DENIAL OF SERVICE ATTACK ON GITHUB

Submitted By:

NAVEEN K

(23CSEH23)

M.Sc.Cyber Security(2024-2025)

Under the Guidance of

Dr.R.RAJESWARI, MCA., Ph.D.,
Professor,
Department of Computer Applications,
Bharathiar University

DEPARTMENT OF COMPUTERAPPLICATIONS
BHARATHIAR UNIVERSITY
COIMBATORE

DECEMBER-2024

DECLARATION

I hereby declare that this submitted Case Study to the Department of Computer Applications, Bharathiar University, is a record of original work done by **NAVEEN K (23CSEH23)** under the supervision and guidance of Dr. R. **RAJESWARI, MCA., Ph.D.**, Department of Computer Applications, Bharathiar University. I affirm that this Case Study has not been submitted for the award of any Degree/Diploma/Associateship/Fellowship or similar title to any candidate of any University.

Place : Coimbatore	Signature of the candidate
Date :	**NAVEEN K**

Countersigned by,

Dr.R.RAJESWARI, MCA., Ph.D.,
Professor,
Department of Computer Applications,
Bharathiar University

CERTIFICATE

This is to certify that the case study titled "**DENIAL OF SERVICE ATTACK ON GITHUB**", submitted to the Department of Computer Applications, Bharathiar University in partial fulfilment of the requirements for the award of the degree of Masters Of Science in Cyber Security, is a record of original work done by **NAVEEN K** (23CSEH23) under the supervision and guidance of **Dr.R.RAJESWARI, MCA., Ph.D.,** during the period of study in the Department of Computer Applications, Bharathiar University, Coimbatore and that this project work has not formed the basis for the award of any Degree/Diploma/Associateship/Fellowship or similar title to any candidate of any University.

Place: Coimbatore

Submitted for the Project VIVA-VOCE Examination held on ________________

Project Guide   Head of the Department

Internal Examiner   External Examiner

TABLE OF CONTENTS

ABSTRACT

In February 2018, GitHub, a leading platform for software development, was targeted by one of the largest Distributed Denial of Service (DDoS) attacks ever recorded, peaking at 1.35 terabits per second (Tbps). The attack utilized a Memcached amplification technique, exploiting misconfigured servers to flood GitHub’s systems with massive traffic, crippling its infrastructure.

Despite the unprecedented scale of the attack, GitHub's swift response, supported by Akamai Prolexic, allowed them to mitigate the attack within minutes, minimizing disruption to services and users. This case study explores the technical and operational aspects of the attack, examining the vulnerabilities in Memcached servers that were exploited and the defensive measures GitHub employed to restore service. It also looks at the broader implications of large-scale DDoS incidents, which pose risks to global internet infrastructure and can cause significant economic damage, including financial losses and reputational harm. The study highlights the growing threat of DDoS attacks, especially with the increasing use of Internet of Things (IoT) devices in botnets and emerging amplification techniques. By analyzing this incident, the case study offers insights into evolving cyber threats and recommends strategies for improving resilience against future attacks. These include securing vulnerable internet services, investing in DDoS protection, and fostering collaboration across industries for better threat intelligence sharing. As cyber threats grow more sophisticated, organizations must adopt proactive, layered cybersecurity approaches to defend against increasingly powerful DDoS attacks.

1. INTRODUCTION

A **Distributed Denial of Service (DDoS)** attack is a coordinated cyber assault where multiple compromised systems, often part of a botnet, flood a target server, service, or network with overwhelming traffic. Unlike a traditional Denial of Service (DoS) attack, which originates from a single source, DDoS attacks involve a distributed network of devices, making them significantly more challenging to detect and mitigate.

The goal of a DDoS attack is to exhaust the target's resources such as bandwidth, processing power, or memory thereby rendering it unable to respond to legitimate user requests. This disruption often results in financial losses, reputational damage, and operational challenges for the targeted organization.

Characteristics of DDOS Attacks

- **Distributed Nature:** DDoS attacks involve multiple compromised devices (botnets) spreading the attack traffic across various sources, making it harder to trace and block.
- **High Traffic Volume:** The attack generates massive volumes of traffic aimed at overwhelming the target's resources, such as bandwidth, memory, or CPU.
- **Layered Attacks:** DDoS attacks can target multiple layers of the OSI model, including the network layer, transport layer, and application layer, complicating defense strategies.
- **Evasion Techniques:** Attackers often use tactics like randomized IP addresses and slow traffic to avoid detection by traditional security defenses like firewalls or intrusion prevention systems.
- **Persistence and Adaptability:** DDoS attacks can be prolonged (ranging from minutes to days) and are adaptable, with attackers frequently evolving their methods to bypass defenses and increase attack efficacy.

2. TYPES OF DDOS ATTACKS

Volumetric Attacks

Goal: These attacks aim to overwhelm the target by consuming all the available bandwidth between the target and the internet.

Examples: UDP Flood, ICMP Flood, DNS Amplification.

Impact: The sheer volume of malicious traffic makes it difficult for legitimate users to access the target website or service, effectively rendering it unavailable.

Protocol Attacks

Goal: Protocol attacks exploit weaknesses in network protocols to exhaust server resources.

Examples: SYN Flood, Ping of Death, Smurf Attacks.

Impact: These attacks force the server to dedicate its resources to handling malicious requests, which can cause crashes or cause the server to become unresponsive to legitimate traffic.

Application Layer Attacks

Goal: These attacks target the application layer (Layer 7) by mimicking legitimate traffic, often aiming to overload web applications or APIs.

Examples: HTTP Flood, Slowloris.

Impact: These attacks are tricky to detect because the traffic looks like normal user requests. As a result, they can slow down or crash servers by exhausting resources without triggering obvious red flags.

Amplification Attacks

Goal: In amplification attacks, attackers exploit vulnerable servers to generate massive volumes of traffic directed at the target by sending small requests that elicit large responses.

Examples: Memcached Amplification, DNS Amplification.

Impact: These attacks can escalate quickly, magnifying the volume of traffic to terabits per second, creating massive disruptions and making it difficult for the target to defend.

3.IMPORTANCE OF DDOS ATTACKS AS A GLOBAL ISSUE

DDoS attacks have become a significant concern in today's interconnected world for several reasons:

Economic Impact

The downtime caused by DDoS attacks can severely affect businesses, particularly those in e-commerce, finance, and online services, leading to major revenue loss. Additionally, companies invest billions each year in mitigating these attacks, reflecting their growing scale and impact.

Threat to Critical Infrastructure

DDoS attacks can disrupt vital services, such as banking, healthcare, transportation, and energy systems. In some cases, nation-states have even used DDoS attacks as a part of cyber warfare tactics, intensifying the global threat.

Proliferation of IoT Devices

The rapid growth of Internet of Things (IoT) devices has expanded the scope of botnets, making DDoS attacks even more powerful. The Mirai botnet attack highlighted how poorly secured connected devices can be hijacked to amplify the scale of these attacks.

Challenges in Mitigation

Due to their distributed nature and the use of legitimate-looking traffic, DDoS attacks are notoriously hard to detect and block. Defending against them requires continuous updates to security strategies and significant investment in defense infrastructure.

