced GitHub**

GitHub experience recorded Highest traffic in History of DDoS and their symptoms are as under

1 slow performance and service continuity issue in terms of accessing web service

2 inability Detection and the reason for a network traffic spike

3 inconvenience to the end-user who is denied to access system resource due to outage

4 The user who continuously trying to access website and un-aware about that the site experience DDoS attack made the scenario worse and complicated

**Cost of Denial service to GitHub**

1 loss of income, however, most of the organization recover from attack up to a certain time frame which will reduce their financial loss

2 Un-ability serve to end-user leads to reputation loss in the market

3 organization lose the productive hour to normalize system function

**The methodology behind the GitHub Attack**

The wide variety of attack performed on the network layer But the GitHub was attacked by the Application layer vulnerability The assault actually leveraged what's known as a "Memcached server," which is linked with a data center (Rao, 2018)

As according to name, Memcached server designed to cached data so it can seamlessly provide repetitive access data without querying to the central database server so in the case same technology used by an attack to amplify the request up to 51000 times.so this exercise can be done when server spoof the IP address of the actual website, then the server sends the floods traffic to the victim which overwhelm traffic and take service offline

Radware's Threat Detection Network signalled an increase in activity on UDP port 11211. At the same time, several organizations began alerting to the trend of attackers abusing Memcached servers for amplified attacks. A Memcached amplified DDoS attack makes use of legitimate third party Memcached servers to send spoofed attack traffic to a targeted victim. Memcached, like other UDP based services (SSDP, DNS and NTP), are Internet servers that do not have native authentication and are therefore hijacked to launch amplified attacks against their victims. (Memcached DDoS Attacks, 2018)

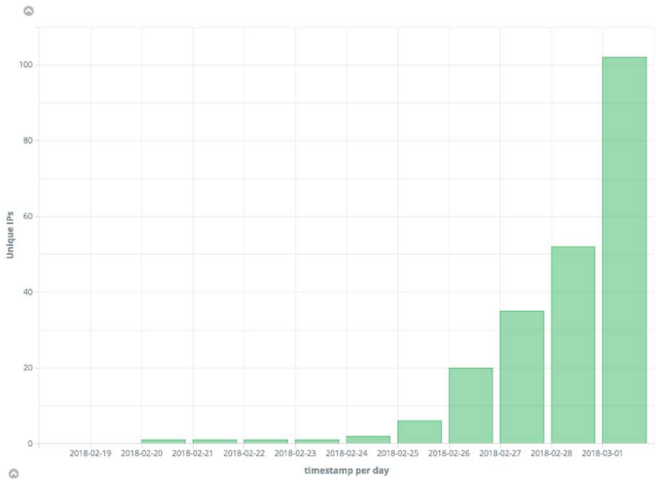



**Figure 2: Threat detection network: UDP port 11211**

A spoofed attack uses IP packets with illegitimate source IP addresses for the purpose of hiding the attackers' true source IP. More ominously, by changing the source IP address of a packet, the targeted machine will send its reply packet to the false IP header address using the reply itself as a secondary attack. Those wishing to launch a DDoS attack without a large number of botnets can, therefore, send packets with random spoofed source

IP addresses to both conceal their own origin IP address and launch volumetric attacks.

Due to the volume that can be reached with a single amplification list, attackers do not need a massive IoT botnet to launch 1Tbps+ assaults as with Mirai. At the core of the Memcached problem is the number of exposed servers on the Internet. With just under 100,000 exposed Memcached servers, it creates a prime reflector for amplified DDoS attacks. On February 27, Memcached version 1.5.6 was released which noted that UDP port 11211 was exposed and fixed the issue by disabling the UDP protocol by default. The following day, before the update could be applied, attackers leveraged this new attack vector to launch the world's largest DDoS attacks.

Memcached is a general-purpose, distributed memory caching system typically used to speed up dynamic web applications by caching data and objects in RAM and reducing backend database or API round-trips. Memcached APIs provide a large hash table (key-value) distributed across multiple systems. Most deployments of Memcached are within trusted networks where clients without authentication connect to any server. Memcached can be compiled with optional SASL authentication support but was deployed with TCP/UDP port 11211 exposed to the Internet. As a result, attackers can abuse this service to launch large-scale amplified attacks. The Bandwidth Amplification Factor (BAF) in the Memcached DDoS attacks ranges between 10,000x and 52,000x, resulting in volumetric DDoS attacks that can easily reach well over 500Gbps. All the attacker has to do is scan the Internet for vulnerable Memcached servers to create an amplification list. Once the attacker has a Memcached amplification list they are able to craft a custom script to send spoofed requests to UDP port 11211 on the amplification list with the victim's spoofed IP address. The Memcached servers will respond to the request by sending an amplified request, vastly larger than the original request, to the victims IP address. The result is pipe saturation and service degradation.

