jamk

Detecting DDOS attacks and how to mitigate them

Studying new possible ways to detect and mitigate DDOS attacks

Jari-Matti Finnberg

Master’s thesis
April 2025
Master's degree in Cybersecurity

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Finnberg Jari-Matti

Detecting DDOS attacks and how to Mitigate them

Studying new possible ways to detect and mitigate DDOS attacks

Jyväskylä: Jamk University of Applied Sciences, January 2025, 40 pages.

Degree Programme in Cyber Security, Engineering. Masters thesis.

Permission for open-access publication: Yes

Language of publication: English

Abstract

Distributed Denial of Service attacks, or DDoS, have been a growing menace on the internet for years. In recent years, the number of attacks has increased, along with their impact on internet services. Attackers tend to use more sophisticated attack vectors in their attempts to bring target systems offline. This thesis aims to document methods for identifying new attack vectors, mitigating them, and providing the reader with a comprehensive overview of how to protect the internet from DDoS attacks. Most new attacks are carried out using botnets across the internet. These botnets typically comprise standard internet-connected equipment. In recent years, Internet of Things (IoT) devices have become commonly exploited for botnets due to their lack of security and default passwords.

Recognizing the risks associated with IT systems and their resilience against DDoS attacks is essential. These risks may result in financial losses, reputational harm, or even disruptions to societal functions. National regulations hold companies more accountable for their cybersecurity efforts and strive to protect society and its services from cyberattacks.

This topic was chosen because most theses only mention DDoS in the context of the cyber domain but do not cover the entire landscape of the attacks. This thesis contributes timely insights into how the attacks have changed and provides predictions on how they might evolve. A critical aspect of DDoS is the use of Artificial Intelligence and Machine Learning in mitigations, as well as their role as a tool for attackers to execute more destructive DDoS attacks.

The data used is mainly collected from various vendors supplying DDoS protection, as well as from Telia. The usage of Telia data is conducted in such a way that no customers can be identified, as that information is not publicly available. Telia commissioned this thesis to serve as training material and a summary of how DDoS attacks are detected and mitigated. The company reference and approval can be found in Appendix 1.

Keywords/tags (subjects)

DDoS, Cyber, Denial of Service

Miscellaneous (Confidential information)

-

Contents

Figures

Tables

Acronyms

ACK	TCP Acknowledgement flag
API	Application Programming Interface
BGP	Border Gateway Protocol
CLDAP	Connection-less Lightweight Directory Access Protocol
CPE	Customer Premises Equipment
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DNS	Domain Name Service
DOS	Denial of Service
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
LoIC	Low Orbit Ion Cannon
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OSI	Open Systems Interconnection Reference Model
SSDP	Simple Service Discovery Protocol
SYN	TCP Synchronization flag
TCP/IP	Transmission Protocol / Internet Protocol
UDP	User Datagram Protocol

1 Introduction

Distributed Denial of Service (DDoS) attacks have been around for years. These attacks have brought down systems over the Internet and caused damage to businesses, as well as civilian infrastructure. Nowadays, attacking is easy with online network booters and even with a single home computer using the home network's bandwidth for more minor attacks. The Internet of Things (IoT) has been used in many botnets in recent years due to their lack of security and poor password protection. Botnets such as Mirai have been around for almost 10 years, and new versions of them are being built and used once the old ones get taken down by authorities.

There are several motivations for carrying out DDoS attacks. Script kiddies initially launched attacks to disrupt their schools or other organizations from which they could gain an advantage. Later, DDoS attacks became a means for attackers to extort money from organizations. Additionally, hacktivists use DDoS attacks to gain visibility. State-sponsored hacker groups have also started using DDoS attacks in their cyber warfare. This kind of attack is meant to disrupt and cause uncertainty in societies. In recent years, some state-sponsored attackers have been targeting other countries for various reasons. These reasons include Nordic countries Sweden and Finland joining NATO and giving aid to Ukraine to fight the war they are in with russia.

A DDoS attack might result in significant losses depending on the target organization. For example, sales losses may be substantial if the attack targets an online vendor. Depending on daily sales, DDoS attacks may result in significant financial losses or reputational damage. Reputational damage can also result in financial losses if consumers lose trust in the company. The risks concerning DDoS attacks need to be recognized in advance for companies to mitigate them early and be able to withstand and protect against the attacks.

The change over the years in DDoS has been subtle, as some attack vectors that were first used in the 1990s continue to persist. Attack vectors that exploit vulnerabilities in network equipment or software typically become obsolete with system updates. However, those that depend on the poor configuration of internet-facing servers will remain as long as the software is misconfigured.

Earlier, the more significant DDoS attacks were primarily UDP-based, making them easier for attackers. In recent years, however, these attacks have shifted toward stateful types, such as TCP

SYN or TCP ACK, which are more demanding for attackers but harder to mitigate, making them more effective.

2 Research background

Telia has fought against DDoS attacks for over 20 years and has seen their evolution. This research mainly focuses on volumetric attacks, as most application layer attacks are usually mitigated with Web Application Firewalls or similar, closer to the servers. However, a theory of application layer attacks is explained since it is essential to understand. As an Internet Service Provider (ISP), Telia mainly protects its core networks from congestion and thus provides customers with better service. The protection method primarily uses scrubbing centers, which clean out the network traffic before it reaches the customer or Telia's services. This thesis focuses on introducing the reader to detecting and mitigating DDoS.

2.1 Research objectives and limitations

The research data comes from Telia and its vendors. The results are left for the reader to draw their own conclusions. In some cases, the world of DDoS is uncertain; for example, why and who orchestrated a particular attack will be left unanswered. One can make assumptions about the attackers, but to be sure, further investigation is needed.

This thesis aims to serve as a guideline for new personnel hired to defend against DDoS attacks. The research questions in this thesis are:

- How have DDoS attacks evolved over the years?
- How can they be mitigated?
- How has the global political situation altered the nature and scope of the attacks?
- How can risks related to DDoS attacks be identified?

2.2 Research Methodology

This thesis is based on the numbers and volumes of DDOS attacks, which makes the research method quantitative. Most of the research has been done by finding sources from the Internet

and Telia logging systems. The Telia data is masked, so there are no customer names or information on Telia's capabilities. Different vendors mask the data found on the internet, and thus, the targets cannot be recognized.

2.3 Method of Writing

This thesis and its data were obtained from various internet sources and books by Janet Finna. Artificial Intelligence services have been used primarily to help find new sources. The spelling and clarity of the text are corrected with the help of Grammarly. In some chapters, Grammarly AI has also been used to improve the text with its “improve text” function, and it is cited with “(Grammarly, Year)” citation.

3 Theoretical background

3.1 History

DDoS attacks have existed for a long time. However, there is a debate on what and when the first DDoS attack occurred; researchers agree that it happened at the beginning of the 21st century. (Sockrider, 2024). The First Denial of Service attack (DoS) was made in 1974 by David Dennis towards the Computer Based Education Research Laboratory (Radware, 2024). Most DOS attacks are based on a vulnerability or a malfunction of software or protocol. A single attacking host usually performs DoS attacks, but DDoS involves multiple attacking hosts conducting the attack. The attacks are generally distributed with various kinds of botnets.

The basic workflow of the attack from the attacker's perspective is mostly the same as any other cyber-attack. The attacker usually starts by finding the target. The target IP addresses can usually be found by a simple nslookup command, which finds the IP addresses associated with a URL (see Figure 1. nslookup command). The choice of attack vector, or method of attack, usually comes with the tool. If an internet service for DDoS attacks —a network booter— is used, the attacker only needs to know the service's IP address to attack it. Some network booters allow the user to choose the attack vector depending on the target.

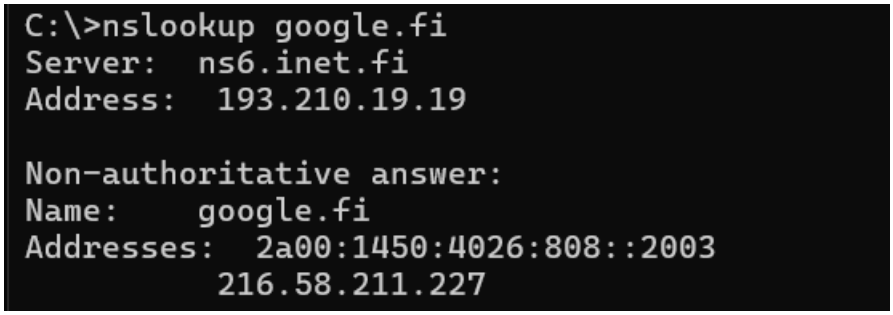

Figure 1. nslookup command

Among the first Denial of Service attack types was “Ping of Death,” used to crash computers and servers. The attack was initially discovered in 1996 (Impreva, 2024) or 1997 (Netragard, 2024), and it was used to crash Windows 95 and Windows NT operating systems (Impreva, 2024). The attack consisted of an oversized PING packet sent in fragments, which caused the operating system to crash when trying to reassemble it. The original vulnerability was fixed in later Windows releases, but new versions were discovered in 2011, 2013, and 2020 in the Windows operating systems (Netragard, 2024).

The early attacks were mainly carried out by people wanting to disrupt each other and some services, such as games. At the beginning of the 21st century, DDOS attacks and other cyber-attacks became more professional, and money became the common motivation for attacking. Also, many state-sponsored actors started using DDOS as a type of cyber warfare. For example, at the beginning of the year 2022, before the full-scale invasion of Ukraine, russia launched several DDoS attacks against Ukrainian IT infrastructure. These attacks intended to disrupt Ukrainian civil infrastructure and thus make the country more accessible to invade.

At the end of 2014, Finnish banks were hit with a big and, at that time, long-lasting DDoS attack. Finnish bank Osuuspankki had the most impact this time, and the bank’s services were affected throughout Christmas and New Year 2015. At the time, the attack was announced to be made by the russian hacker team Core Sec, which later was revealed to be two young males from Finland who were pretending to be class-A criminals (Kerkkänen, 2016). This attack was a classic example of an extortion attack. The attackers posted demands on Twitter (now x.com). None of the banks

affected paid the attackers anything. This attack caused many companies to invest in DDoS protection (Kerkkänen, 2016). The attackers were caught and charged with several crimes. The leading attacker was convicted and required to pay Osuuspankki 14,500 € and sentenced to one year and four months of conditional imprisonment. The second attacker was convicted to three months of conditional imprisonment for assisting in the cyber crimes. (STT, 2017)

Even today, some attacks are done by gamers and private individuals as revenge or to gain monetary value, for example, in online poker or other gambling. Some online poker sites have an auto-fold function that folds if the user has not reacted in a specific time. If the user is DOSed, they cannot respond and thus automatically fold and give the money to the co-playing attacker.

Due to digitalization, DDoS attacks have become more effective. Many companies and organizations that provide services over the Internet are vulnerable to DDoS attacks. In return, many ISPs have started offering their customers DDoS protection. Since the ISPs need to protect their network, they can offer DDoS protection with the same equipment also to their customers—chapter Mitigations describes this protection in more detail Mitigations.

In recent years, attacks have evolved toward OSI Layer 7 attacks. While volumetric attacks have not disappeared, most attacks against web services are now application-layer attacks.

3.2 Attack Types

3.2.1 Flooding attacks

Attack types tend to change along with the services and applications attacked. Volumetric flooding attacks can congest the whole network where the target is located and disrupt all the other users and customers. Volumetric attacks use a large bandwidth to deny the target service or server. The bandwidth can be gained using botnets, servers vulnerable to amplification attacks, or attackers' excessive bandwidth.

There are several ways of conducting a traffic flood attack. The primary method of attacking a single host is to send excessive bogus data from one server to another. This way requires the attacker to have enough resources in the attacking server and the internet connection. The most basic way of doing this is by using, for example, an application called hping3. Hping3 is an application that can send arbitrary TCP/IP packets to test out a server/web application/computer/network equipment, etc. (Kali.org, 2024)

3.2.2 Reflection or Amplification Attacks

Reflection or Amplification attacks are done with legitimate yet vulnerable services on the Internet. Amplification is done by requesting something from a legitimate source by spoofing the victim's IP address. This results in the intermediary responding with many packets toward the victim. The attacker can send thousands of requests to these vulnerable services and make them react to the victim with numerous packets. (Netscout, 2024d). Reflection attacks are similar but react with significantly larger packets toward the victim.