Global Connectivity

Our increasingly digital world means that an attack on one organization can ripple through and affect users, businesses, and services worldwide, making DDoS a global problem that requires collaborative defense efforts.

4. BIGGEST DDOS ATTACK EVER RECORDED

This graph provided by Akamai shows inbound traffic in bits per second that reached their edge:

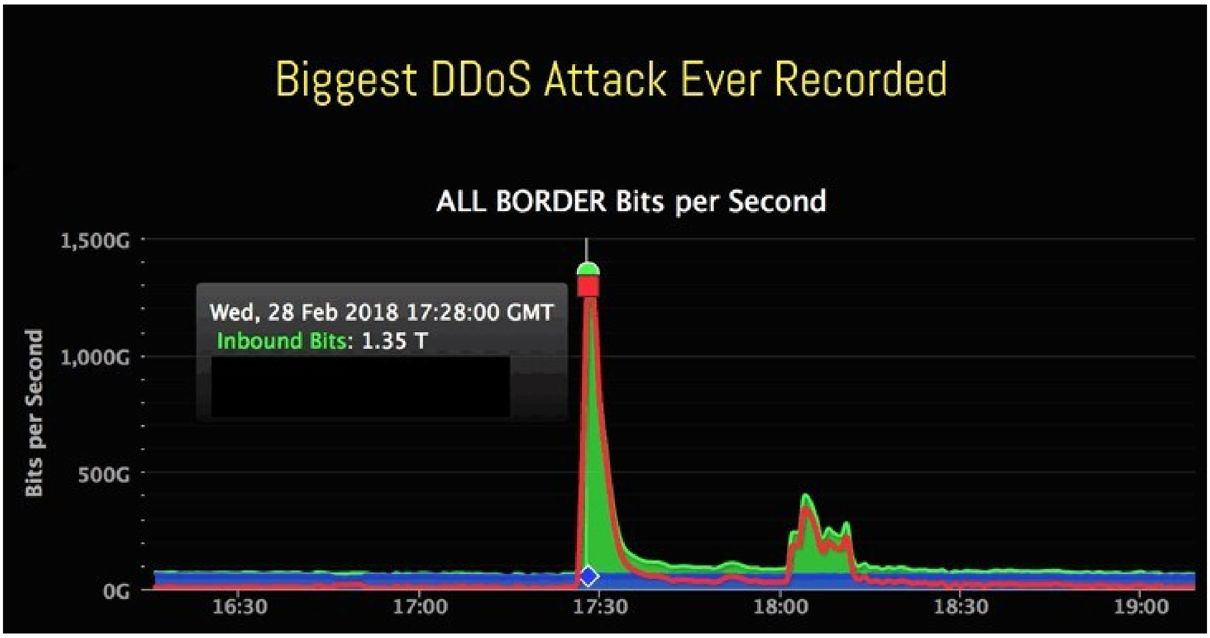


Figure 4.1 Biggest DDOS Attack Ever Recorded

On Wednesday, February 28, 2018 *GitHub.com* was unavailable from 17:21 to 17:26 UTC and intermittently unavailable from 17:26 to 17:30 UTC due to a distributed denial-of-service (DDoS) attack. We understand how much you rely on GitHub and we know the availability of our service is of critical importance to our users. To note, at no point was the confidentiality or integrity of your data at risk. We are sorry for the impact of this incident and would like to describe the event, the efforts we've taken to drive availability, and how we aim to improve response and mitigation moving forward.

The incident

Between 17:21 and 17:30 UTC on February 28th we identified and mitigated a significant volumetric DDoS attack.The attack originated from over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints. It was an amplification attack using the memcached-based approach described above that peaked at 1.35Tbps via 126.9 million packets per second. At 17:21 UTC our network monitoring system detected an anomaly in the ratio of ingress to egress traffic and notified the on-call engineer and others in our chat system. This graph shows inbound versus outbound throughput over transit links:

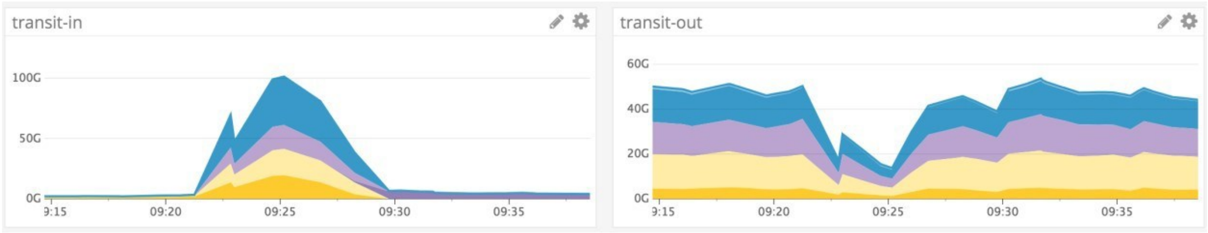


Figure 4.2 Inbound and Outbound Transit Bandwidth

Given the increase in inbound transit bandwidth to over 100Gbps in one of our facilities, the decision was made to move traffic to Akamai, who could help provide additional edge network capacity. At 17:26 UTC the command was initiated via our ChatOps tooling to withdraw BGP announcements over transit providers and announce AS36459 exclusively over our links to Akamai.

Routes reconverged in the next few minutes and access control lists mitigated the attack at their border. Monitoring of transit bandwidth levels and load balancer response codes indicated a full recovery at 17:30 UTC. At 17:34 UTC routes to internet exchanges were withdrawn as a follow-up to shift an additional 40Gbps away from our edge.

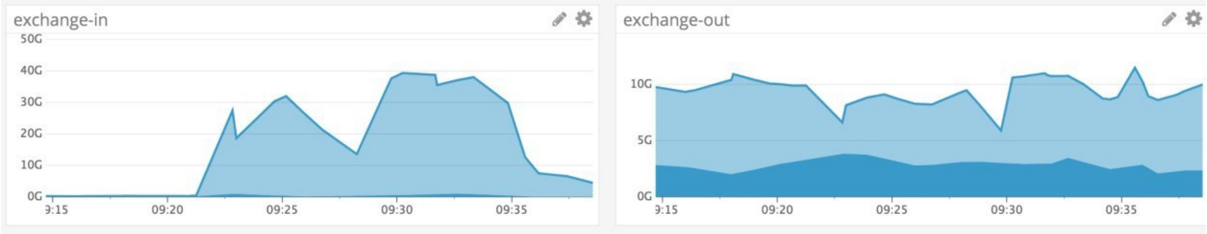


Figure 4.3 Attack Peaked Graph

The first portion of the attack peaked at 1.35Tbps and there was a second 400Gbps spike a little after 18:00 UTC.