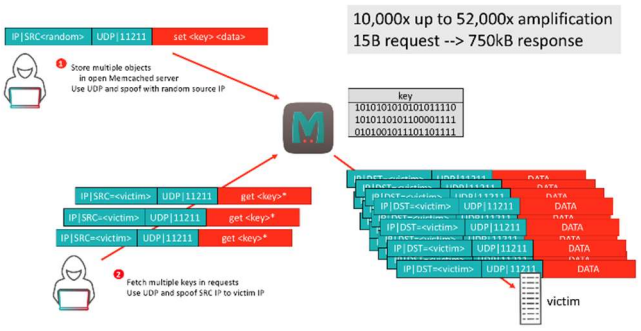



**Figure 3: Memcached DDoS Attack** (Memcached DDoS Attacks, 2018)

**Attack Formulation**

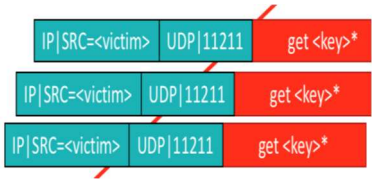
(Alam, 2018, pp. 10-28)

**1.Attacker scan the internet and find Memcached server which listening to UDP Port 11211 and Send Max Size Value Data**

**2.Run a memcache SET command and fills 1 key to it's max size with data to ensure high payload**

**3.Sends multiple forged GET requests for that key using continuous UDP and spoof victim IP**

**Vulnerable Memcached servers exposed at Internet and listening at UDP, Port: 11211**




Attacker's UDP Packets Contained:

- UDP GET key requests
- Size: 15B, SRC IP: spoof Target IP, DST Port:11211, Des. IP: MemcaheHost


**<Victims/Targets>**
**GET commands reflected to the victim IP with (key, value)**
**Value of DATA is high, i.e, T. Size=(key, value)*# of requests**
**GET Request 15B=> 750kB response, 50000x amplification (Akamai Report)**
SRC IP: Memcache host, DST IP: Target, SRC Port: 11211


(Alam, 2018, pp. 11-28)

**Figure 4: How Amplification Achieved Using Multiple Memcached Server**

How to Prepare

On the Memcached server-side, mitigation includes disabling UDP, updating to the latest code version (1.5.6 as of this writing) which disables UDP by default or enabling the optional SAML authentication.

On the client-side, Radware's Emergency Response Team confirms that Radware Defence Pro owners are fully protected from Memcached reflection attacks who use the configuration settings recommended in the table below, which includes Radware's Behavioural Analysis (BDoS) technology:

Effective DDoS Protection Essentials

- Hybrid DDoS Protection - On-premise and cloud DDoS protection for real-time DDoS attack prevention that also addresses high volume attacks and protects from pipe saturation
- Behavioural-Based Detection - Quickly and accurately identify and block anomalies while allowing legitimate traffic through
- Real-Time Signature Creation - Promptly protect from unknown threats and zero-day attacks
- A Cyber-Security Emergency Response Plan - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

For further network and application security and DDoS protection measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Effective Web Application Security Essentials

- Full OWASP Top-10 coverage against defacements, injections, etc.
- Low false positive rate – using negative and positive security models for maximum accuracy
- Auto policy generation capabilities for the widest coverage with the lowest operational effort
- Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- Flexible deployment options - on-premise, out-of-path, virtual or cloud-based

**CONCLUSION**

In the present study, it was analysed how DDoS attack Executed on GitHub what were Potential cause for its success and what are the defence mechanism available in order to prevent and minimize the Incident occurred by DDoS .It is essential that every establishment who holding the IT Infrastructure publicly must update their computers and networks with the latest patches given by the provider. And also prepare the Risk Management and Disaster Recovery plan to combat with future threat and attack, Firewall system must be implemented on central network as well endpoints network machine which can fight against fraudulent request generated by zombie machine.in case of any DDoS incident still happen on organization, they should have the redundancy for the system and networks so the can alter the users request to another resource and keep the business function high-available for the end user The DDoS hacking mechanism is getting More Complicated as it hide the identity of real attacker therefore it is necessary to implement the strongest preventive