DNS amplification attack

Domain Name System (DNS) amplification attacks use vulnerable DNS servers around the Internet to amplify the attack traffic by spoofing the victim's IP address and creating a DNS request with this address. The vulnerable DNS server responds with a much larger packet to the victim. When this is done with hundreds of vulnerable DNS servers, the number of requests will be high, and the victim’s service will be denied. See Figure 2 (Sagatov et al., 2023)

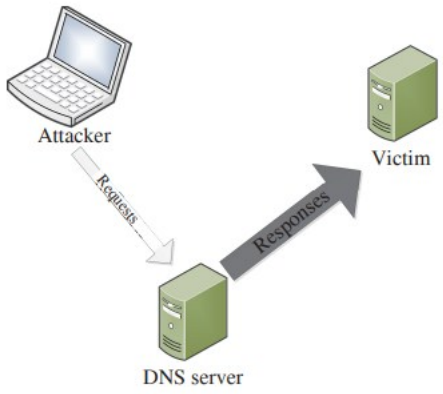

Figure 2. DNS Amplification attack (Sagatov et al., 2023)

These attacks use User Datagram Protocol (UDP), a connectionless packet. This way, the attacker can spoof or substitute his IP address to a victim's address and thus get the vulnerable DNS server to send significant responses to the victim. The attacker sends the DNS server an "ANY" query, which returns all the records for a specific domain. In comparison, the attacker must send only one request to the server, which responds to the victim with a larger packet. This attack-type amplification factor is 160:1 (Netscout, 2024c), so if the attacker sends one byte of traffic, the vulnerable server responds with 160 bytes.

NTP amplification attack

NTP amplification attacks are another way of amplifying the attacker's traffic. Like DNS amplification, NTP amplification uses UDP traffic to overwhelm the victim's network bandwidth. NTP keeps the devices in the network at the same time and phase. The attack uses a Monlist request from the NTP server. The attacker sends multiple Monlist requests from a Botnet with a spoofed victim IP address. (Cloudflare, 2024a) The monlist response sends out a maximum of 600 last client IPs that have recently communicated with the NTP server.

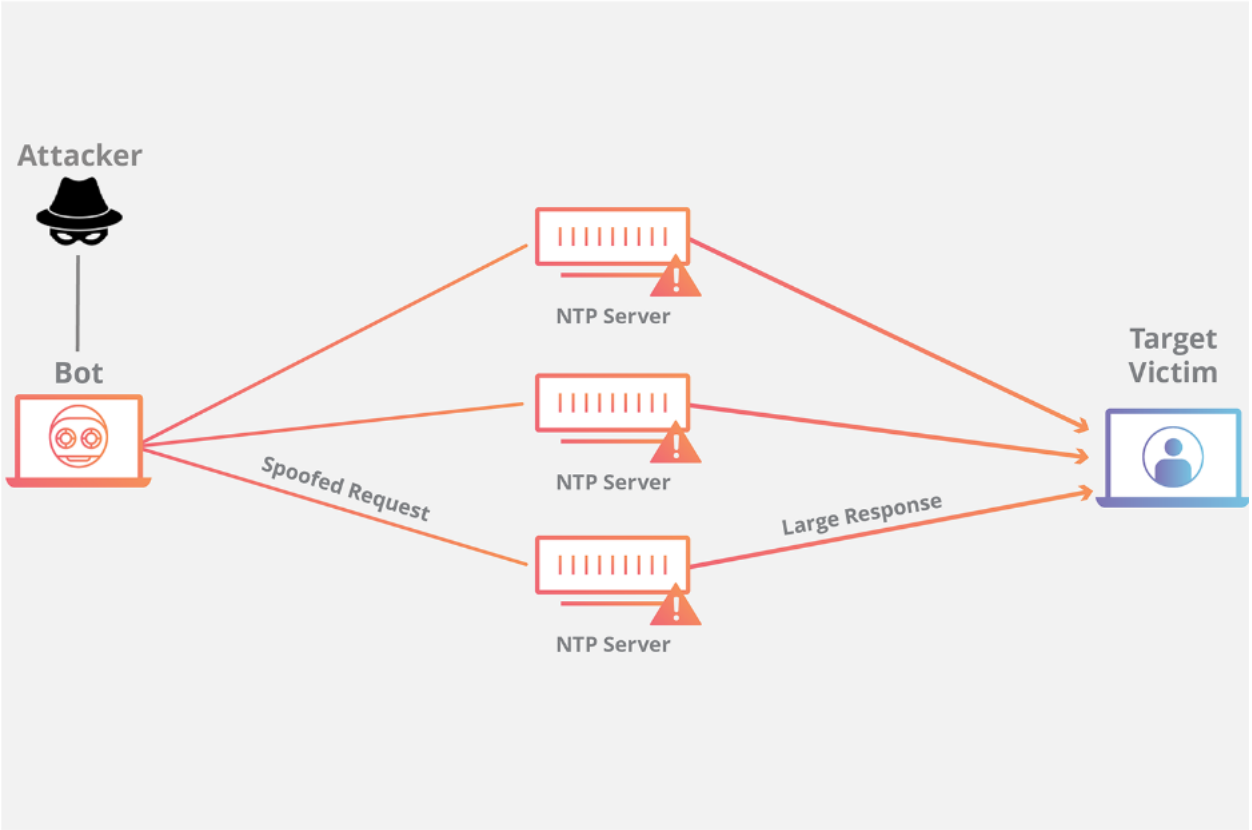

Figure 3. NTP amplification attack(Cloudflare, 2024a)

SSDP amplification attack

Simple Service Discovery Protocol (SSDP) is widely used to discover the Internet of Things (IoT) devices such as cameras, printers, or refrigerators connected to the Internet and vulnerable or open to sending traffic anywhere. In recent years, Internet of Things devices have grown significantly and will continue. The lack of security updates from the vendors and the inexperienced users who do not update their systems frequently enough will keep this kind of attack on the rise. It is also worth mentioning that these vulnerabilities are not limited to DDoS attacks but can compromise the user's information security. (Cloudflare, 2024b)

SSDP protocol allows devices to broadcast their presence to other devices in the network. The attacker first needs to find the devices connected to the internet and list them for later use. In the attack phase, the attacker sends a request with a spoofed IP address to the vulnerable device with flags such as ssdp:rootdevice or ssdp: all. As in the other amplification attacks, this results in

a significantly bigger packet to be sent to the victim. As a result, the SSDP device sends up to 30 times more data to the victim than the attacker sent (Cloudflare, 2024b).

CLDAP amplification attack

Connectionless Lightweight Directory Access Protocol (CLDAP) is a protocol for getting information from information services such as Active Directory (AD). Like other amplification attacks, the CLDAP attack also uses multiple vulnerable servers over the internet to amplify the number of packets sent to the victim. The way of attacking is to send spoofed packets to the vulnerable servers with the victim's IP and gain significantly larger packets to respond to the victim. The main impact of the attack is either a whole network congestion or a Denial of Service in the victim's server. (Mohan, 2024)

3.2.3 Stateful Attacks

Nowadays (2024), the TCP-Syn attack is the most common type of attack. It can be done with, for example, the Hping3 tool. The attack is simple since it only sends the victim a TCP handshake SYN packet. When many of these SYN packets exist, the victim host resources send SYN-ACK packets back to the attacker. After SYN-ACK, the victim host waits for the ACK packet but never receives it. The three-way handshake process of the TCP protocol is shown in Figure 4 Furthermore, it is explained more after the figures.

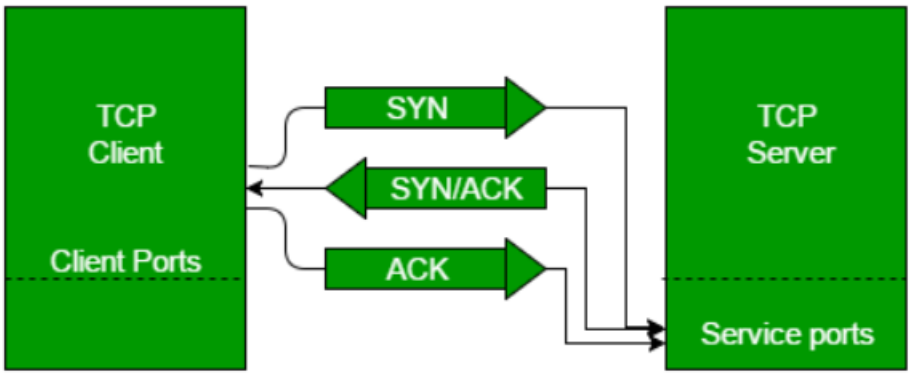

Figure 4. Three-way TCP handshake(GeeksforGeeks, 2024)

The TCP-SYN packet is pictured in Figure 5 Moreover, shows the SYN flag enabled in the packet. The SYN packet is the first TCP packet handshake, followed by a SYN-ACK packet from the destination server. After this, the server waits for the ACK packet from the sender. This attack is meant to make the destination server stand waiting on the ACK packets from all the senders, thus using up most or all the resources on the destination server.

```
Transmission Control Protocol, Src Port: 19601, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 19601
    Destination Port: 443
    [Stream index: 17]
  ▸ [Conversation completeness: Incomplete (61)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1797240919
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1010 .... = Header Length: 40 bytes (10)
  ▾ Flags: 0x002 (SYN)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Accurate ECN: Not set
       .... 0... .... = Congestion Window Reduced: Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...0 .... = Acknowledgment: Not set
       .... .... 0... = Push: Not set
       .... .... .0.. = Reset: Not set
     ▸ .... .... ..1. = Syn: Set
       .... .... ...0 = Fin: Not set
       [TCP Flags: ·····S·]
    Window: 26883
    [Calculated window size: 26883]
    Checksum: 0xd85c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  ▸ [Timestamps]
```

Figure 5. TCP-SYN Packet

3.2.4 Application layer attacks

In recent years, basic DDoS attacks have evolved into application-layer attacks. The application layer is the seventh layer in the OSI model. As volumetric DDoS attacks are made in layer three, the networking layer, and layer seven attacks are mainly targeted toward web services and applications.

The application layer can be attacked using vulnerabilities in web servers. The attacks are usually low in volume, so their detection can be difficult with standard DDoS protection equipment. Common types of Layer seven attacks are:(Bienkowski, 2024)

- DNS water torture.
- Slowloris.
- Slow Post.
- Slow Read.
- HTTP(S)-Flooding.
- Low and Slow Attack.
- Large Payload POST.

For example, SlowLoris attacks use HTTP requests to open connections to web servers and keep these connections open without requesting or using them. This results in consuming the web server's available connections so that a regular user cannot connect there anymore. These attacks are common against Apache 1. x and Apache 2. x servers. (Netscout, 2024e). Newer versions of Apache servers have a setting to prevent these attacks. These mitigations are discussed in the chapter 3.6.4.

3.2.5 DNS Water Torture Attack

DNS water torture is a form of attack used to exhaust the Domain Name Servers (DNS). The DNS servers can be regarded as the backbone of the Internet since they help with the usability of the Internet and networks. The typical internet user cannot remember the IP addresses of the various services online; thus, DNS services are Essential. DNS floods have been around since 1997, but they have evolved toward water torture attacks (Netscout, 2024b)

DNS converts the IP address to a human-readable name, see Figure 6. The DNS is based on a structure that consists of the top-level domain (google.***com***), second-level domain (***google***.com), and possible subdomains (***mail***.google.com). Root DNS servers handle the top-level domains, and the lower-level servers handle the rest of the domains and sub-domains.