5.MEMCACHED SERVER

Memcached Servers Abused for Massive Amplification DDoS Attacks

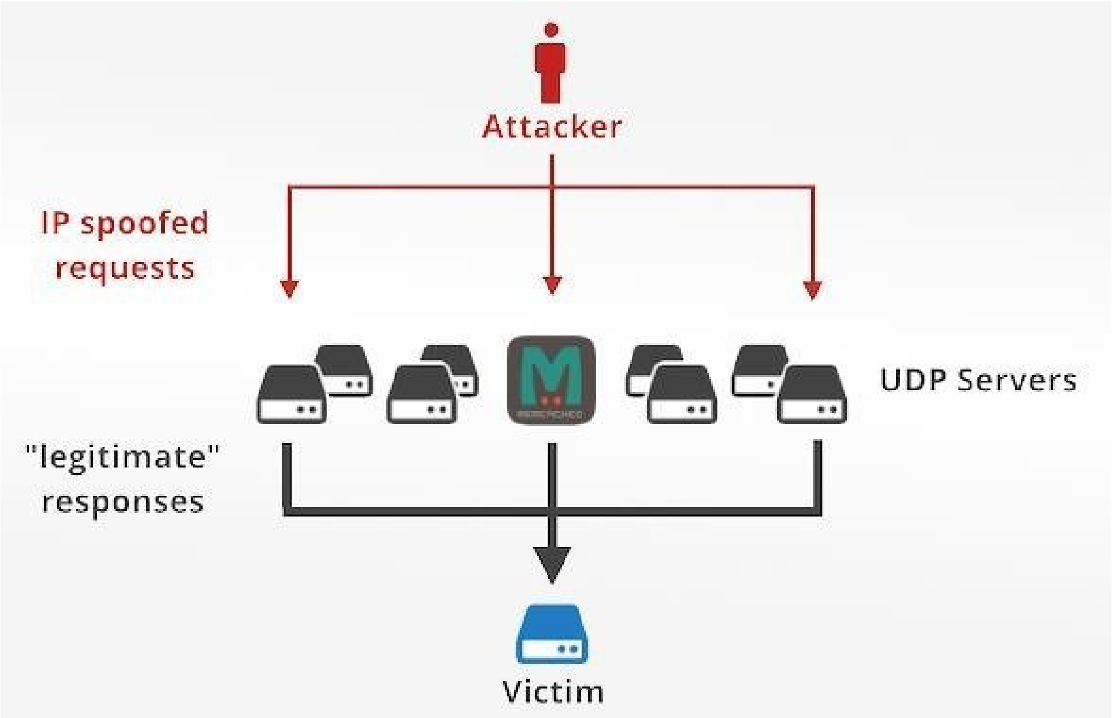


Figure 5.1 Memcached Server

Cybercriminals have figured out a way to abuse widely-used Memcached servers to launch over 51,000 times powerful DDoS attacks than their original strength, which could result in knocking down of major websites and Internet infrastructure.

Memcached is a popular open-source and easily deployable distributed caching system that allows objects to be stored in memory and has been designed to work with a large number of open connections. Memcached server runs over TCP or UDP port 11211.

The Memcached application has been designed to speed up dynamic web applications by reducing stress on the database that helps administrators to increase performance and scale web applications. It's widely used by thousands of websites, including Facebook, Flickr, Twitter, Reddit, YouTube, and Github.

Dubbed Memcrashed by Cloudflare, the attack apparently abuses unprotected Memcached servers that have UDP enabled in order to deliver DDoS attacks 51,200 times their original strength, making it the most prominent amplification method ever used in the wild so far.

In recent days, security researchers at Cloudflare, Arbor Networks, and Chinese security firm Qihoo 360 noticed that hackers are now abusing "Memcached" to amplify their DDoS attacks by an unprecedented factor of 51,200.

6. AMPLIFICATIONS ATTACKS

Figure 6.1 Amplification

The DDoS techniques have massively increased with the attackers becoming more skillful at working around the network security. A massive 300Gbps DDoS attack launched against Spamhaus website almost broke the Internet a year ago and also earlier this year, hackers have succeeded in reaching new heights of the massive DDoS attack targeting content-delivery and anti-DDoS protection firm CloudFlare, reaching more than 400Gbps at its peak of traffic.

Akamai's Prolexic Security Engineering and Response Team (PLXsert) issued a threat advisory on Thursday reporting a significant surge in DDoS attacks last month abusing the Simple Network Management Protocol (SNMP) interface in network devices.

Simple Network Management Protocol (SNMP) is a UDP-based protocol which is commonly known and often used to manage network devices. SNMP is typically used in devices such as printers, routers and firewalls that can be found in the home and enterprise environments as well.

Just as DNS amplification attacks, SNMP could also be used in Amplification attacks because a cyber criminal can send a small request from a spoofed IP address in order to sent a much larger response in return.

Over the past month, researchers have spotted 14 Distributed Denial-of-Service (DDoS) attack campaigns that have made use of SNMP amplified reflection attacks. The attacks targeted a number of different industries including consumer products, gaming, hosting, non-profits and software-as-a-service, mainly in the United States (49%) and China (18.49%).

The Distributed Denial of Service (DDoS) attack is becoming more sophisticated and complex and so has become one of favorite weapon for the cyber criminals to temporarily suspend or crash the services of a host connected to the Internet.

"The use of specific types of protocol reflection attacks such as SNMP surge from time to time," said Stuart Scholly, the senior vice president and general manager of the Security Business Unit at Akamai. "Newly available SNMP reflection tools have fueled these attacks."

The attack only targets the devices that runs an older version of SNMP, i.e. version 2, which by default is open to the public Internet unless the feature is manually disabled. The latest version of SNMP, version 3 is more secure management protocol.

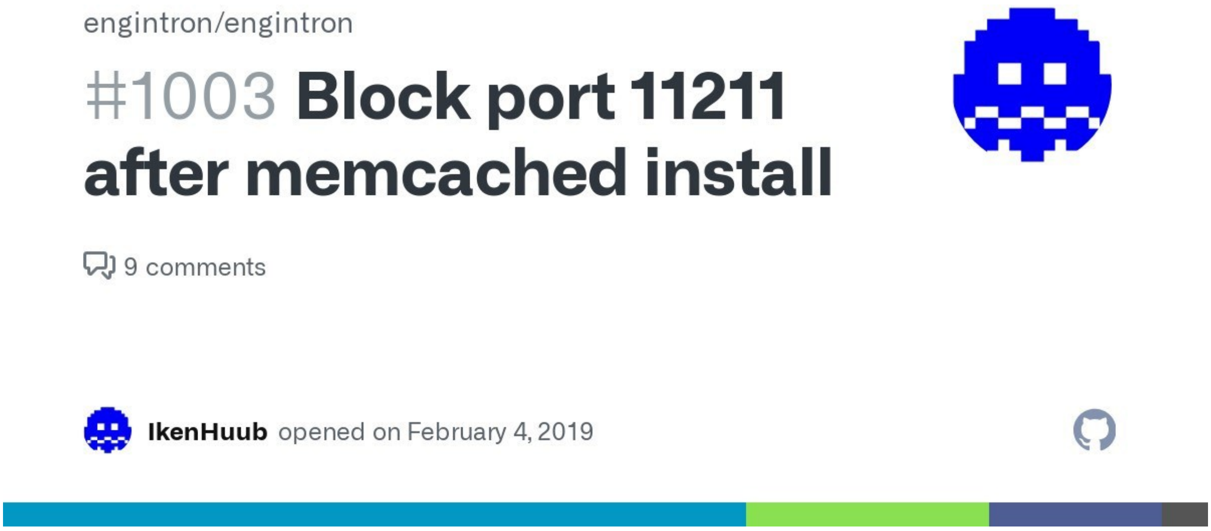
The cyber criminals made use of affective DDoS tools in an effort to automate the GetBulk requests against SNMP v2 that caused a large number of networked devices to send their entire stored data at once to a target in order to overwhelm its resources.

