UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

Resilience to DDoS attacks

João Ye

Mestrado em Segurança Informática

Dissertação orientado por:
Prof. Doutor Mário João Barata Calha

2022

Agradecimentos

Gostaria de começar por agradecer à minha família, principalmente, aos meus pais, Ye Boguang e Wu Yongjuan, que com os seus esforços garantiram-me que conseguisse completar esta grande etapa da minha vida.

Agradecer à Rute Guerreiro, Gonçalo Correia e avô Ida por me suportarem nos meus problemas e incertezas que foram decorrendo ao longo do meu percurso académico. Sem o vosso suporte muito dificilmente conseguiria alcançar este novo marco da minha vida.

Quero deixo um agradecimento às pessoas que continuam a fazer parte da minha vida, mesmo antes de começar este percurso académico, fazendo com que nunca me sentisse sozinho e que conseguisse superar quaisquer adversidades e preocupações da vida académica. Principalmente ao António Sousa, Gonçalo Vieira, Marta Martinho, Rita Salvador, Rúben Vinagre e Tomás Pinto que me ajudaram a suportar a solidão durante a pandemia.

Agradecer aos meus amigos, David Silva, Eduardo Pereira, Inês Sousa e Raúl Koch que estiveram presentes ao longo dos meus 5 anos académicos. A vossa presença e apoio fez com que não existissem impossíveis. A minha experiência académica, com vocês, não poderia ter sido melhor.

Quero também agradecer ao meu coordenador da EY, Sérgio Sá, que me acompanhou ao longo da dissertação e que me ajudou quando precisei.

Um enorme obrigado ao meu orientador Prof. Dr. Mário Calha que me orientou da melhor forma possível e acompanhou o desenvolvimento da minha dissertação, indicando os melhores caminhos a seguir para que não terminasse este percurso académico com arrependimentos.

Por fim, quero agradecer a todas as outras pessoas que cruzaram comigo durante o meu percurso académico.

Para a minha família e amigos

Resumo

Os ataques de negação de serviço *(Denial of Service* - DoS), ao longo dos anos, têm evoluído para ataques mais sofisticados, perigosos e mais furtivos, originando assim, os ataques de negação de serviço distribuído (*Distributed Denial of Service* - DDoS), o que adicionou uma nova dimensão, em que múltiplas máquinas atacam uma única vítima, em vez de o ataque ser feito por apenas uma máquina, como acontece em ataques de DoS.

O principal objetivo dos atacantes ao realizarem ataques de DoS e de DDoS, é perturbar e interromper os serviços fornecidos pelas vítimas, através do consumo de todos os recursos, tais como a largura de banda da rede e recursos dos servidores (CPU, memória, entre outros) disponíveis nos seus servidores e dispositivos.

Atualmente, existe um grande número de diferentes tipos de ataques de DDoS que exploram diferentes vulnerabilidades, principalmente nos protocolos de comunicação mais utilizados na Internet, como por exemplo os protocolos TCP e UDP.

Um exemplo real que demonstra como estes ataques de DDoS conseguem provocar grandes danos às empresas, foi o ataque realizado ao fornecedor de serviços Dyn, em outubro de 2016, que utilizou a botnet Mirai para criar um ataque que alcançou um volume de tráfego de 1.1 Tbps.

Outros dois exemplos de ataques que ocorreram recentemente, tiveram como alvo a Microsoft e alcançaram volumes de tráfego de 2.5 Tbps e 3.47 Tbps. A Microsoft informou que conseguiu mitigar os ataques não tendo sido causado danos. O ataque de 3.47 Tbps foi reportado em novembro de 2021, tendo como origem 10,000 diferentes dispositivos distribuídos por diversos países, tais como China, Rússia e India.

Com estes ataques, Dyn em 2016 e Microsoft em 2021, pode-se verificar que estes ciberataques continuam a evoluir, tornando-se cada vez mais sofisticados, sendo assim crucial que as empresas continuem a investir na sua cibersegurança, de forma a aumentar a robustez e a resiliência perante ataques desta dimensão.

Adicionalmente, com as pesquisas realizadas, verificou-se que não existe um documento disponível e acessível na Internet que descreva de forma detalhada as ferramentas que as empresas devam utilizar para se conseguirem proteger contra ataques de DDoS.

Portanto, verificou-se assim a necessidade de construir uma *framework* para auxiliar as empresas na tomada de decisão das soluções de DDoS que deverão implementar fazendo com que desenvolvam a sua robustez e resiliência contra ataques de DDoS.

Este trabalho iniciou-se com o estudo da arquitetura dos ataques de DDoS, onde se verificou que é constituída por quatro componentes, sendo estes, o botmaster (i.e., o ator malicioso que coordena e ordena o ataque), o servidor de Comando e Controlo (*Comand and Control* - C&C) que controla os agentes, os agentes (i.e., bots) que são dispositivos infetados que executam o ataque de DDoS e a vítima que é a entidade que sofre o ataque.