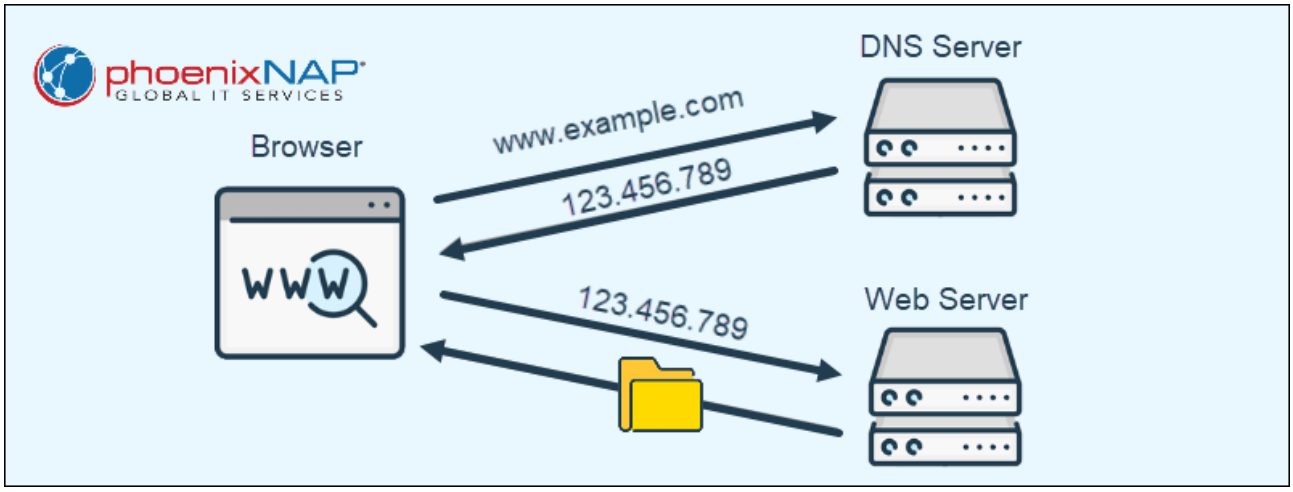

Figure 6. DNS server basics (Phoenixnap, 2024)

DNS water torture is usually targeted toward DNS resolvers that give out IP addresses of subdomains. The attack aims to exhaust the resolving server's capacity by asking for several bogus domains from the resolver, such as ***abcdefg***.google.com. Since all DNS servers must answer all queries, the server uses CPU time and memory to determine if it has a bogus subdomain in its database. In the worst case, the server might become unresponsive and unable to serve legitimate requests.

In many systems, water torture attacks can cribble the whole infrastructure since the users cannot use the services. Most users do not know the IP address of the services, and even if they do, many services have their SSL certificates applied only for the Fully Qualified Domain Name (FQDN) and not the IP, so modern browsers might alert the site as being “not secure.” Many services use only FQDN in their site-to-site communications, such as APIs. This results in total denial of services and can cause a widespread impact over the internet.

Figure 5 shows an introductory DNS water torture attack packet. For security reasons, the actual domain name has been obscured. The specific subdomain request is displayed in the queries section. When a DNS server is flooded with these—often creative—subdomains, its resources are diverted to finding them instead of serving actual customers. Attackers might also use an online dictionary or wordlists in creating these fake domain queries.

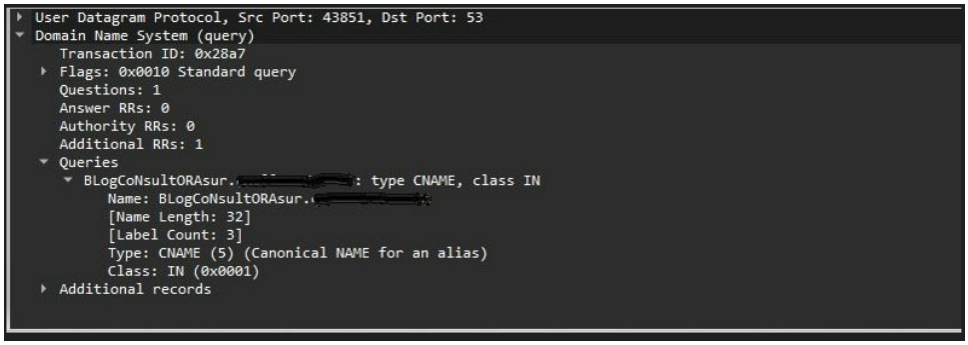

Figure 7. DNS water torture attack packet

3.2.6 Carpet Bombing Attack

Carpet Bombing attacks have been around for a few years, mainly used to congest the target network or the ISP. These attacks are difficult to detect because the traffic originates from multiple IP addresses. In Carpet Bombing attacks, both the source and the victim are distributed. The bandwidth of the attack per host is typically less than that of more common attacks, making detection more challenging. Most ISPs detect attack traffic per host, so in the case of carpet bombing, the detection systems do not trigger an alert or automatic mitigation (Netscout, 2024f). Carpet bombing attacks are not a primary attack vector, as the actual vector is some other attack vector mentioned previously. Carpet bombing attacks have recently evolved from NTP or DNS amplification vectors to TCP SYN and TCP ACK attacks.

These attacks are often combined with some amplification attack. However, it is configured so that instead of a single host, the victim is an entire subnet, for example, a/24 subnet, which has

255 addresses. If the attack traffic per host is, for example, 10 Mbps, the total ramps up to 255 × 10 Mbps = 2.5 Gbps, thus disturbing the router and denying internet service to the entire organization.

3.2.7 Summary of DDoS Attacks

Over the years, mitigation and detection systems have improved. Flooding, Reflection, Amplification, and stateful attacks are no longer effective enough for some attackers' purposes. This is the reason why more and more attacks are based on the application layer. Application-layer attacks are more challenging to detect since most are slower and use less bandwidth. The biggest problem in detecting application-layer attacks is that they mostly use HTTPS, eq. packets are encrypted. The decryption of HTTPS is done on the web servers, and internet service providers cannot decrypt it.

Several examples of botnets used in DDoS attacks exist. Botnets can be created with malware, allowing an attacker to send traffic to an unsuspecting victim's computer or IoT device. Most botnets consist of an enormous number of devices, so in most cases, the botnet victim does not know that the device is used in this kind of activity. (A10, 2024) Most hacker groups have their botnets; the most known are Mirai and Killnet. Killnet is a botnet used by the pro-russia hacker group NoName057(16). NoName057(16) has made a tool that volunteers can download and share their bandwidth with DDoS attackers. Participants can also get paid with cryptocurrencies if their contribution is good. (Patil, 2023)

Many Internet services are officially used to test websites. However, some do not check whether the system being attacked is the buyer's website; these are network booters or network stressers (Cloudflare, 2024c). The booters are an on-demand service provided by enterprising criminals to deny the services on the internet. These services are available to a typical consumer who, for some reason, wants to bring down a service or another consumer. Using these stressers or booters is illegal if they are used without the target's consent. Legitimate stressers use more strict ways of confirming that the system attacked is legitimate. For example, Amazon Web Services (AWS) approves DDoS testing with NCC-group plc, Redwolf Security Inc., and Red Button. (AWS, 2024) Testing against AWS-run services is strictly under terms and conditions, which include bit, packet, and request volume limitations. From the AWS-approved partners, Redwolf requires C-level approval and ISP approval to conduct DDoS testing.

3.3 Attack effects on operations and business

DDoS attacks can cause many problems for organizations. Depending on the business, the impact can cause significant financial damage to a company. Revenue loss can be calculated by multiplying the hourly revenue of a company with the duration of an attack. As described in the chapter 3.1 At the beginning of 2015, the Finnish bank Osuuspankki suffered substantial losses due to a DDoS attack. OP demanded over 400,000 euros of compensation for the losses, but the court ruled that 14500 euros compensation for damage caused to the company.

The damage caused to the victim is not always directly financial; reputational damage is also an important side to consider. In the long term, reputational loss might also result in losing sales and customers. In the online world, even the slowness of the website might push customers away. Even loading times of 250 milliseconds might cause the customer to use a different vendor (Kenig, 2013).

3.4 How DDoS attacks are described

As stated in the beginning, the basic attack is called a Denial of Service, which can be done in several ways. Usually, when talking about attacks on the internet, they are called Distributed Denial of Services (DDoS), which is denial of service done from multiple sources at a time. This adds more bandwidth to the attack and makes it difficult to mitigate.

Measuring DDoS attacks is straightforward, as it is done using either bits per second (bps) or packets per second (PPS). When measuring web servers, requests per second are used. Some companies want DDoS attacks reported by source countries and even at the source IP address level. In most cases, the source IP addresses used are spoofed, and there is no meaningful way to use them in any filter list or as proof. ISPs might observe some malicious activity in their customer networks, and this is reported to the customer to update their routers or other internet equipment.

3.5 Detecting attacks and new attack vectors

DDoS attacks are typically detected within ISP core networks. For instance, Netscout protection systems employ collectors that receive NetFlow data from core and edge routers for detection. NetFlow, a network protocol developed by Cisco Systems, is crucial in network monitoring. Routers and other network equipment gather detailed information about network traffic, such as source and destination, ports, and protocol, and send it to a collector device. (Petryschuk, 2024). Beyond DDoS monitoring, NetFlow is also instrumental in monitoring network performance.

This data is processed using special collector equipment that finds attacks with a fingerprint database. In ISP networks, the amount of data is enormous, and some sampling is needed to reduce the amount of data required to be processed. The services are configured to the protection system as Objects to improve the system's detection of attacks. The configuration usually consists of the fingerprint detection rates a single host can handle. The equipment vendor usually does the fingerprints.

Some cyber security vendors employ a collaborative DDoS attack detection and mitigation approach. They use honeypot networks and network probes over the Internet to identify various attack vectors, including DDoS. These vendors receive attack traffic information from their customers, enabling them to investigate and enhance their fingerprints and strengthen the collective defense against DDoS attacks.

Overall, collaboration between companies is an important aspect of identifying new attack vectors. Sharing as much information as possible about attacks and attack vectors will benefit all companies in the long run. The shared information must not include any internal company information.

3.6 Mitigations

Mitigating DDoS attacks can be a complex task. While volumetric attacks can often be mitigated on the ISP side, application-layer attacks typically require the deployment of Web Application Firewalls (WAF) or Next-Generation Firewalls (NG-FW). These tools effectively block malicious traffic, but their CPU and network resources are finite. Therefore, the role of DDoS mitigation systems as integral components of network protection cannot be overstated. Most Internet Service Providers (ISP) have their own DDoS mitigation capabilities. These capabilities come from the need to protect the ISP's infrastructure and their customers. Basic protection usually comes from the ISP network protection, but customers must purchase the service if they want more granular protection.

The process of handling DDoS attacks can be the same as that used in other cyber-related attacks. The National Institute of Standards and Technology (NIST) has published a computer incident-handling guide that provides the best practices for handling an incident. This workflow can also be used in the case of a DDoS attack. In Figure 8 Incident Response Lifecycle (Cichonski et al., 2012)- The stages of incident response are divided into four phases.

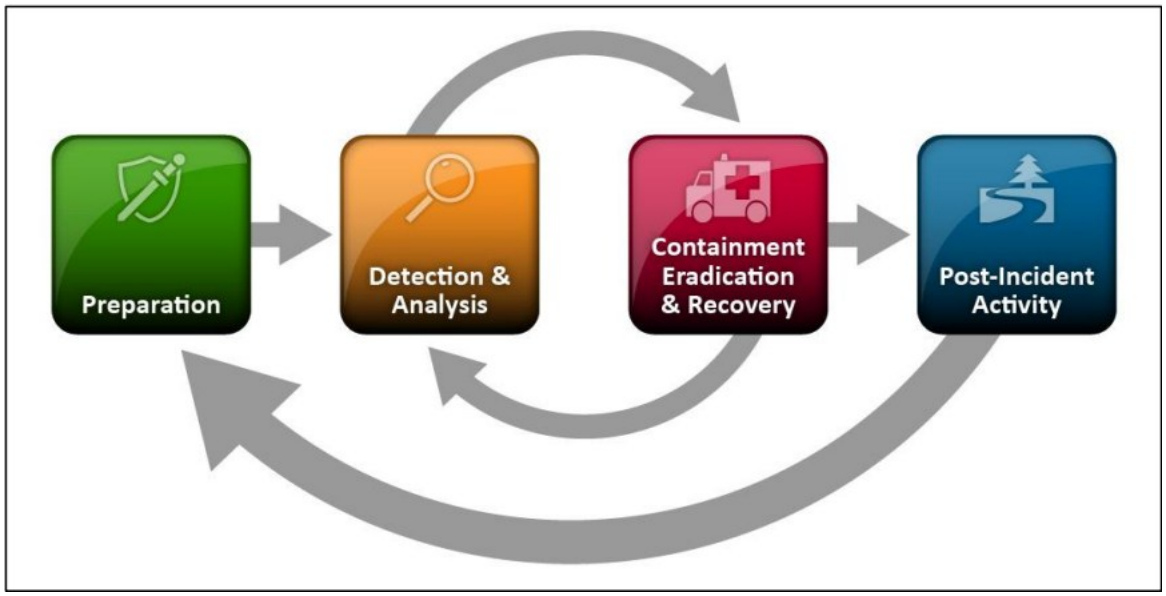

Figure 8. Incident Response Lifecycle (Cichonski et al., 2012)

Examining this lifecycle regarding DDoS attack detection and prevention, the first phase, “preparation,” is usually done with a customer or a stakeholder. The preparation phase is mandatory since the DDoS protection team usually does not have the necessary information on the functionality of the protected asset. In addition to the process described in the NIST computer incident handling guide, the functionalities must be documented to configure the best possible DDoS protection; otherwise, during the mitigation, the protection platform might drop legitimate traffic and make the protected system unusable.