The attack is nothing but a distributed reflection and amplification (DrDoS) attack that allows an attacker to use a little skill and relatively small amount of resources in an attempt to create a larger data flood.

"Network administrators are encouraged to search for and secure SNMP v.2 devices," added Scholly. "The Internet community has been active in blacklisting the devices involved in recent DDoS attacks, but we also need network administrators to take the remediation steps described in the threat advisory. Network administrators can help prevent more devices from being found and used by malicious actors."

Since 2013, Hackers have adopted new tactics to boost the sizes of Distributed Denial of Service (DDoS) attack which is also known as Amplification Attack', leveraging the weakness in the UDP protocols. The most common is the (Domain Name System) DNS and (Network Time Protocol) NTP Reflection Denial of Service attack, but now cyber criminals have manage to use (Simple Network Management Protocol) SNMP to cause major damage.

7. MAJOR AMPLIFICATION ATTACKS FROM UDP PORT11211



engintron/engintron

#1003 Block port 11211 after memcached install

9 comments

IkenHuub opened on February 4, 2019

Figure 7.1 Port 11211

The general idea behind all amplification attacks is the same. An IP-spoofing capable attacker sends forged requests to a vulnerable UDP server. The UDP server, not knowing the request is forged, politely prepares the response. The problem happens when thousands of responses are delivered to an unsuspecting target host, overwhelming its resources - most typically the network itself.

Amplification attacks are effective, because often the response packets are much larger than the request packets. A carefully prepared technique allows an attacker with limited IP spoofing capacity (such as 1Gbps) to launch very large attacks (reaching 100s Gbps) "amplifying" the attacker's bandwidth.

STUPIDLY SIMPLE DDOS PROTOCOL(SSDP) :

The attack was composed of UDP packets with source port 1900. This port is used by the SSDP and is used by the UPnP protocols. UPnP is one of the zero configuration networking protocols. Most likely your home devices support it, allowing them to be easily discovered by your computer or phone. When a new device (like your laptop) joins the network, it can query the local network for specific devices, like internet gateways, audio systems, TVs, or printers. UPnP is poorly standardized.

When a control point is added to the network, the UPnP discovery protocol allows that control point to search for devices of interest on the network. It does this by multicasting on the reserved address and port (239.255.255.250:1900) a search message with a pattern, or target, equal to a type or identifier for a device or service.

IP-SPOOFING:

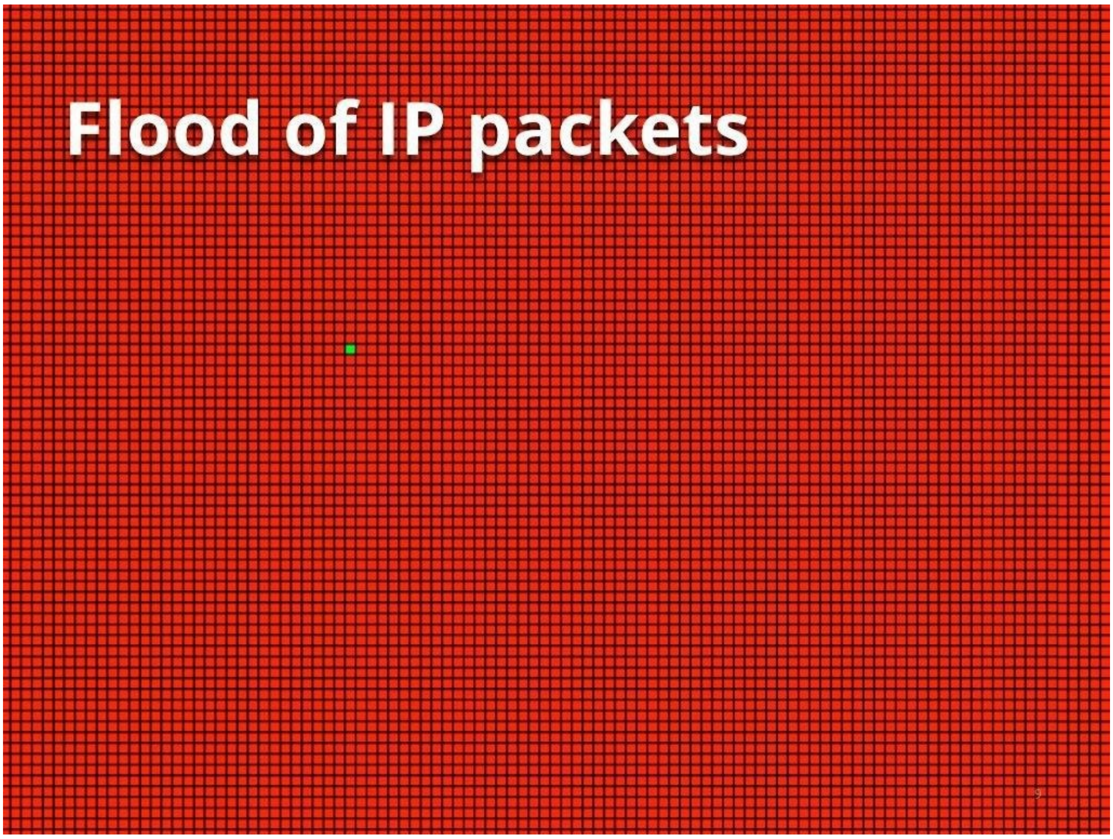


Figure 7.2 Flood of IP Packets

To be large they must be composed of a large, a very large number of packets. It's very hard to generate substantial traffic with legitimate fully established TCP connections. Instead these record breaking attacks are composed of a very large number of packets not belonging to valid sessions. They are often UDP or arbitrary TCP packets.

It's not uncommon that only one in ten thousand packets hitting our servers is legitimate. Very often the vast majority of packets belong to the attack.