O fluxo de execução de um ataque de DDoS envolve quatro fases, que são o Recrutamento, Exploração e Infeção, Comunicação e Ataque.

A fase de Recrutamento acontece quando o atacante utiliza diferentes técnicas e estratégias para encontrar novos dispositivos considerados vulneráveis. Existem duas estratégias que o atacante pode utilizar para encontrar dispositivos, *host scanning* e *vulnerability scanning*.

Após serem descobertas as máquinas vulneráveis, é necessário explorar a vulnerabilidade identificada e infetar o dispositivo, tornando-os em agentes. O código malicioso utilizado para infetar o dispositivo pode ser propagado de três formas diferentes, *Central Source Propagation*, *Back-Chaining Propagation* ou *Autonomous Propagation.*

O atacante, ao possuir um conjunto significativo de dispositivos infetados, utiliza o servidor C&C para comunicar com os agentes, de modo que estes iniciem a execução do ataque de DDoS à vítima especificada pelo atacante, sendo estas as últimas duas fases do fluxo.

Depois de descrever como é efetuado o processo dos ataques de DDoS, é importante salientar que é possível categorizar os diferentes tipos de ataques de DoS e DDoS de diferentes formas. As duas formas de categorização são Esgotamento da Largura de Banda e Esgotamento de Recursos ou Ataques baseados em volume, Ataques de Protocolo e Ataques de Aplicação.

Na categoria de Esgotamento da Largura de Banda e Esgotamento de Recursos, os ataques classificados como Esgotamento da Largura de Banda são aqueles que têm como objetivo consumir a largura de banda da vítima, enquanto os ataques que têm como objetivo consumir os recursos disponíveis da vítima são classificados como Esgotamento de Recursos. No entanto, esta categorização pode causar dificuldades na classificação de novos tipos de ataques porque os ataques de DDoS podem afetar tanto a largura de banda da vítima como os seus recursos, dependendo da infraestrutura implementada pela vítima.

Por esta razão, foi escolhida a utilização da classificação dos ataques na categoria Ataques baseados em volume, Ataques de Protocolo e Ataques de Aplicação, por ter sido considerado que se compreendem melhor as diferenças entre si. Os Ataques baseados em volume, são os ataques que têm como objetivo inundar a largura de banda da vítima, os Ataques de Protocolo e Ataques de Aplicação são os ataques de DDoS que exploram vulnerabilidades, nas camadas 3/4 e na camada 7 do modelo OSI, respetivamente, que levam ao consumo dos recursos da vítima.

Para as empresas se defenderem contra ataques de DDoS, precisam de utilizar/implementar soluções de DDoS. As soluções de DDoS podem ser inseridas em três categorias diferentes. Essas categorias são: Soluções Comerciais de DDoS, Soluções Open-Source e Freeware, e Outras Soluções que são apresentadas na literatura.

Na categoria de Soluções Comerciais de DDoS estão inseridas as soluções que precisam de ser compradas pelas empresas, ou seja, são as soluções que são vendidas por diferentes fornecedores, tais como a NetScout, Akamai, Radware e Cloudflare. Portanto, estas soluções requerem pouco esforço por parte da empresa, visto que o fornecedor está encarregue da implementação e manutenção dos serviços.

A categoria das Soluções Open-Source e Freeware, engloba as soluções que estão disponíveis na Internet e podem ser utilizadas por qualquer empresa, não implicando qualquer custo o que as diferencia das Soluções Comerciais de DDoS. Esta categoria tem a vantagem de não existir a necessidade de um custo adicional para a empresa. Por outro lado, as soluções desta categoria deixam a sua implementação e manutenção a cargo da empresa, levando a que a empresa necessite de realizar formações aos seus colaboradores para que estes consigam utilizar a solução da melhor forma.

Por último, a categoria das Outras Soluções apresentada na literatura, engloba soluções que se diferenciam das outras pela ausência de um software/aplicação utilizável, existindo apenas a sua descrição nos documentos disponíveis na Internet. Estas soluções apresentam técnicas e/ou metodologias inovadores para prevenir, detetar e/ou mitigar ataques de DDoS, permitindo a proteção face a certos ataques, não cobertos pelas soluções das outras categorias, usando as técnicas descritas. Contudo, como não existe uma aplicação utilizável, é necessário efetuar a sua implementação, que irá

requerer esforço adicional às empresas tanto no desenvolvimento como em formação dos seus colaboradores.

Após a categorização das soluções, foi construído um questionário com o objetivo de entender como é que, nos dias de hoje, as empresas se protegem de ataques de DDoS. Com os resultados do questionário conseguiu-se identificar as ferramentas e técnicas que as empresas utilizam para se protegerem. Para além disso, conhecendo as ferramentas e técnicas implementadas pelas empresas, foram identificados os ataques detetados e mitigados, e também os que conseguiram passar sem serem detetados. Outro ponto importante dos resultados foi ter o conhecimento das ações executadas pelas empresas quando estão perante um ataque de DDoS.

