Name: Ayush Patel Enrolment: 22162171038 Class B Batch 55

Report on AWS DDoS Attack

(February 2020)

Introduction:

In February 2020, Amazon Web Services (AWS) was the target of one of the largest Distributed Denial of Service (DDoS) attacks recorded to date. This attack reached a peak of 2.3 terabits per second (Tbps), demonstrating the growing scale and sophistication of DDoS threats. This report provides a detailed analysis of the attack, the targeted devices and services, the type of attack used, other potential attack vectors, prevention strategies, and a conclusion summarizing the key learnings.

Details of the Targeted Device:

Targeted Infrastructure:

AWS, a leading cloud services provider, offers a wide array of services including computing power, storage, and databases to millions of customers worldwide. The attack specifically targeted AWS's infrastructure, aiming to disrupt service availability and degrade the performance of the cloud-based applications hosted on their platform.

Key Services Affected:

While AWS successfully mitigated the attack without any reported impact on customer services, the primary targets included:

- **Elastic Compute Cloud (EC2):** A service providing resizable compute capacity.
- **Simple Storage Service (S3):** A scalable object storage service.
- **Route 53:** A scalable Domain Name System (DNS) web service.

These services are integral to AWS's cloud offerings and are critical for the operation of numerous applications and websites worldwide.

Name: Ayush Patel Enrolment: 22162171038 Class B Batch 55

Types of Attack

Primary Attack Vector: CLDAP Reflection:

The AWS DDoS attack employed a **CLDAP Reflection** technique, characterized by:

- **Amplification:** Attackers exploited the Connectionless Lightweight Directory Access Protocol (CLDAP) to amplify traffic. By sending requests with a spoofed source IP (belonging to the target), they received larger responses, overwhelming the target with amplified data.
- **Magnitude:** CLDAP can produce an amplification factor of 56-70 times the original request size, making it an effective vector for DDoS attacks.

Other Types of DDoS Attacks:

In addition to CLDAP reflection, several other types of DDoS attacks exist, including:

1. **UDP Flood:**
    - **Description:** Uses User Datagram Protocol (UDP) packets to flood the target.
    - **Effect:** Overwhelms the network with large volumes of packets, leading to resource exhaustion.
2. **SYN Flood:**
    - **Description:** Exploits the TCP handshake process by sending numerous SYN requests.
    - **Effect:** Consumes server resources, preventing legitimate connections.
3. **HTTP Flood:**
    - **Description:** Sends HTTP requests to overwhelm web servers.
    - **Effect:** Exhausts server processing power and memory, causing service disruption.
4. **DNS Amplification:**
    - **Description:** Similar to CLDAP, uses DNS servers to amplify traffic.
    - **Effect:** Generates massive volumes of data directed at the target.
5. **Ping of Death:**
    - **Description:** Sends malformed or oversized packets using the Internet Control Message Protocol (ICMP).
    - **Effect:** Crashes or destabilizes the target system.
6. **Botnet-based Attacks:**
    - **Description:** Utilizes a network of infected devices (botnet) to conduct coordinated attacks.
    - **Effect:** Generates overwhelming traffic, making mitigation difficult.

Name: Ayush Patel Enrolment: 22162171038 Class B Batch 55

How to Prevent and Mitigate DDoS Attacks:

Best Practices for Prevention

1. **Implement DDoS Protection Services:**
    - **Services like AWS Shield:** Offers automatic detection and mitigation against DDoS attacks.
    - **Third-Party Solutions:** Consider services like Cloudflare, Akamai, or Arbor Networks for additional protection.
2. **Rate Limiting and Throttling:**
    - **Traffic Control:** Implement rate limiting to manage incoming traffic and prevent overload.
    - **API Gateway:** Use tools that can restrict the number of requests to your APIs.
3. **Traffic Monitoring and Analysis:**
    - **Real-time Monitoring:** Deploy monitoring tools to identify abnormal traffic patterns.
    - **Anomaly Detection:** Use machine learning to detect and respond to unusual behavior.
4. **Network Security Measures:**
    - **Firewalls and Intrusion Detection Systems (IDS):** Use firewalls and IDS to block malicious traffic.
    - **Geo-blocking:** Restrict access from regions with high levels of malicious activity.
5. **Redundancy and Load Balancing:**
    - **Load Balancers:** Distribute traffic across multiple servers to prevent overload.
    - **Failover Systems:** Implement failover systems to maintain service availability during attacks.

Mitigation Strategies:

1. **Blackhole Routing:**
    - **Description:** Redirects traffic to a null route, dropping malicious traffic.
    - **Consideration:** Can impact legitimate traffic; use cautiously.
2. **Traffic Scrubbing:**
    - **Description:** Redirects traffic through a scrubbing center to filter out malicious packets.
    - **Benefit:** Allows only legitimate traffic to reach the target.
3. **Auto-Scaling:**
    - **Description:** Automatically adds resources to handle increased traffic.
    - **Benefit:** Provides resilience against large-scale attacks.
4. **Engage ISPs and Partners:**
    - **Collaboration:** Work with Internet Service Providers (ISPs) and DDoS protection partners to improve defense mechanisms.
    - **Response Coordination:** Ensure coordinated responses to large-scale attacks.

Name: Ayush Patel Enrolment: 22162171038 Class B Batch 55

Conclusion and Summary:

Conclusion

The 2020 AWS DDoS attack highlights the increasing scale and sophistication of DDoS threats in today's digital landscape. The successful mitigation by AWS underscores the importance of robust security measures and proactive strategies to protect against such attacks. As cloud services continue to play a critical role in business operations, investing in comprehensive DDoS protection and staying informed about emerging threats is essential for maintaining service availability and security.

Summary

- **Target:** Amazon Web Services (AWS), with a peak traffic of 2.3 Tbps.
- **Primary Attack Vector:** CLDAP Reflection, leveraging amplification to overwhelm AWS infrastructure.
- **Key Strategies:** AWS successfully mitigated the attack using AWS Shield and its extensive security infrastructure.
- **Prevention Measures:** Implement DDoS protection, monitor traffic, use load balancing, and collaborate with ISPs.
- **Other Attack Types:** Include UDP Flood, SYN Flood, HTTP Flood, DNS Amplification, and Botnet-based attacks.