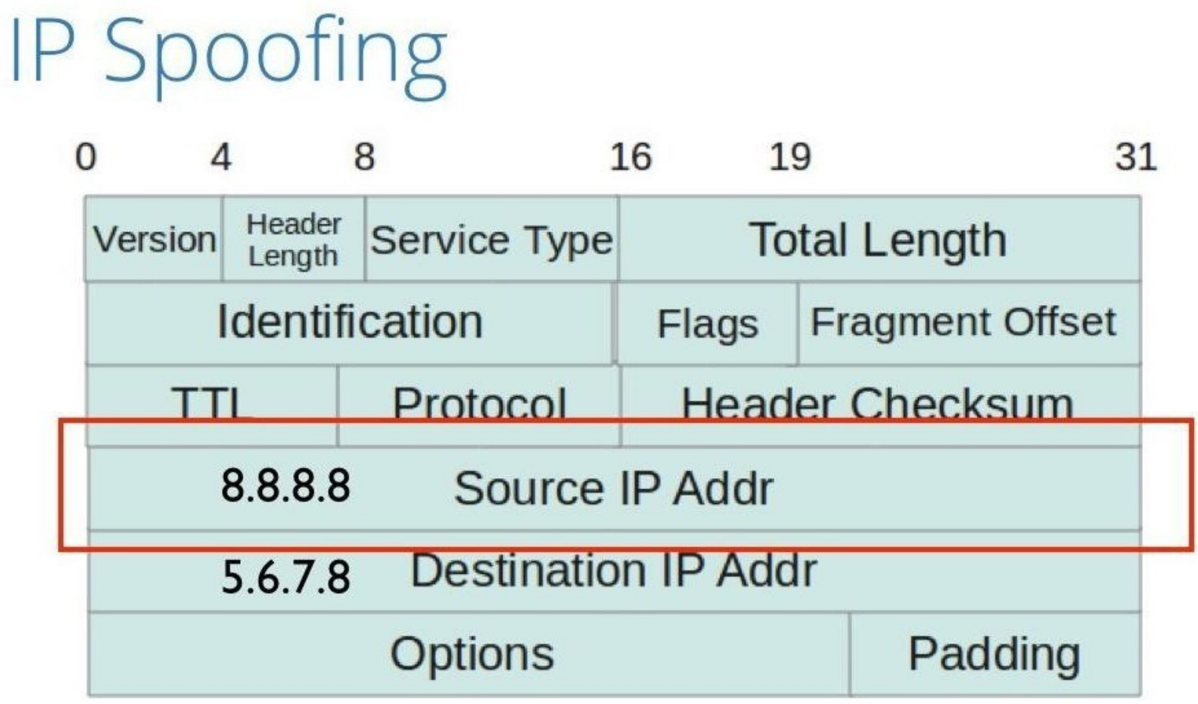
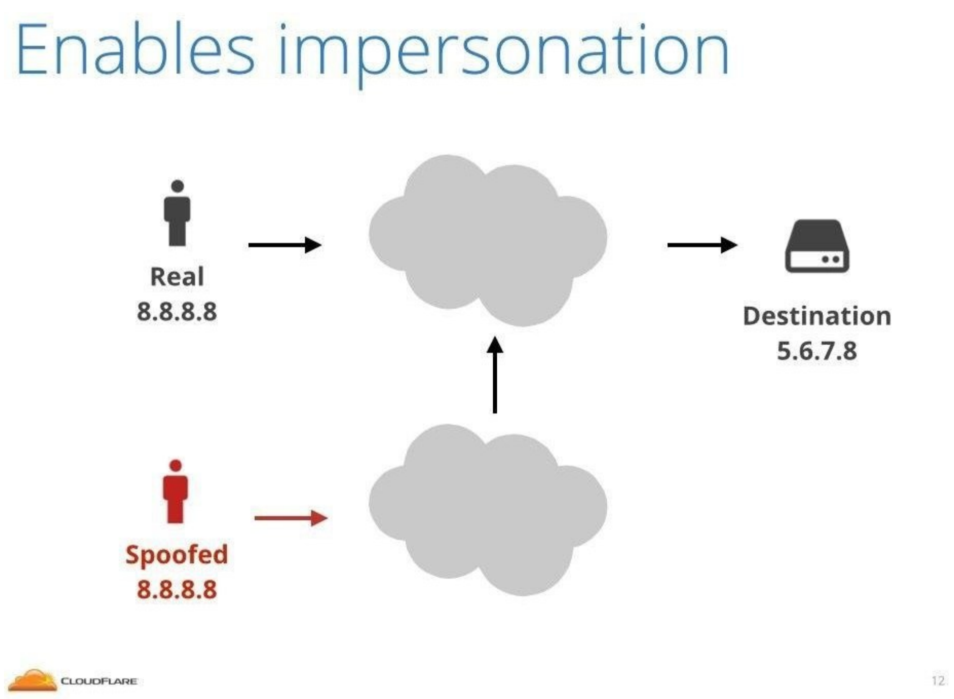


Figure 7.3 IP Spoofing

In the internet the data is chopped and delivered in packets. Each internet packet contains a header in which there are many of interesting fields, among them the source and destination IP addresses.

But the packet is just a series of bytes and whoever sends it can fully control it. If you transmit one over the wire, you can totally put anything you want inside the packet and inside the headers.

IP spoofing is an idea of rewriting the source IP address.

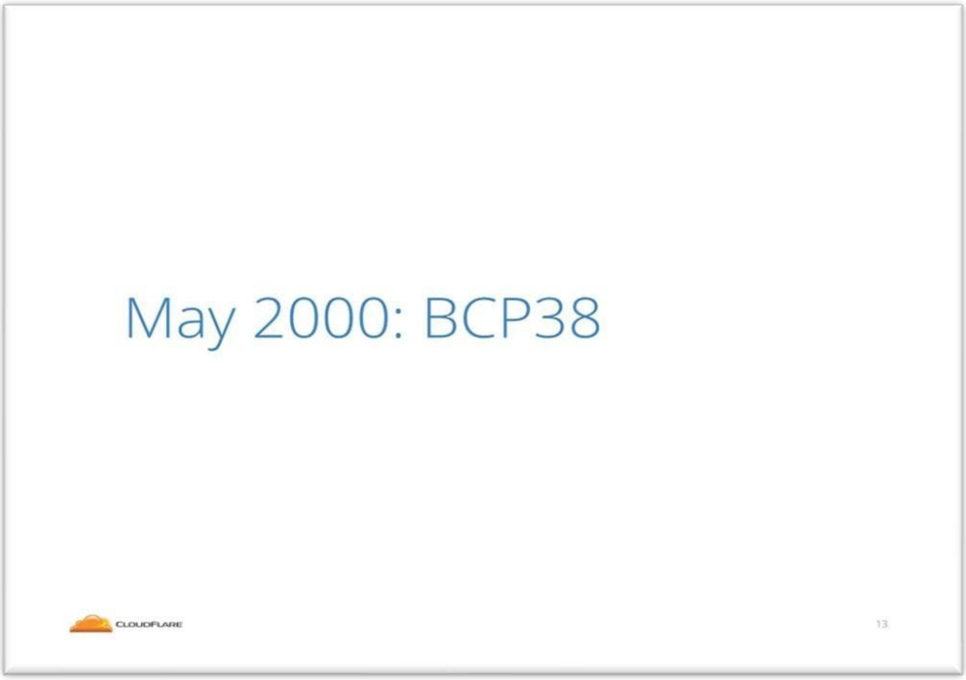


Enables impersonation

Figure 7.4 Impersonation

It might sound benign, but in fact IP spoofing is pretty bad.

One of the problems is that it enables impersonation. From the receiving end it's impossible to determine if the received packet was really transmitted by the real host or was maliciously injected into the internet by some impostor.