The second part of the lifecycle is detection and analysis. Regarding DDoS attacks, this part mainly collects traffic flow from routers and other network equipment. The chapter describes collecting NetFlow in more detail in Chapter 3.5. Detecting attacks and new attack vectors. Thorough preparation is the key to successful detection and analysis. All IPs and services in the systems must be adequately documented to collect the right NetFlow. Logging practices should be defined and practiced in advance. In case of a DDoS attack that is not “basic,” many actions are taken during the mitigation phase, which should be documented.

In the event of a DDoS attack, the phases of Containment, Eradication, and Recovery come into place. In the attack prevention and mitigation phase, the specialists doing the actual mitigation must log their actions with proper timestamps. The mitigation actions might end up blocking legitimate traffic. Communication with the stakeholders becomes crucial, ensuring the system remains usable.

3.6.1 Scrubbing Centers

The primary function of the scrubbing center is to move all the traffic affected to the scrubbing center with the Border Gateway Protocol (BGP). This example is from NetScout’s Arbor product. The announcement moves all the affected prefix traffic to the Threat Mitigation System. The mitigation system is configured to drop all malicious traffic according to predefined rules. The most common attacks are mitigated automatically since they are usually done with predefined tools such as Low Orbit Ion Cannon (LoIC). LoIC is a tool shared over the internet to make DDoS attacks

and has been widely used. Since the tool is available, protection vendors such as Netscout can analyze it and improve its protection.

3.6.2 Flowspec

Many scrubbing centers can become congested due to the sheer volume of traffic when dealing with massive volumetric attacks. Available scrubbers are often licensed based on the maximum volume of attack traffic they can handle, which can result in equipment failure. A black hole or more advanced version called Flowspec can be used to avoid this congestion.

BGP Flow Specification, or Flowspec, is a BGP router-based method for mitigating DDoS attacks and other unwanted traffic. The traffic is dropped at the network border and will not affect internal traffic. Flowspec consists of more granular routing entries, such as source prefixes, destination prefixes, or network ports. These entries allow routers to have more specific traffic filtering rules.

Flowspec rules can be applied manually, but they are usually announced through BGP Flowspec rules from the Mitigation system to the routers. This allows systems to mitigate even larger attacks automatically. The mitigation is done by dropping unwanted packets from the traffic. As in Blackholing, all traffic is dropped. (Alcatel-Lucent et al., 2014) The components used in Flowspec are shown in Table 1.

Type	Component
1	Destination Prefix
2	Source Prefix
3	IP Protocol
4	Port
5	Destination Port
6	Source Port
7	ICMP type
8	ICMP code
9	TCP flags
10	Packet Length

11	DiffServ Code Point
12	Fragment

Table 1. Flow Specification components (Alcatel-Lucent et al., 2014)

Many current threat mitigation systems can announce Flowspec to routers, automating the entire mitigation process. Typically, these systems are configured so that the scrubbing center handles traffic until it reaches a predetermined threshold. Once the traffic volume exceeds this threshold, the Flowspec is announced for the pre-defined traffic.

It is essential to recognize that the Flowspec filter, while potent, may not always be sufficient to handle all malicious traffic. In such instances, the mitigation system steps in, demonstrating its resilience in further cleansing the traffic before it reaches its destination. This process, though challenging, underscores the system's effectiveness, particularly in the face of constantly evolving cyber threats.

Flowspec, like other mitigation systems, has limitations. The number of Flowspec rules that can be announced in a single router is permanently restricted. These rules also consume resources from the routers, which means that during carpet bombing attacks, the routers might run out of resources. In such cases, announcing a Flowspec rule to a whole /24 block is advisable. Flowspec rules work differently in different vendor routers, and not all routers support all of the components presented in Table 1.

3.6.3 Blackhole

During a significant volumetric DDoS attack, the entire network can become congested. In many cases, other services connected to the same Customer Premise Equipment (CPE) device can be affected, and there is a need to keep other services running in the same network. If the victim is a virtual host, the single virtual machine can consume all the resources from the host device. In this case, one practical way to mitigate the attack is through blackhole routing. Blackhole routing, which routes the traffic to a null route, is a practical and effective solution. Usually, blackholing is done on the ISP side since they have much capacity on their routers. A normal CPE can also make a black hole, but more resources might be needed.

Blackhole was the first way to defend against attacks in Telia, likely in most other ISPs. This was during the early 2000s, when dedicated mitigation systems were not widely available. At that time, the frequency of attacks was low, and Blackhole routing was reasonably practical, implemented as per customer request. However, the need for dedicated mitigation systems became apparent as DDoS attacks became more common.

As demonstrated below, a black hole can be announced in Cisco routers as a null route, providing a practical example of implementing blackhole routing. This is done similarly on other vendor routers. The black hole can be implemented in a peering edge router to have it working inside its own Autonomous System (AS)

Router> enable

Router# configure terminal

Router(config)# ip route 192.0.2.0 255.255.255.0 Null0

Black holes are a good way of protecting a single server or a cluster from becoming unresponsive, but one must note that black holes drop all traffic toward the destination and thus cannot be connected from anywhere.

3.6.4 Application layer mitigations

Most application-layer attacks involve HTTP protocol vulnerabilities. Setting up web server protection can mitigate some of these. For example, Apache server software protects against HTTP exhaustion. The Apache server has a timeout setting in the httpd.conf file, as shown in Figure 9. By default, it is 300 seconds, which makes the server vulnerable to a Slowloris attack and other HTTP connection denial of service attacks. It is recommended that this setting be changed to 60 seconds. This setting must be tested to make the website function properly. (Kumar, 2024)

```
DefaultRuntimeDir ${APACHE_RUN_DIR}

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
# This needs to be set in /etc/apache2/envvars
#
PidFile ${APACHE_PID_FILE}

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100
```

Figure 9. Apache server timeout setting

Microsoft's IIS server also has a Dynamic IP Restrictions setting. This setting can block IP addresses based on the number of concurrent requests or over a period. It also has allowed lists and full support for IPv6 addresses.(Microsoft, 2022)

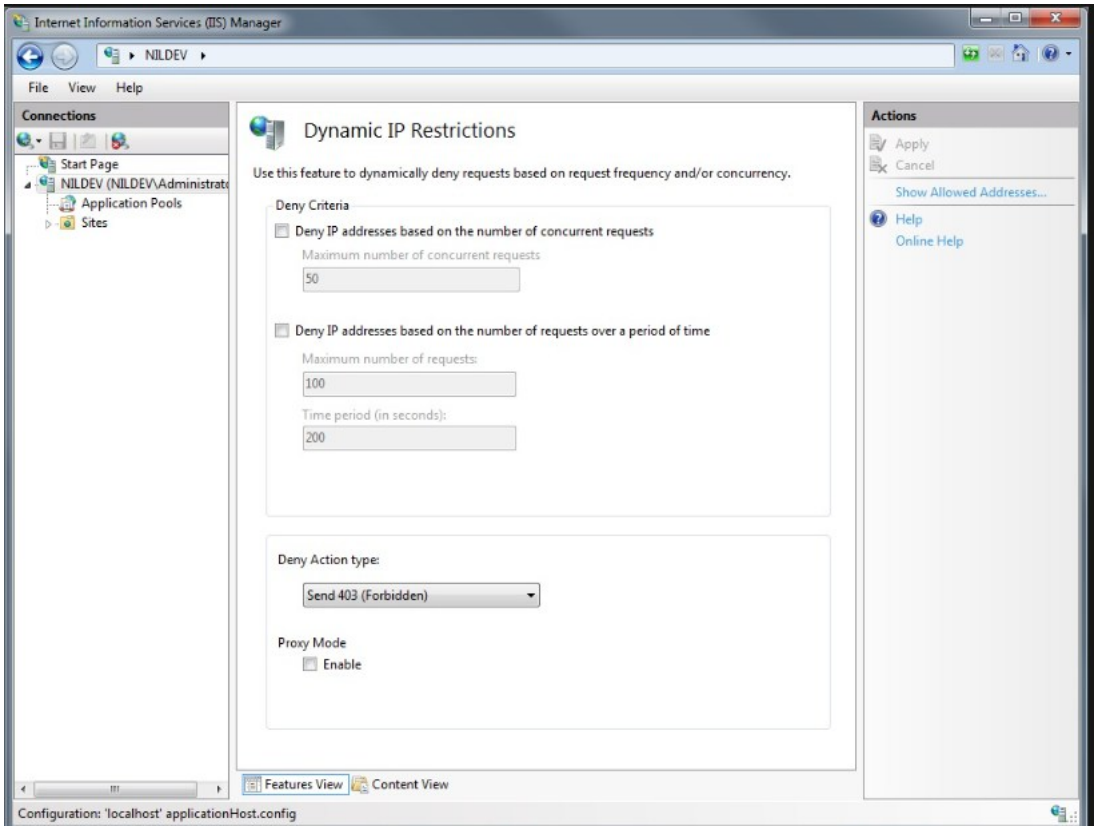

Figure 10. Microsoft IIS Dynamic IP Restrictions (Microsoft, 2022)

3.6.5 Amplification Attacks Mitigation

Mitigating amplification attacks depends on how the victim wants to be mitigated. Usually, a company, maybe a bank or, for example, a webshop, wants its system to stay online no matter what. In this case, the solution for mitigating is a scrubbing center service, which can usually be bought from their ISP. The scrubbing center can drop malicious traffic with predefined rules, such as source port, destination port, packets per second coming from a single host, or packet size. The most common attacks usually do not require interaction with humans, as the systems can mitigate them automatically. If the attack vector is new or the system, for some other reason, does not have the correct fingerprint, there might be a need for human intervention. Protection platforms can be configured with regex functions to better find and drop malicious packets from the traffic.

3.6.6 DNS Water Torture Mitigation

DNS water torture attacks can be mitigated with a scrubbing center by either limiting the number of queries to the DNS servers or by maintaining a list of valid domains on the server and dropping

all unmatched requests. Mitigating DNS water torture attacks has become more complicated in recent years. At first, most of the attacks consisted of fixed-length subdomains, which were easy to mitigate by simply dropping all requests that had that length. In recent years, attack scripts have evolved to more randomized requests requiring more mitigation. Mitigating the newer water torture packets requires the protection device to know all the subdomains in a DNS domain to determine if the request is valid.

3.7 Earlier research of DDoS attacks

Researching DDoS attacks on their own is not typical. Most research, theses, and conference papers related to DDoS focus on cybersecurity within various systems or applications, with one area of interest being the prevention of DDoS attacks or specific aspects of the phenomenon. Cybersecurity vendors and companies that sell devices and services to mitigate DDoS attacks are also involved in this field. Additionally, cloud computing companies regularly publish their quarterly reports on DDoS activities. These reports can be considered research since the companies conduct extensive studies to stay updated on trends, attack vectors, and methods for mitigating attacks. I have used reports from Netscout, Radware, and Cloudflare for this thesis. (Grammarly, 2025)

International conferences and their corresponding publications can be accessed through https://www.ieee.org/. The Institute of Electrical and Electronics Engineers (IEEE) serves as an organization for technical professionals, facilitating the publication and examination of research across various topics. A search for conference papers reveals many research studies regarding DDoS attacks. These studies address a broad spectrum of DDoS-related subjects, ranging from individual attack vectors to comprehensive analyses of the topic. (Grammarly, 2025)

4 Implementation

4.1 DDoS attacks in Nordic countries between 2021 and 2024

DDoS attacks from 2021 to 2024 varied greatly. The year 2021 and the year before were the “normal” attacks, primarily targeting consumer customers such as online gamers. Toward the end of the year, the attacks began to become more complex and volumetric due to the rise of new botnets. A state-sponsored actor created some of the botnets. The year 2022 marked a new era for DDoS attacks, which were primarily conducted by nation-state-sponsored groups.

2021 was the year before russia started the full-scale war in Ukraine. By the end of the year, the attacks increased toward russia's neighboring countries. Most of the attacks conducted during 2021 were, according to Netscout. (2022b), basic UDP, and total traffic attacks. From this, we can assume that professional attackers did not initiate the attacks or were merely probes for what was to come.

