Task-7: Report on Recent DDoS Attack

Report on the Cloudflare 22.2 TBps DDoS Attack

1. Introduction

The DDoS attacks, that is to say Distributed Denial of Service, keep being one of the main dangers to the internet infrastructure all over the globe. On 14th of September 2025, Cloudflare managed to put an end to a DDoS attack that was going to 22.2 terabits per second (Tbps) and thus, breaking the records for the highest DDoS attack volume. The new DDoS attack sizes and complexities are going to be the benchmarks from now on. Moreover, these developments reveal that the attackers are becoming more proficient and the defenders have to step up their game to be able to cope.

2. Target

Main Target:

• The attack was aimed at a European network infrastructure company that used Cloudflare's security services.

• The name of the target company was not given for privacy and security reasons.

Nature of Target:

The company is in charge of the backbone of critical infrastructure that makes it possible for both businesses and possibly the public sector to work.

3. Technology Used in the Attack

Attack Vector:

They used UDP carpet bomb attack tactic that generally aims at sending a massive number of UDP packets to targeted networks. As a result, these networks are not only saturated with their bandwidth but they also run out of resources.

Sources and Size:

•There were over 404, 000 different IP addresses that participated in the attack and a great number of those were scattered across the globe.

•These IPs were distributed over 14 or more Autonomous System Numbers (ASNs), which suggests that the botnet was very widely distributed.

Botnet Infrastructure:

It was the AISURU botnet, basically the hijacked IoT devices like home routers, DVRs, and network cameras that contributed the most to this botnet, that was the source of the attack.

Features of the Attack:

•Peak Bandwidth: 22.2 terabits per second (Tbps)

•Peak Packet Rate: 10.6 billion packets per second (pps)

•Length: Around 40 seconds (brief, but very powerful)

•Amplification and Evasion: The perpetrators exploited amplification tactics and rapidly altered their traffic sources to attain the highest impact and stay undetected.

4. Attacker's Motive

Major Motive:

•AISURU botnet, as per the reports, is a DDoS, for, hire project. The team behind it profits from leasing the access to this botnet to the criminals or companies that want to bring down the businesses of their rivals by targeting them with DDoS attacks.

•Notoriety and Publicity: Demonstrating the power of the botnet is one of the ways to increase its value in the dark market, and thus bringing in more clients.

Involved Actors:

The security researchers managed to identify three personalities who were central to the operation of the AISURU botnet.

•Snow: The technical part, managing, as well as developing malware

•Tom: Conducting research in the area of exploitation and finding vulnerabilities

•Forky: The underground sales and business development

5. Total Impact

Service Disruption:

Basically, the convoluted automated mitigation systems utilized by Cloudflare resulted in the minimal negative effect on the services of the targeted firm due to the attack. Everything worked fine from the side of the end users as well as the customers, who were mostly unaffected.

Technical Significance:

•This stripe set a new world record for the size of the DDoS attack that exceeded the previous best 17.2 Tbps.

•The amount of data was equal to that required to stream one million, 4K resolution, videos simultaneously or update 1.3 web pages for every human being on the Earth per second.

Security Community Response:

The incident induced unease not only among the general public but also the community of cybersecurity professionals who saw IoT botnets as an increasing threat and the necessity for yet more countermeasures.

6. Defensive Strategies and Mitigation

Cloudflare's Response:

•Automated Mitigation: The Cloudflare distributed network and the software filters made in, house automatically got rid of the attack.

•Threat Detection: Anomaly detection was done in real, time; malicious packets were correctly identified out of normal traffic.

•Scrubbing and Filtering: At the multiple data centers where the traffic was scrubbed, the packets were dispersed and removed.

Recommended Defensive Steps for Organizations:

1. Cloud, Based DDoS Protection: Install a DDoS mitigation system that can operate on a global scale and is distributed worldwide.

2. Network Redundancy: Plan a failover or distribution process that can handle loads from more than one point to guarantee continuance of the infrastructure.

3. Traffic Rate Limiting: Impose limits and shape the network traffic at the periphery to avoid overload and the loss of packets.

4. Behavioral Analytics: Use AI, based monitoring systems that can recognize and signal abnormal increases in traffic.

5. Device Security: Internet, facing devices should always be up, to, date, have the latest patches, and be monitored closely to prevent botnet recruitment and compromising of the device.

6. Upstream ISP Partnership: Establish a close relationship with ISPs for the purposes of being provided with an early warning and setting up upstream filters to prevent an attack.

The 22.2 Tbps DDoS strike on September 14, 2025, is not only a warning but also an example of network security that works. While the bad guys are increasing the power of their operations and enhancing their strategies, this is a showcase of today's cutting, edge, automatic, globally, distributed security that can conquer even the noisiest of attacks with almost zero service impact. It takes constant effort in terms of alertness, technological creativity, and collaboration throughout the cybersecurity community to stay one step ahead of these burgeoning dangers.

8. References

Cloudflare Incident Response Blog (September 2025)

SecurityWeek: Largest Recorded DDoS Attack Defended (September 2025)

BleepingComputer: IoT Botnet Causes Historic DDoS (September 2025)

TechRadar: DDoS Attack Trends and Cloudflare's Defense (September 2025)

Primary research and industry news sources

Prepared for: *MuLearn Bootcamp*

Prepared By: *Atul H*