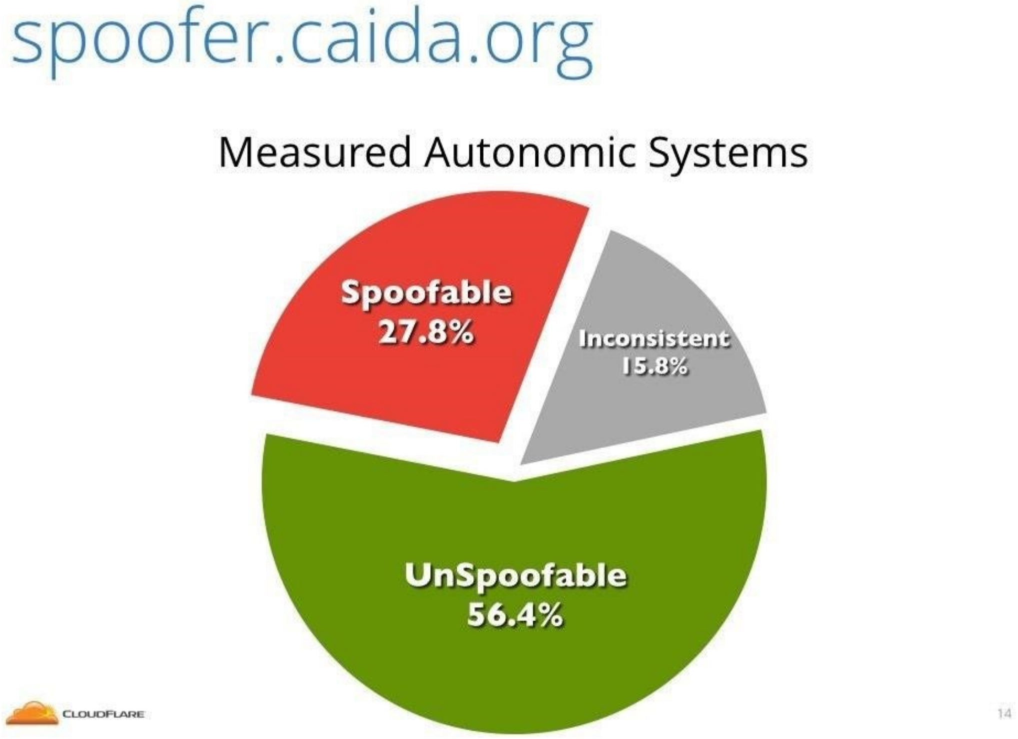
May 2000: BCP38

CLOUDFLARE

13

Figure 7.5 BCP38

Long time ago it was recognized that this can lead to significant problems. In May 2000 a famous document was published, called BCP 38. BCP stands for Best Current Practices, it's like an RFC document but a bit less formal. BCP 38 said clearly - IP spoofing may allow attacks and the internet community must proactively fight it.

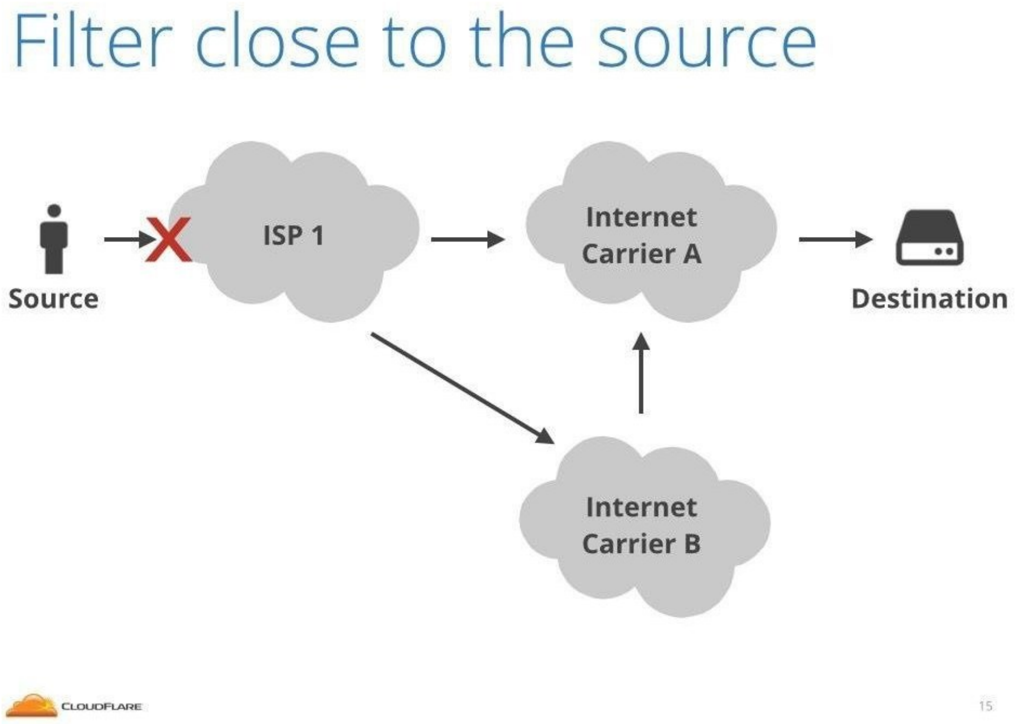


spoofer.caida.org

Measured Autonomic Systems

Figure 7.6 Automated Systems

Over the last 16 years much progress had been done in this direction, but it's still not fully solved. According to spoofer.caida.org project, still about 27% of the internet service providers do allow their customers to send spoofed IP packets. Unfortunately this number is not dropping these days. You may ask: why? What is so hard about not allowing spoofed packets to be transmitted?



Filter close to the source

Figure 7.7 Filtering

Basically the only way to stop IP spoofing is to do filtering very close to the source, the party originating the packets. If you have a home DSL connection, the filtering will be done on your modem. If you own a server it's the closest switch or router that must filter out the packets with spoofed IP addresses. This is not always simple. This requires the ISP's to have hardware that can do filtering, then to maintain the configuration. It costs money and expertise.

8. AMPLIFICATION

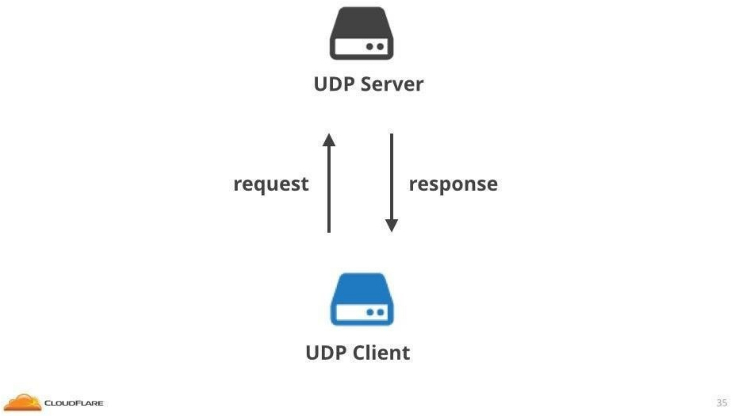


Figure 8.1 UDP Request Response

In order to explain amplification, we need to step back first. Let's talk about a protocol design.

Let's imagine a simple request-response protocol using UDP as the transport layer. The client asks some query, the server responds with an answer. This is for example how DNS and NTP work.