The year 2021 was also a year of ransom DDoS attacks, which increased during the fourth quarter of 2021 by 29% (Yoachimik & Ganti, 2022). Netscout also noted this same increase in their 2nd Half of 2021 report. (Netscout, 2022b) The volumetric amplification attacks decreased during the second half of the year 2021.

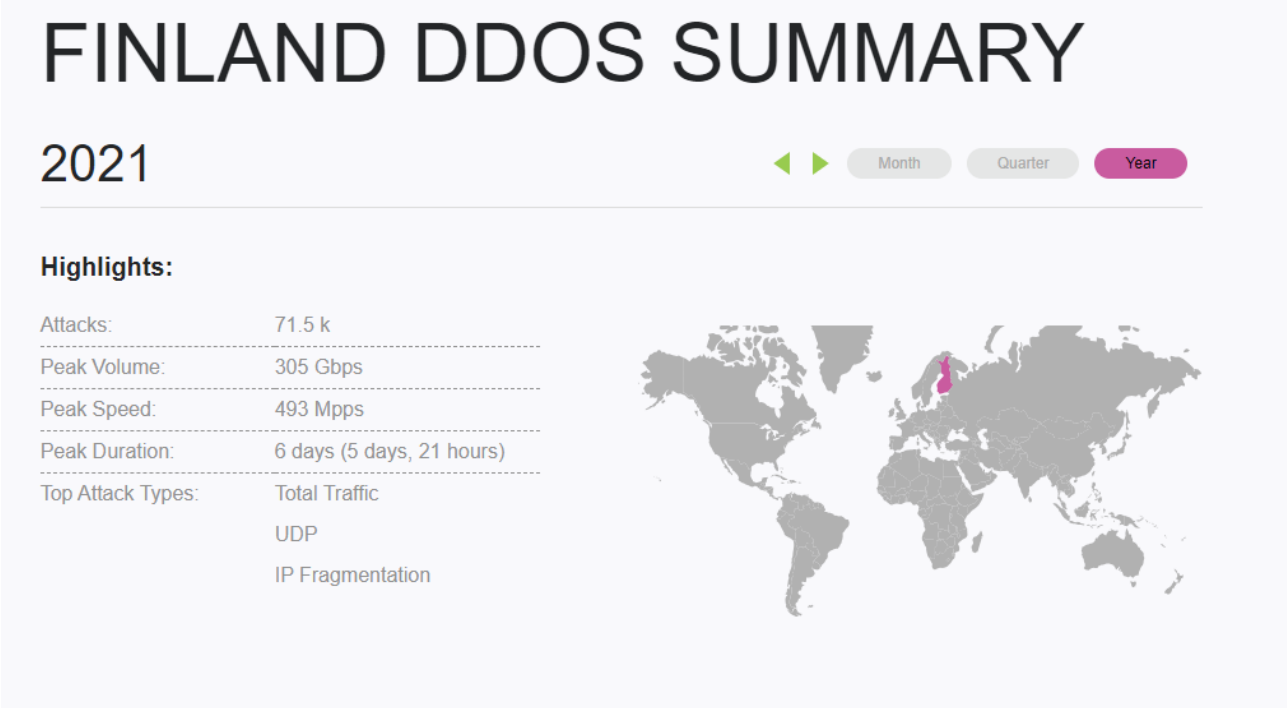

Figure 11. Custom DDoS Summary of 2021 Finland (Netscout, 2024a)

In 2021, most DDoS attacks worldwide were extortion attacks, with petroleum operators in the United States and Canada as the main targets. In the Nordic countries, for example, there were only a few DDoS-related news articles.

4.2 DDoS Attacks During 2021 – 2024 Toward Telia

4.2.1 Attacks During the Year 2021

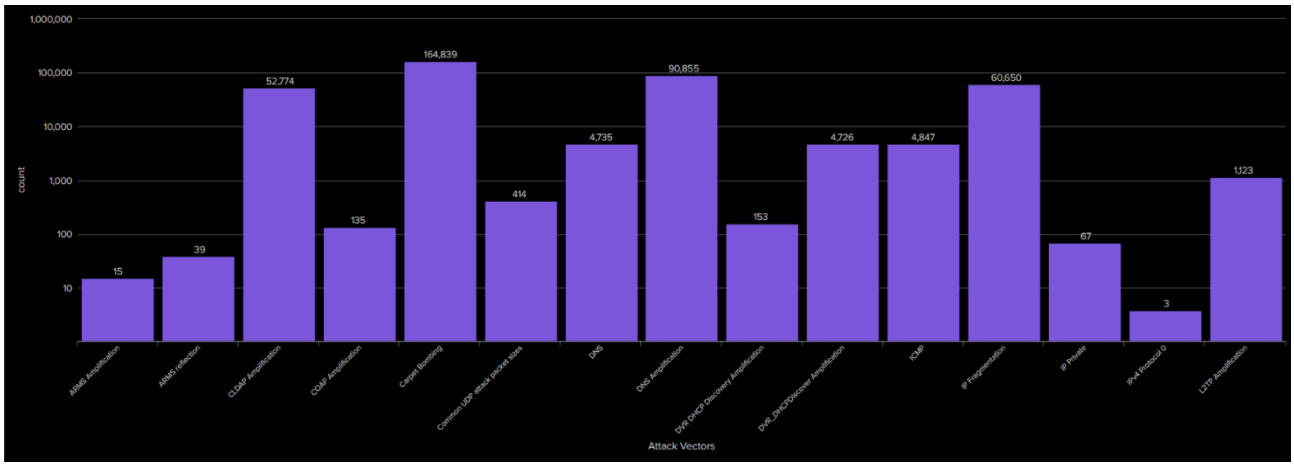

Figure 12. Telia Detected attack Vectors 2021

Figure 12. Telia Detected attack Vectors 2021, the most used DDoS attack vectors were CLDAP, DNS amplification, and IP fragmentation. Even if the amplification attacks were down at the end of the year, the volumetric attack vectors still exist. The attacks most likely were not directed toward Telia itself but were made with online tools that either use botnets or vulnerable DNS servers and are directed toward regular consumers. The motivation behind these attacks is, of course, not known. However, the assumption is that these were targeted private gaming servers or online gamers to gain advantages in various online games (Lucas & Shattuck, 2024). According to the Netscout 2023 threat report press release, gaming and gambling were the main reasons for DDoS attacks. These attacks were motivated by either financial gain or the goal of disrupting competitors.

As mentioned before, the year 2021 was the year before russia started its full-scale invasion of Ukraine. Before the attack, the number of DDoS attacks in the Telia countries was high. Towards the end of the year, the number of attacks decreased, presumably to allocate resources toward Ukraine. As said before, most attacks can only be assumed to be conducted by russian hacker groups as the attacking sources are spoofed or otherwise masked.

4.2.2 Attacks during the year 2022

At the beginning of 2022, russia launched a full-scale aggression against Ukraine. There was a surge in DDoS attacks leading up to the invasion, but these began to decline once Ukrainians relocated their servers outside the country. In the first half of the year, the countries most heavily targeted were Finland and Ireland. (Netscout, 2022a). According to statistics from Telia, the amount of DDoS attacks had already started to decrease at the end of 2021, and significant volumetric attacks were not observed in early 2022. A threat report from Netscout for the first half of 2022 indicated a shift in attack vectors toward TCP SYN/ACK attacks, suggesting that OSI Layer seven attack vectors became the dominant form of attack.(Netscout, 2022a) (Grammarly, 2024)

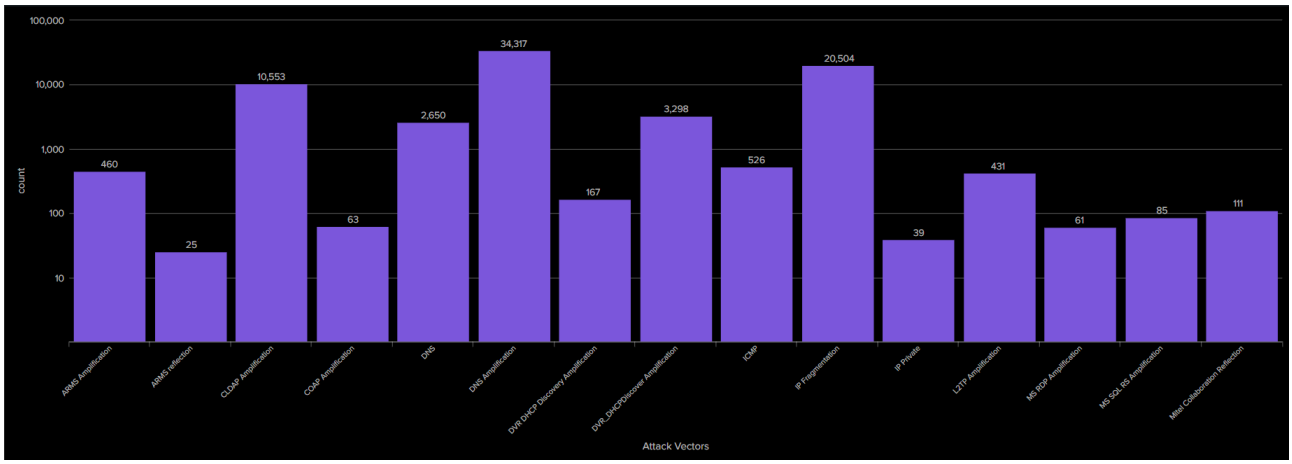

Figure 13. Telia detected attack vectors 2022

4.2.3 Attacks during the year 2023

As Finland joined NATO on 4.4.2023, the DDoS attacks in the Nordic started to rise. The most common attack vector in Telia networks was still a DNS amplification attack, but we started seeing

more and more Carpet-Bombing attacks. The most notable incident in the Nordics was when protesters in Sweden burned a Quran book. Apart from the large protests in Sweden due to this incident, a new hacker group called Anonymous Sudan started attacking Swedish and other Nordic targets. The targets included Schools, transportation companies such as airlines, airports, banks, and national authorities. The attacks usually lasted 24 hours and were conducted using TCP-SYN Flood attacks.

Many different hacker groups back up the hacker group Anonymous Sudan, but what is common in these supporters is their connections to either russia or Islamic countries.

Figure 14. Anonymous Sudan proclamation in Telegram (@Cyberknow20, 2023)

The NoName057 group was responsible for many DDoS attacks in 2023. Most of these attacks were conducted with their botnet, Killnet. Anonymous Sudan also used the Killnet botnet, which was used to attack several Swedish companies and organizations after the incident in which a Muslim holy book, the Quran, was burned in Sweden.

As seen from Figure 13, Telia Attack Vectors Year 2023 DNS-related attacks and Carpet Bombing were the dominant attack vectors. The most prevalent DNS attack type turned out to be a DNS water torture attack, which aimed mainly to target a single organization but was most likely targeted toward Telia DNS servers. As said on page 14, the DNS water torture attack is commonly used toward the DNS resolvers, not the single DNS hosting customer.

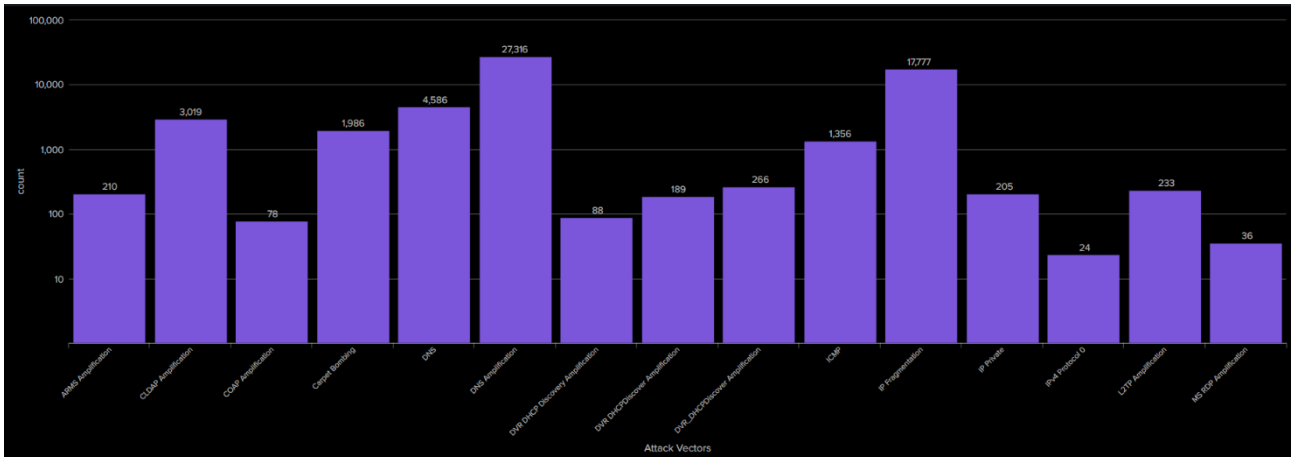

Figure 15. Telia Attack Vectors Year 2023

4.2.4 Attacks during the year 2024

In 2024, nation-state-sponsored attacks continued throughout the year. At the beginning of the year, most attacks targeted DNS servers, which caused some challenges for regular Internet customers.

A new botnet called Gorilla Botnet emerged at the end of 2024 and caused trouble for several companies across Europe. The botnet was created to spread malware that infects computers worldwide and is used for DDoS attacks. The botnet offers at least 19 different types of DDoS attacks, as shown in Figure 16 the domains used by Gorilla Bots were registered in the .su top-level domain, the former Soviet Union's top-level domain.(NCSC-CH, 2024)

ID	Attack Name
0	udp generic
1	udp vse
3	tcp syn
4	tcp ack
5	tcp stomp
6	gre ip
7	gre eth
9	udp plain
10	tcp bypass
11	udp bypass
12	std
13	udp openvpn
14	udp rape
15	wra
16	tcp ovh
17	tcp socket
18	udp discord
19	udp fivem

Figure 16. Gorilla Botnet Attack Vectors (NCSC-CH, 2024)

In the year 2024, the US government reported that they had arrested two Sudanese brothers for running DDoS attacks against various targets across the world. The arrested persons ran under the name of Anonymous Sudan. Anonymous Sudan used the Russian-sponsored Killnet botnet for their attacks and is thus thought to be Russian-sponsored actors. The Anonymous Sudan was taken down after this arrest. (Krebs, 2024)

4.2.5 Timeline

Figure 15, the Total amount of DDoS attacks, presents the number of attacks or alerts in the Telia DDoS protection platform. The data shows a distinct drop in attacks after Q1 2020. The number of detected alerts started to decrease during the year 2021. Definite reasons for this decline are hard

to say. Governments worldwide do a significant job taking down botnets and other known attackers, which might partly explain the gap between the quarters. Also, an aspect worth noticing in this data is the constant development of the platform to keep false positive alerts away from detection. The number of alerts is not usually a factor in the mitigation platforms. A license sometimes limits the overall number of attacks being mitigated, so the calculations must be done thoroughly.

The significant drop in the second half of 2021 might also indicate that the DDoS attackers concentrated their resources on Ukraine and Eastern Europe before russia's full-scale invasion at the beginning of 2022, but the statistics change also due to the continuous development in the detection settings.

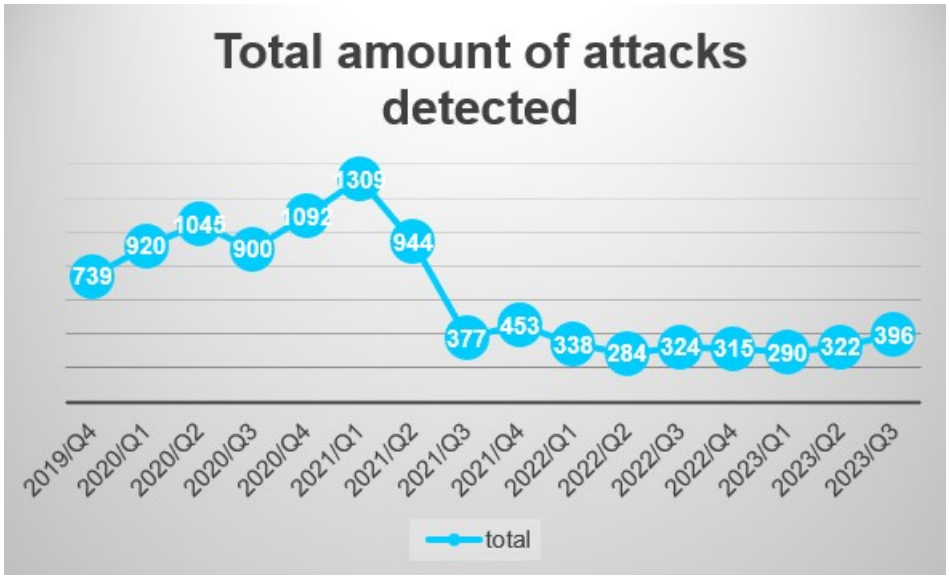

Figure 17. Total amount of DDoS attacks detected in Telia Finland

The most persistent attack vectors have remained consistent for several years: ICMP and DNS amplification. While the number of attacks using these vectors has decreased over time, the continuous development of protection platforms may explain the reduction in these attacks. Additionally, the attack vectors have evolved and become more evenly distributed. It is also important to note

that the number of attacks shown in Figure 17 is recorded only from Finland, whereas Figure 18 represents all Telia Nordic countries combined.

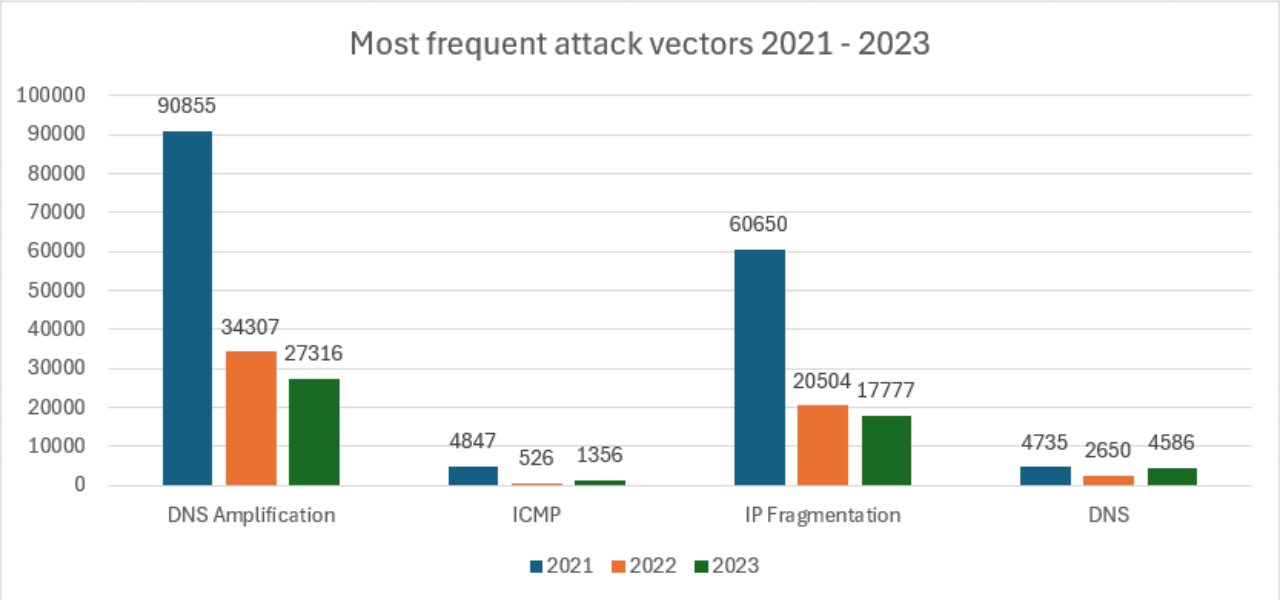

Figure 18. Most frequent attack vectors comparison

4.2.6 DDoS Attack Vectors, Sizes, and Targets

DDoS attacks usually vary by the target and the attacker. In most cases, the most common attack vector is the common vector that is usable at a given time by the network booter services and botnets. The most used attack vector has been many years of DNS-amplification in these most used attacks. The reason for using this is that the attacker must find a usable DNS server over the internet, and in most cases, this can be done with automation. The more sophisticated attack vectors require the attacker to create a botnet by infecting many hosts around the internet to be used as bots. The state-sponsored DDoS actors have their botnets. State-sponsored actors also have lots of resources to develop their botnets and get them to perform better. For example, the No-Name(057) 16 group started to pay everyday internet users in russia to download their botnet connector application to be able to use their bandwidth to conduct attacks.

The attacks with larger bandwidth usually use UDP to get lots of traffic without the synchronization packets of TCP. This allows the attacker to send a large amount of traffic without receiving many return packets. One attack vector shown in the figures in the above chapters is IP fragmentation. IP fragmentation usually uses more than one attack vector, but the packet size has been made larger to get more impact.

4.3 Methods of mitigating DDoS attacks

The DDoS protection platforms have evolved with the attacks over the years. The Basic mitigation flow is presented in Figure 19. Basic Flow of DDoS Detection and Mitigation. The green parts in the flow represent the usual time when the attacks are mitigated automatically. The DDoS protection system is in monitor mode (number 1 in the flowchart) and inspects the traffic from the NetFlow data. When abnormal traffic is detected (2.), the system gives out an alarm and starts an auto-mitigation (4.) according to its configuration. The typical operations in the flowchart are painted green. In typical cases, the essential monitoring and automatic mitigation are sufficient to protect the customer, given that the monitoring and mitigation settings are correctly done. If there is no impact on customer service, the system will automatically end the mitigation.

Figure 19. Basic Flow of DDoS Detection and Mitigation

The red part of the flowchart represents the out-of-ordinary scenarios where the automatic detection either fails to detect the attack, the auto-mitigation does not drop enough malicious traffic, or it drops too much due to a misconfiguration. In these cases, an operator must inspect the traffic and change the auto mitigation accordingly. If there is a misconfiguration in the mitigation, thresholds can be changed. If the mitigation does not drop enough traffic, the attack might be something that has not yet been configured in the system. By inspecting the traffic, the operator finds standard variables in the attack traffic, such as packet length and source or destination port.

For example, the common factor in DNS water torture attacks is the bogus subdomain requested. If the protection system has a list of the correct domains in the target DNS server, it can easily drop the requests not found on the server.

After the mitigation is found to be effective and there is no or little impact on the customer side, it can be left running for the duration of the attack. If the attack vector changes during the attack, the flow returns to traffic inspection and finding common variables or usable threshold changes to mitigate appropriately.

The attack is usually over when the alerts clear on the protection system. After more complicated DDoS attacks, the operators must verify that the attack is over since, in some cases, the attack might have just slowed down under the detection threshold values and is still ongoing. When an attack is over, most systems do an auto report and send it to the stakeholders. As in all cyber-related incidents, a post-incident review must be conducted when targets have been significantly impacted. The post-incident review can be done according to the company guidelines, but it should at least involve information on the following:

- Timeline
- Impacted services
- Mitigation actions taken
- Attack vectors used
- Source information, if it is applicable
- Intelligence on public sources on who might be behind the attack

Reporting the attacks on customers is mainly done automatically by the protection platform. The reports usually consist of attack vectors, source countries, and the amount of traffic received, mitigated, and passed through to the customer. These reports should give the customer and DDoS protection professionals an insight into how the protection system performs and if it needs to be tuned for future attacks. In most cases, the attack traffic leaked to the customer is due to changes in their network that have not been applied to the protection platform. Documenting and sharing information between the customer and the protection company is crucial to mitigate attacks effectively.

4.4 Mitigating DDoS Attacks in the Future

DDoS protection vendors have visibility to DDoS attacks globally, and with this information, they are developing tools to block unwanted traffic. Cloudflare reported in 2024 that almost 7% of all internet traffic is malicious (Schneier, 2025). Internet service providers are the most critical factor in blocking this traffic. Stopping it is not the most straightforward task; it also blocks unwanted traffic in most cases.

Predicting the future of mitigating DDoS attacks is challenging. While artificial intelligence (AI) and machine learning may help identify patterns to block malicious traffic, human intervention is often necessary. Human-created block lists and filters are crucial in effectively combating these attacks. (Grammarly, 2024)

Artificial intelligence can be used in the botnets' Command-and-Control (C2) servers to enable fast response to mitigation action. AI can also detect services vulnerable to DDoS faster.

4.4.1 Risk Management

Organizations should consider implementing an ISO 27001 certificate to prepare for cyberattacks, including DDoS attacks, effectively. While the certificate does not provide direct protection, the proper tools and controls can make a significant difference when implemented correctly. Since ISO

certificates can be costly, smaller organizations could implement the ISO controls without certification. This will be helpful in the future if customers, etc., require certification.