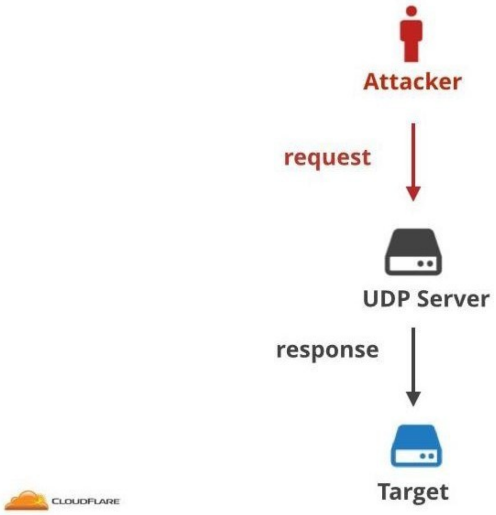


Figure 8.2 Amplification

The idea of amplification comes from abusing this design. The attacker fakes the request packet, and tricks the server into treating it as legitimate request. The server, unaware of the real source of the request, parses it and with all the good will sends the response to the target. But target never really asked for this data! This may not sound like a big deal, until you realize that often the response packet is much larger than the request!

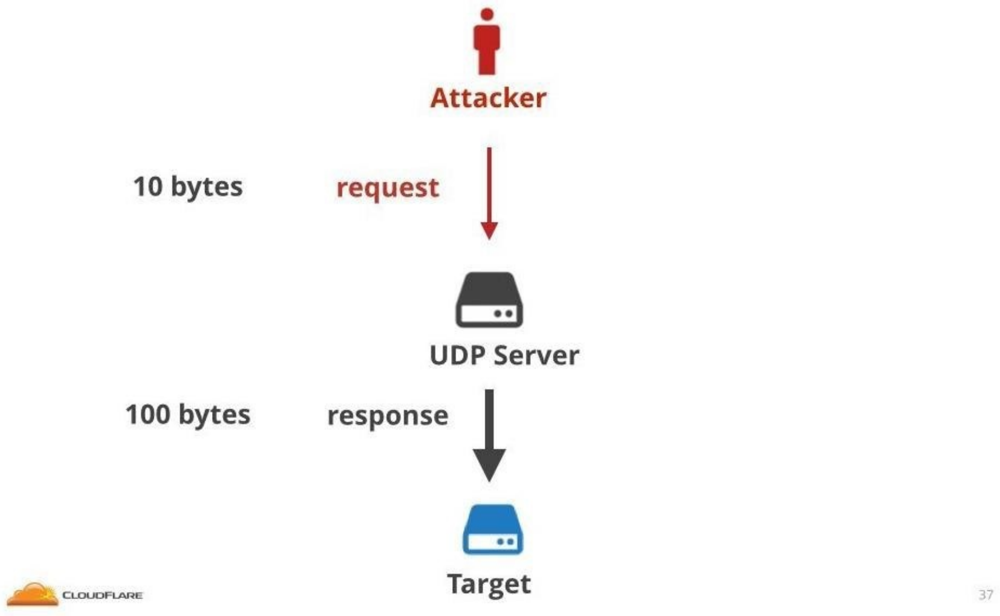


Figure 8.3 Amplification factor

For example, it's pretty common in DNS protocol that the request is trivial, consisting of only couple of bytes. While the answer is large with hundreds of bytes of payload.

This is the idea of amplification. Instead of sending traffic directly hassling the target it is possible to generate much larger bandwidth by bouncing out of some server.

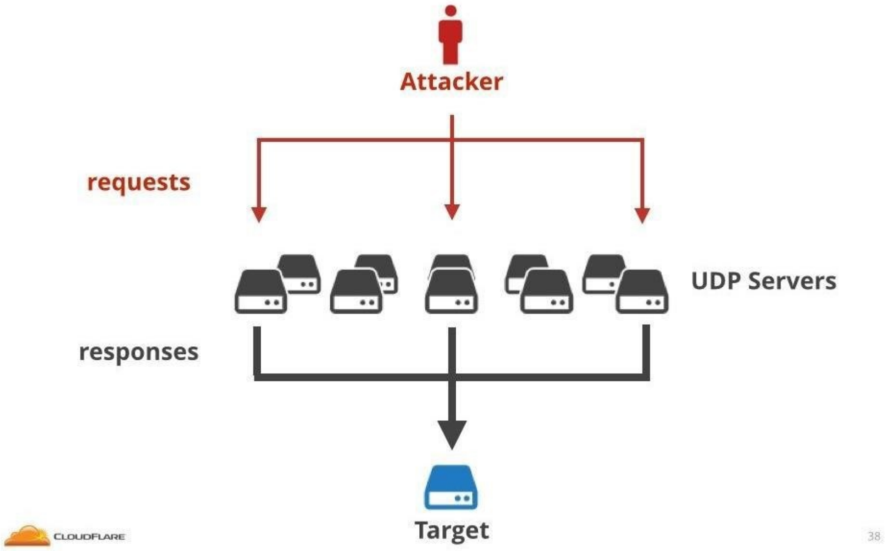


Figure 8.4 Scale Up

Bouncing off one server won't generate much load. But it's possible to scale up the attack and use an army of exposed UDP servers!

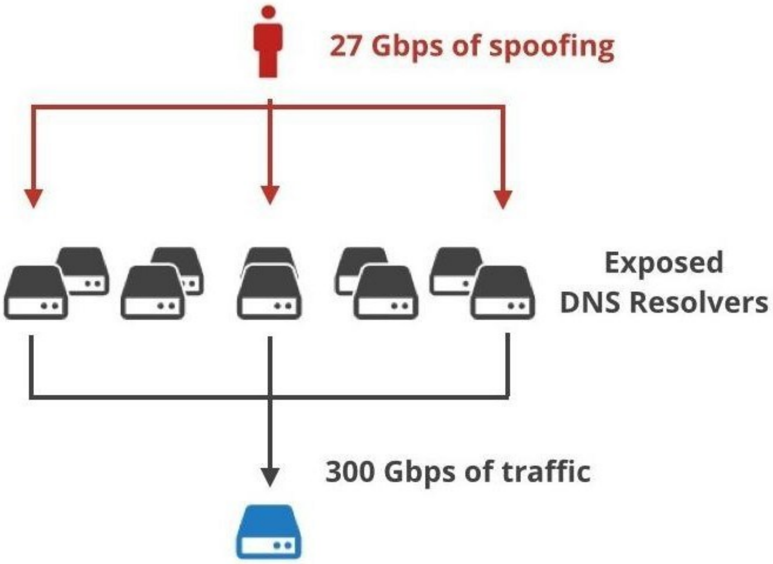
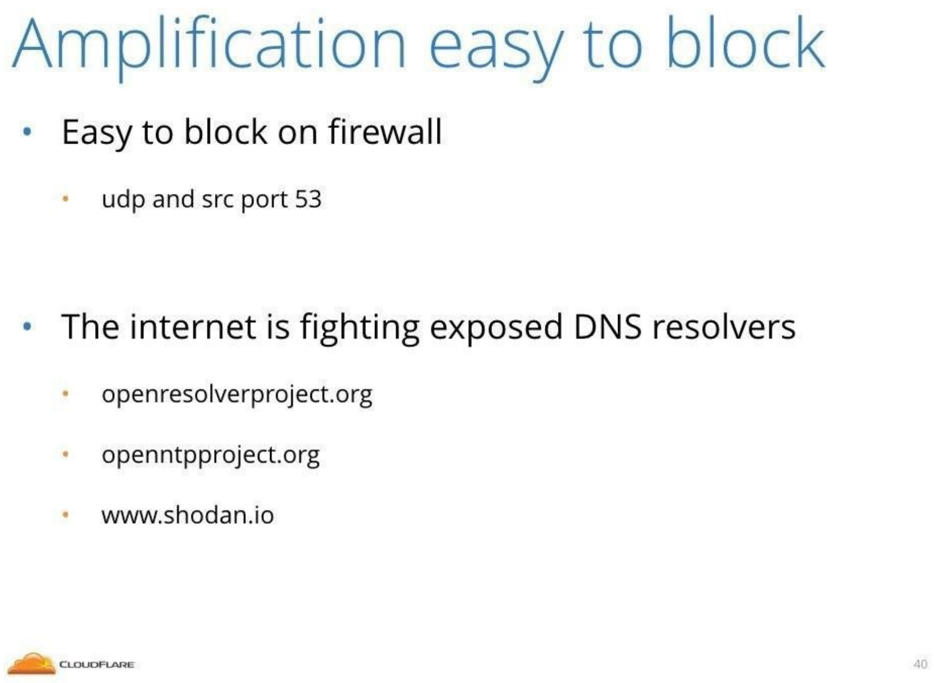


Figure 8.5 March 2013 Spamhaus

This is exactly what happened in March 2013. Back then we were hit by a very large attack directed at Spamhaus. We estimate that the attackers had access to three servers with 10Gbps connectivity. In total they had 30Gbps of IP spoofing capacity. They were able to amplify this power by bouncing off exposed DNS servers. In the end this generated 300Gbps of traffic hitting our servers.



Amplification easy to block

- Easy to block on firewall
  - udp and src port 53

- The internet is fighting exposed DNS resolvers
  - openresolverproject.org
  - openntpproject.org
  - www.shodan.io

CLOUDFLARE

40

Figure 8.6 Block Amplification

But I'll claim that amplification is not the most sophisticated type of attacks these days. First, they're fairly easy to block on firewall. Blocking DNS amplifications is as simple as dropping unwanted DNS answers by filtering packets coming from port 53.

9. OBSERVATIONS AND RECOMMENDATIONS

OBSERVATIONS FROM THE STUDY:

Proactive Defense Works

GitHub's quick response and use of Prolexic showed that being prepared can stop even massive attacks.

The Internet Has Weak Points

Servers with bad settings and open protocols like UDP are easy targets for attackers.

Amplification Makes Attacks Worse

Techniques like Memcached amplification let attackers turn small efforts into huge waves of traffic.

Cyber Threats Are Growing

As more IoT devices connect online, poorly secured devices make these attacks bigger and more frequent.

Global Impact

Big attacks don't just hurt the target; they can affect businesses, services, and people around the world.

MY RECOMMENDATIONS FOR DDOS ATTACK:

1. **Secure Server Settings**
   - **What Happened:** Attackers exploited poorly configured Memcached servers, which were accessible to anyone on the internet without security controls.
   - **What to Do:**
     - Turn off the **UDP** function if your service doesn’t need it.
     - Add strong passwords and restrict access to systems like Memcached using tools like **FirewallD** or **iptables** to block unwanted traffic.
     - Use Nmap or Qualys to regularly scan your servers for security vulnerabilities and misconfigurations.

2. **Use DDoS Protection Services**
   - **What Happened:** GitHub mitigated the attack quickly by working with Akamai Prolexic, a DDoS mitigation service.
   - **What to Do:**
     - Partner with services like Akamai Prolexic, Cloudflare, or AWS Shield, which specialize in stopping large-scale DDoS attacks.
     - Deploy scalable solutions capable of handling massive traffic surges using platforms like Imperva or Radware for cloud-based protection.

3. **Improve Monitoring and Detection**
   - **What Happened:** GitHub detected the attack early, which allowed them to respond quickly.

- **What to Do:**
    - Use monitoring tools like **Nagios, Zabbix, or SolarWinds** to identify unusual traffic patterns in real-time.
    - Implement AI-based tools such as **Darktrace or Cisco Secure Analytics** to analyze traffic and distinguish between legitimate users and attackers.

4. **Work Together Globally**
    - **What Happened:** Large-scale attacks don’t just affect one organization they can impact internet stability worldwide.
    - **What to Do:**
        - Share attack data using platforms like **ThreatConnect** or **MISP** (Malware Information Sharing Platform) to help others strengthen their defenses.
        - Collaborate with internet providers and organizations through alliances like **FIRST** (Forum of Incident Response and Security Teams) for a coordinated response.

5. **Test and Update Your Defenses**
    - **What Happened:** DDoS attack methods, like the one used on GitHub, are constantly evolving.
    - **What to Do:**
        - Run regular simulated attacks using tools like **LOIC** (Low Orbit Ion Cannon) or Hping3 to test your defenses.
        - Keep your systems up to date with tools like **WSUS** (Windows Server Update Services) or Patch Manager to prevent exploitation of new vulnerabilities.

6. **Train Your Team**

- **What Happened:** Responding to the attack required technical expertise and seamless teamwork.
- **What to Do:**
  - Provide cybersecurity training using platforms like **Cybrary** or **Immersive Labs** to prepare your team for real-world attacks.
  - Develop a clear incident response plan and rehearse it with your team using tools like Splunk Phantom or IBM Resilient for effective crisis management.

By incorporating these tools and practices, organizations can enhance their readiness and resilience against DDoS attacks.

10. CONCLUSION

Distributed Denial of Service (DDoS) attacks represent a persistent and evolving threat to digital infrastructure worldwide. Their ability to disrupt services, exploit vulnerabilities in systems like Memcached, and leverage amplification techniques to generate massive volumes of malicious traffic underscores their significance as a global issue. The sheer scale of the largest recorded attacks, such as the GitHub attack in 2018, demonstrates the critical need for robust defense mechanisms.

Mitigating DDoS attacks requires a multi-faceted approach, including advanced traffic filtering, securing vulnerable protocols, implementing rate-limiting, and adhering to best practices in network routing and encryption. Collaboration between organizations, governments, and security experts is vital to counter these sophisticated threats effectively.

As cybercriminals continue to innovate, the fight against DDoS attacks will remain an ongoing challenge. However, with proactive measures, improved infrastructure, and global awareness, the impact of these attacks can be minimized, ensuring the stability and security of our increasingly connected world.

11. REFERENCES

1. Research Gate

   https://www.researchgate.net/publication/259941506_DoS_and_DDoS_Attacks_Impact_Analysis_and_Countermeasures

2. Sagepub Journal

   https://journals.sagepub.com/doi/full/10.1177/1550147717741463

3. Springer

   https://link.springer.com/article/10.1007/s00500-021-06608-1

4. Github Blog

   https://github.blog/news-insights/company-news/ddos-incident-report/

5. Hackernews

   https://thehackernews.com/2018/02/memcached-amplificationddos.html

6. Popcount Organization

   https://idea.popcount.org/2016-09-20-strange-loop---ip-spoofing/

7. Sciencedirect

   https://www.sciencedirect.com/science/article/abs/pii/S1389128622005874

8. Chatgbt

   https://chatgpt.com/share/67482871-68a8-8013-be73-fdf1203751d5

9. Netscount

   https://www.netscout.com/blog/asert/memcachedreflectionamplification- description-and-ddos-attack

10. IEEE

    https://ieeexplore.ieee.org/document/10439150