Building a risk management system within the organization is an excellent starting point. This can be done using a simple Excel sheet, but advanced software options can aid the process. A risk management system should include a list of identified risks, their impact assessments, and, most importantly, the strategies for mitigation. (Grammarly, 2025)

The entire organization must commit to identifying all information security risks, including DDoS-related risks. The risks must be reviewed periodically to ensure that every risk is either mitigated or at least acknowledged. The organization's commitment should include C-level management to ensure adequate resources and budget for mitigating these risks.

The risks involving DDoS attacks can vary. Most companies must acknowledge that their web shops and other web-related services are at least in some way vulnerable to Denial-of-Service attacks. Most companies rely on internal systems such as HR, email, and file storage for external services. These systems should also be noted as a potential risk for DDoS, and the vendors should be required to present their ways of mitigating the DDoS attacks, among all other information security controls. Figure 17 Risk list for consideration in the risk identification process This figure gives some ideas on risks identified across different organizations. It can be used as a baseline for risk identification.

Suggested risk list related to DDoS	**Risk explanation**
Network congestion by a significant attack	Network congestion can be significant; in the worst case, it can take the whole organization offline.
Financial losses	The organizations' webshops or other services are down. This quickly leads to financial losses since the customer does not get the service or the products.
Reputational damage	The organization's reputation might be damaged due to unplanned downtime.

Increased operational costs	Operational costs might increase due to a DDoS attack. If there is a pay-as-you-go subscription, the costs might come from the cloud provider. Other operational costs might include additional help purchased from protection vendors.
Legal and regulation risks	Suppose an organization has obligations from the government, etc. A DDoS might have legal consequences.
Data breach	In some cases, DDoS attacks are used as a screen to get the company's security's attention elsewhere while attacking a different server.

Table 2. Risk list for consideration in the risk identification process

4.4.2 NIS2 compliance in the EU

At the beginning of 2023, the European Union enforced the Network and Information Security (NIS2) Directive on member states. While it has similar controls as ISO 27001, this directive aims to enable the essential entities within the member states to have baseline protection against cyber threats. This directive applies to the essential organizations of EU member states regarded as either important or essential to the said state's functions (Traficom, 2024).

The directive ensures that the organizations are up to date for protecting critical functions of society.

The ten key items in the directive, according to Traficom, (2024) are:

1) policies on risk analysis and information system security;

2) incident handling;

3) business continuity, such as backup management, disaster recovery, and crisis management;

4) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

5) security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure;

6) policies and procedures to assess the effectiveness of cyber security risk management measures;

7) basic cyber hygiene practices and cyber security training;

8) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

9) human resources security, access control policies, and asset management;

10) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

As mentioned in chapter 4.4.1 The NIS2 directive also emphasizes risk management in the cyber domain. The regulations in the EU and at the country level are constantly evolving, and organizations should keep their documentation up to date to make it easier for them to comply with new demands.

5 Conclusion

Table 3. Benchmark on the results Table 3 represents the benchmark on the results of this thesis, which will be opened in the sub-chapters below.

Benchmark on results			
Stakeholder			
	Recommended Protection	**How to detect future DDoS**	**How to Mitigate / Prevent Future DDoS Attacks**
Government agencies running production on-premises	ISP level protection	New attack vectors might be challenging to detect and require constant monitoring. Machine learning and Artificial Intelligence might help find new vectors from the vast amount of data collected over the Internet.	Keep track of the Internet forums for intelligence.
Internet service providers	ISPs need protection to keep the networks operational. A DDoS attack cannot affect customer service. Scrubbing centers and Flowspec need to be configured appropriately.	AI or machine learning might help detect standard variables in attack traffic.	Continuously enhance the protection and verify its effectiveness with internal and external customers. Post-incident reviews and AI?
Businesses	depending on the IT infrastructure and identified risks. Usually, the ISP-provided protection service is enough	Logging of traffic. The traffic logs help identify new attack vectors and make mitigations more effective	Verify protection with the provider and keep the IT environment properly documented
End users	ISPs should offer essential DDoS protection to their consumer customers. Regular users might experience basic DDoS if they are active in internet gaming or gambling.	Must rely on ISP	

Table 3. Benchmark on the results

5.1 How have DDoS Attacks changed over the years

DDoS attacks have been around for years, but they are constantly evolving. As stated before, the attacks depend on the targets and their infrastructure. The evolution from script kiddies' extortion attacks toward different organizations to gain financial benefit to attacks on society's backbone, such as banks and government websites, aims to cause uncertainty and confusion in people. Nation-state-sponsored actors promote the agenda of the states. One example of this is the attacks on Sweden and Finland before they joined NATO.

The political situation worldwide, particularly in Europe, has altered the nature of attacks, which now target critical services for society. Key targets include financial institutions, transport companies, and ISPs. Many nation-state-sponsored attackers often aim to create uncertainty among the general public. For instance, the russian influence policy seeks to sway opinions on various topics, such as NATO and the war in Ukraine.

The attacks have been around for a long time, and as they are evolving, there are still old attack vectors used, as can be seen from the Figure 20. Flooding attacks are still valid since they congest the networks, and DNS and NTP amplification attacks can still be carried out since the vulnerable servers they use constantly come online. Their usage in the attacks is possible due to configuration errors.

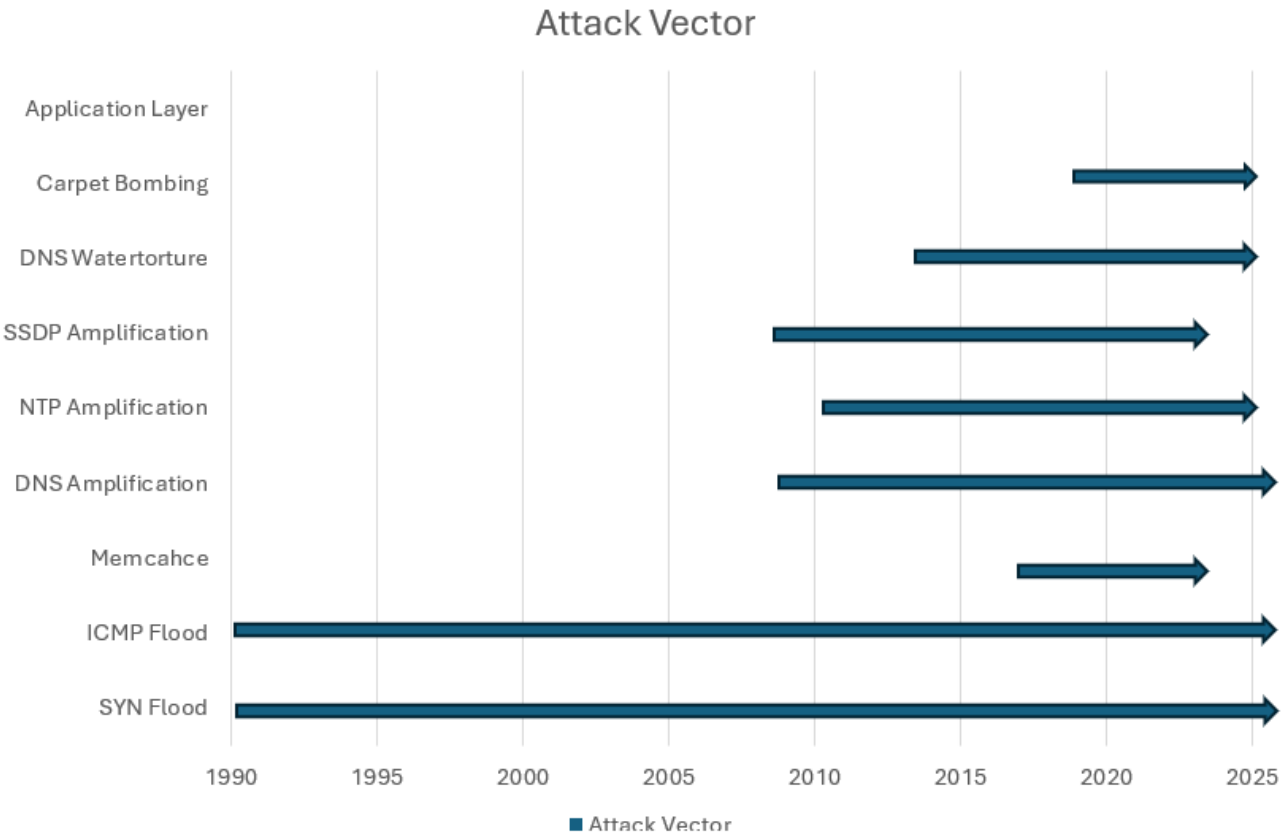

Figure 20. DDoS attacks over the years

5.2 Predictions and precautions for the future

As in all matters, predicting the future is not easy. Multiple variables affect the conclusions, and there is no sure way of predicting. DDoS attacks and botnets conducting them will continue to evolve. AI will be a new way of controlling botnets and vectors. AI will help attackers develop new ways of attacking different online platforms without the current protection systems detecting the attacks. Protection providers and vendors are creating more intelligent ways of detecting attacks and implementing AI or machine learning to detect malicious traffic patterns. As a prediction from the literature reviewed in this thesis, the old attack vectors are still valid, and more intelligent attacks are changing the attack vector dynamically to keep the victim down as long as possible. Artificial Intelligence will detect the protection measures enabled and change the attack vector accordingly. The attackers will also use AI to create new attack vectors by making it evaluate the systems over the internet.

Mitigating these new DDoS attacks will require greater intelligence from the vendors, who will gather more information than their customers. This would enable the protection platforms to detect traffic from known botnets and threat actors. So, even if the platform cannot detect the actual attack, there would be an indication of an attack based on the traffic received from the botnets. As always, this type of protection likely requires new equipment and software from the vendors, which will come at a cost. A thorough review is needed to determine if the protection is worth the extra expense.

IoT-related botnets have been used for DDoS attacks in recent years. The main reason for this is that many IoT devices are not adequately secured, and their vulnerabilities are exploited for these attacks. The main vulnerability in these devices is the use of default passwords, so the attacker can quickly get access to many devices. Securing these devices is a vital precaution for preventing future DDoS attacks. The Mirai Botnet was one of the first ones to use IoT devices in 2016. The use of IoT botnets will continue to rise, and new botnets will be taken into use. (Gelgi et al., 2024)

5.3 How to Mitigate Future DDoS Attacks

Attackers frequently find new attack vectors by scanning and assessing their botnets. Old attacks are not going anywhere soon. For example, many vulnerable servers on the Internet can still be used in amplification attacks. New servers are being implemented constantly, and the attackers do constant scans to find them to use in their attacks. For example, many internet DNS servers are not protected enough to not send all their data toward a victim during a DNS Amplification attack. In most cases, these servers are unaffected by the attack since they only send the traffic to the victim server, so the administrators might not even know that their server is used in this kind of attack. This is also why companies should have an abuse team to get emails and notifications if their servers are used in DDoS attacks or other malicious activities.

Company threat intelligence should be highly valued. Many threat actors must keep an online presence to make their DDoS attacks as effective as possible. The botnets used in the attacks must be run by a command-and-control server (C2), which, in some cases, can reveal the botnet's future targets.

As with current protection, future protection starts with adequately documenting and maintaining the organization's IT infrastructure. The documentation should be updated to ensure that all stakeholders in the protection know what they are protecting. Suppose there is a miscommunication between the DDoS protection and the IT infrastructure. In that case, it can lead to many false-positive alerts and unnecessary mitigations, disrupting the system's normal operations.

5.4 Future DDoS Attack mitigation and prevention survey

Some DDoS protection specialists were sent a survey to gain a more advanced view of DDoS's future. The questions asked were:

- What is your prediction of where the DDoS attacks will evolve in the next 2 years?
- What is the best way of preventing DDoS attacks?
- What is the best way to mitigate DDoS attacks?

The questionnaire was delivered to people working with DDoS protection to get valid answers. As in all questionnaires, these answers had some joke answers. Among them, an answer to the question “What is the best way to mitigate DDoS attacks?” was “pull the plug.” As this is a joke answer, it comes from an actual way of mitigating an attack, a black hole. Additionally, this answer suggests methods for preventing attacks and keeping all possible IT infrastructure components off the public internet through the use of firewalls, etc.

What is your prediction of where the DDoS attacks will evolve in the next 2 years?

The predictions about future DDoS attacks contain many similarities to what has been previously written in this paper. Primarily, the attacks are shifting from UDP-based protocols to TCP-based ones, which can be more challenging to detect and mitigate in some cases. The attacks are evolving. More sophisticated attack vectors may become available in network stressers or booter services. This allows anyone to carry out more complex attacks against anything online while moving away from basic UDP volumetric attacks.

What is the best way of preventing DDoS attacks?

As mentioned, there is no single best way to prevent the attacks. One tongue-in-cheek response to this was not to have an online presence. This needs to be considered when building IT infrastructure so that only the systems that require an outside connection are provided with one. The internal company networks should be hardened so that potential attackers cannot detect them by scanning. This is usually achievable, for example, with a Next-Generation Firewall.

According to the survey, it is essential to have protection from the ISP and to secure the networks promptly once attacks are detected. ISP protection needs extensive documentation and testing before it is considered adequate.

What is the best way to mitigate DDoS attacks?

As stated earlier, there is no single “silver bullet” for mitigating all potential methods of DDoS attacks. According to the survey, the future of DDoS attacks will lean toward more complex strategies, complicating mitigation efforts. The survey responses indicated that all resources must contribute to mitigations. These resources include ISP scrubbing centers, firewalls, and WAFs. Each must be appropriately configured to manage its role in the mitigation process. ISPs will handle most volumetric attacks, but for application-layer attacks, the final segment of the connection must be protected with a WAF and firewall. To enable the best possible mitigation, all components of the IT environment must be thoroughly documented to the level of the IP address and port used, ensuring that protection configurations can be implemented as quickly as possible.

6 Discussion

DDoS attacks are here to stay and will continue to evolve. Luckily, many internet service providers, protection providers, and other cybersecurity-related companies are continuously researching the topic.

6.1 Reliability of the research data

The data provided by different vendors can be trusted, but the challenge is that the providers will only see the data coming from their customers. Due to security and confidentiality reasons, the providers cannot receive complete information on single DDoS attacks, only the duration, country, and attack vector. This data is a good starting point but does not cover all aspects of the DDoS world. Partial data always influences the reliability of the study. However, since most data is gathered from different sources, the final data can be considered a good basic knowledge on the topic.

6.2 Ethical review

This thesis collects data from various protection providers, including cloud services and security equipment vendors. The data represents merely what a single vendor can detect and is closely tied to customers in different countries. The information is gathered anonymously to safeguard the privacy of customer data. As an ISP, Telia also does not provide user IP addresses or any other personal information to vendors, so the data mainly consists of attack vector information, duration, and the volume of a particular attack. Personal data is regulated in the EU by the GDPR, and companies could face severe penalties if they share it for some reason. Despite its limitations, this data is essential in researching DDoS attacks and new possible ways of detecting and mitigating them.

6.3 Sustainability

However, DDoS protection is primarily done to protect companies and organizations. Another perspective on protection is the durability of humans as users of Internet services. At least in the case of state-sponsored groups making DDoS attacks, the aim is seldom to gain profit but to disrupt the services to create confusion and uncertainty. There is also this social aspect to preventing these

attacks, to keeping societies running normally and not letting the attacks make people uncomfortable.

Since almost everything is connected to the internet in one way or another, the disruptions caused by DDoS attacks can vary significantly. On the one hand, the impact may be on the financial well-being of individuals, and on the other, critical infrastructure, such as water and electricity, can be disrupted. Water infrastructure or electric infrastructure malfunction can also cause environmental effects, in which case the impact moves from the virtual world to the real world. The ecological effects are often highly hypothetical but not entirely impossible.

6.4 Future research

DDoS attacks have a vast number of different variables to study. Most protection vendors research to better protect their customers. However, although interesting topics exist, academic studies of DDoS are not often conducted.

One of the most intriguing areas for future research is undoubtedly DDoS and AI. Artificial intelligence needs to be implemented to defend against DDoS. AI can assist in detecting new attack vectors and even help in studying new ways to mitigate the attacks.

Research or evaluation of the available tools must be continuous for companies that offer protection. Attacks and protection methods evolve quickly, and new methods usually result in operational costs. The available resources must follow the new ways of detecting and mitigating since overusing detection and mitigation can make the process too stiff or costly.

References

A10. (2024). *What is a Volumetric DDoS Attack?* https://www.a10networks.com/glossary/what-is-a-volumetric-ddos-attack/

Alcatel-Lucent, Bookham, C., & Alcatel-Lucent (Firm). (2014). *Versatile Routing and Services with BGP Understanding and Implementing BGP in SR-OS* (1st ed). Wiley. https://ja-net.finna.fi/Record/jamk.993620534906251

AWS. (2024). *DDoS Simulation Testing Policy*. https://aws.amazon.com/security/ddos-simulation-testing/

Bienkowski, T. (2024, January 26). *Application Layer DDoS Attacks*. https://www.netscout.com/what-is-ddos/application-layer-attacks

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide*. NIST. https://doi.org/10.6028/NIST.SP.800-61r2

Cloudflare. (2024a). *NTP amplification DDoS attack*. https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/

Cloudflare. (2024b). *SSDP DDoS attack An SSDP DDoS attack exploits vulnerabilities in Universal Plug and Play.* https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/

Cloudflare. (2024c). *What is a DDoS booter/IP stresser?* https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/

@Cyberknow20. (2023, February 18). *Anonymous #Sudan claims there will be "huge outages" across #Sweden* [Tweet]. https://x.com/Cyberknow20/status/1626721152856121346

GeeksforGeeks. (2024, December 27). *TCP 3-Way Handshake Process*. https://www.geeksforgeeks.org/tcp-3-way-handshake-process/

Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., & Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors*, *24*(11), 3571. https://doi.org/10.3390/s24113571

Impreva. (2024). *Ping of Death (POD)*. https://www.imperva.com/learn/ddos/ping-of-death/#:~:text=The%20Ping%20of%20Death%20was%20first%20presented%20in,it%20also%20affected%20many%20router%20and%20firewall%20vendors.

Kali.org. (2024). *Hping3*. https://www.kali.org/tools/hping3/

Kenig, R. (2013, May 14). *How Much Can a DDoS Attack Cost Your Business?* https://radware.com/blog/security/how-much-can-a-ddos-attack-cost-your-business/#:~:text=The%20Ponemon%20Institute%20study%20estimates%20that%20the%20average,DDoS%20attack%2C%20this%20amounts%20to%20a%20heavy%20toll.

Kerkkänen, T. (2016, October 30). *Motiivina hillitön pätemisen ja rahan tarve – Näin teinihakkerit kaatoivat OP:n verkkopankin*. https://yle.fi/a/3-9258886

Krebs, B. (2024, October 17). Sudanese Brothers Arrested in 'AnonSudan' Takedown. *Krebsonsecurity.Com*. https://krebsonsecurity.com/2024/10/sudanese-brothers-arrested-in-anonsudan-takedown/

Kumar, C. (2024, September 28). *Apache Web Server Hardening and Security Guide*. Apache Web Server Hardening and Security Guide. https://geekflare.com/apache-web-server-hardening-security/

Lucas, C., & Shattuck, C. (2024, April 25). *Geopolitical Unrest Generates an Onslaught of DDoS Attacks, According to the Latest NETSCOUT Threat Intelligence Report*. Press Release.

Microsoft. (2022, March 22). *Using Dynamic IP Restrictions*. https://learn.microsoft.com/en-us/iis/manage/configuring-security/using-dynamic-ip-restrictions

Mohan, D. (2024, January 23). *What Are CLDAP Attacks? What Are The Risks And Impacts Of Such Attacks?* https://prophaze.com/blog/what-are-cldap-attacks/

NCSC-CH. (2024, October 10). *Technical Analysis of Gorilla Bot*. National Cyber Security Center Switzerland. https://github.com/govcert-ch/CTI/blob/main/20241010_GorillaBot/20241010_NCSC-CH-GorillaBot.pdf

Netragard. (2024). *Inside the 2020 Ping of Death Vulnerability*. Netragard. https://netragard.com/inside-the-2020-ping-of-death-vulnerability-2/

Netscout. (2022a). *FINDINGS FROM 1ST HALF 2022 NETSCOUT DDoS THREAT INTELLIGENCE REPORT*. https://www.netscout.com/resources/threat-report/netscout-ddos-threat-intelligence-report-1h-2022-highlights

Netscout. (2022b). *ISSUE 8: FINDINGS FROM 2ND HALF 2021*. Netscout. https://www.netscout.com/sites/default/files/2022-03/ThreatReport_2H2021_WEB.pdf#:~:text=NETSCOUT%20THREAT%20INTELLIGENCE%20REPORT.%20NETSCOUT%20Omnis%20Threat%20Horizon.

Netscout. (2024a). *Custom DDoS Summary 2021, Finland*. https://horizon.netscout.com/?atlas=summary&filters=destination.region.SE-destination.region.FI-destination.region.NO-destination.region.DK&y=2021

Netscout. (2024b). *DDoS Threat Intelligence Report Revealing Adversary Methodology*. https://www.netscout.com/threatreport/revealing-adversary-methodology/

Netscout. (2024c). *NETSCOUT DDoS THREAT INTELLIGENCE REPORT / FINDINGS FROM 1ST HALF 2023*. https://www.netscout.com/threatreport/ddos-attack-vectors/

Netscout. (2024d). *What Is a Reflection/Amplification DDoS Attack?* https://www.netscout.com/blog/what-reflection-amplification-ddos-attack

Netscout. (2024e, February 24). *Slowloris DDoS Attacks*. https://www.netscout.com/what-is-ddos/slowloris-attacks

Netscout. (2024f, March 2). *Defending Against Carpet Bombing DDoS Attacks*. https://www.netscout.com/use-case/carpet-bombing-attacks

Patil, A. (2023). The cyberwar has expanded rapidly beyond Ukraine and Russia, new data shows. *New York Times (Online)*. https://www.proquest.com/docview/2831502944?parentSessionId=VFIu-KaoaEo21f6SJ6CO4ufYL%2FbTe%2FQLnCT6ZuRSXWIk%3D&accountid=11773&sourcetype=Blogs,%20Podcasts,%20&%20Websites

Petryschuk, S. (2024, September 26). *NetFlow Basics: An Introduction to Monitoring Network Traffic*. https://www.auvik.com/franklyit/blog/netflow-basics/

Phoenixnap. (2024). *What is a Domain Name System (DNS) & How Does it Work?* https://phoenixnap.com/kb/what-is-domain-name-system#:~:text=The%20DNS%20space%20uses%20a%20client-server%20architecture%3A%201,used%20system%20component%20%28e.g.%2C%20through%20a%20browser%29.%20

Radware. (2024). *DDoS Attacks History*. https://www.radware.com/security/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/

Sagatov, E., Mayhoub, S., Sukhov, A., & Calyam, P. (2023). Countering DNS Amplification Attacks Based on Analysis of Outgoing Traffic. *Journal of Communications and Information Networks*, *8*(2), 111–121.

Sockrider, G. (2024). *Every 3 Seconds: The Evolution of DDoS Attacks*. https://www.netscout.com/blog/every-3-seconds-evolution-ddos-attacks

STT. (2017, May 12). *Oikeus tuomitsi 20-vuotiaan miehen ehdolliseen vankeuteen palvelunestohyökkäyksistä – Kohteina pankit ja mediat*. https://yle.fi/a/3-9963284

Traficom. (2024, April 11). *Important information on the European Union Cybersecurity Directive (NIS2)*. https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/important-information-european-union-cybersecurity

Yoachimik, O., & Ganti, V. (2022, October 1). DDoS Attack Trends for Q4 2021. *The Cloudflare Blog*. https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/

Appendices

Appendix 1. Approval and evaluation comments from the commissioning company representative

Telia has ordered this thesis to be able to get internal study material on Distributed Denial of Service attack detection, mitigation, and protection to be used as insight, training, and awareness material for DDoS Protection contributors, stakeholders, and wider internal audience at Telia. This thesis provides Telia with a thorough view of the attacks and how and why they occur. The Risk Management chapter provides a good reference on how to better prepare the businesses' resilience for possible upcoming DDoS campaigns.

This thesis also provides valuable insights for the cyber community, addressing a topic with limited literature. DDoS has been employed as a tool for hybrid warfare, and this has been seen in the Ukraine war in recent years. DDoS has also been used as retaliation for countries and companies supporting Ukraine, so sharing information is crucial.