Por fim, com o conhecimento dos tipos de categoria de ataques de DDoS existentes, das diferentes soluções de DDoS e com a informação de como são protegidas as empresas em contexto real, foi construído e propôs-se uma *framework* que tem o objetivo auxiliar as empresas a escolherem as soluções de DDoS para que a sua infraestrutura se torne mais robusta e resiliente perante estes ataques.

A *framework* está dividida em três fases. A primeira fase tem como propósito conhecer a empresa do ponto de vista da sua dimensão e indústria, visto que empresas de diferentes dimensões têm diferentes orçamentos e recursos e certas indústrias tendem a ter uma maior probabilidade de serem alvo de atores maliciosos.

Após ter o contexto da empresa, avançou-se para a segunda fase, onde é preciso conhecer os ativos que a empresa pretende proteger porque os ataques de DDoS podem atingir diferentes ativos, como por exemplo *sites* Web, aplicações e servidores. Os ativos possuem diferentes superfícies de ataque, derivado da forma de como estes são implementados e, portanto, é necessário analisar as diferentes superfícies de ataque, como também os riscos associados.

A terceira e última fase, é a fase que se verifica a solução de DDoS mais indicada para tornar a empresa mais robusta e resiliente, tendo como base todo o contexto e informação das duas fases anteriores.

Palavras-chave: DoS, DDoS, Botnet, Soluções DDoS, DDoS framework

Abstract

Distributed Denial-of-Service (DDoS) is one of the most common cyberattack used by malicious actors. It has been evolving over the years, using more complex techniques to increase its attack power and surpass the current defense mechanisms.

Due to the existent number of different DDoS attacks and their constant evolution, companies need to be constantly aware of developments in DDoS solutions

Additionally, the existence of multiple solutions, also makes it hard for companies to decide which solution best suits the company needs and must be implemented.

In order to help these companies, our work focuses in analyzing the existing DDoS solutions, for companies to implement solutions that can lead to the prevention, detection, mitigation, and tolerance of DDoS attacks, with the objective of improving the robustness and resilience of the companies against DDoS attacks.

In our work, it is presented and described different DDoS solutions, some need to be purchased and other are open-source or freeware, however these last solutions require more technical expertise by cybersecurity agents.

To understand how cybersecurity agents protect their companies against DDoS attacks, nowadays, it was built a questionnaire and sent to multiple cybersecurity agents from different countries and industries.

As a result of the study performed about the different DDoS solutions and the information gathered from the questionnaire, it was possible to create a DDoS framework to guide companies in the decision-making process of which DDoS solutions best suits their resources and needs, in order to ensure that companies can develop their robustness and resilience to fight DDoS attacks.

The proposed framework it is divided in three phases, in which the first and second phase is to understand the company context and the asset that need to be protected. The last phase is where we choose the DDoS solution based on the information gathered in the previous phases. We analyzed and presented for each DDoS solutions, which DDoS attack types they can prevent, detect and/or mitigate.

Keywords: DoS, DDoS, Botnet, DDoS Solutions, DDoS framework

Contents

List of Figures

List of Tables

Acronyms

DoS Denial-of-Service

DDoS Distributed Denial-of-Service

RDOS Ransom Denial-of-Service

DaaS DDoS-as-a-Service

IoT Internet of Things

IIoT Industrial Internet of Things

APT Advanced Persistent Threat

CVE Common Vulnerabilities and Exposures

C&C Command and Control

ISO International Organization for Standardization

ISP Internet Service Provider

CSP Communication Service Provider

OWASP Open Web Application Security Project

P2P Peer-to-peer

SDN Software-Defined Network

TCP Transmission Control Protocol

UDP User Datagram Protocol

NTP Network Time Protocol

DNS Domain Name System

ICMP Internet Control Message Protocol

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

SNMP Simple Network Management Protocol

SSDP Simple Service Discovery Protocol

SIP Session Initiation Protocol

LDAP Lightweight Directory Access Protocol

CLDAP Connection-less Lightweight Directory Access Protocol

OSINT Open-Source Intelligence

IDS Intrusion Detection System

IPS Intrusion Prevention System

Chapter 1
Introduction

Denial-of-Service (DoS) attacks, over the years, evolved into a more sophisticated, powerful, dangerous, and stealthiest attack, Distributed Denial-of-Service (DDoS) attacks, adding the many-to-one dimension that miss in DoS attacks, staying only in the one attacker device dimension. The main goal of DoS, as well as the DDoS attacks is the disruption of services by exhausting the available resources from the victims' devices. These attacks hinder the victims to provide their services in a correct way, that is, without disturbances, by affecting their network's bandwidth and/or resources, such as CPU and memory. Currently, exists a huge number of DDoS attack types which exploits different vulnerabilities, some of those vulnerabilities are from the main protocols used over the internet, such as TCP and UDP.

The first-ever DoS attack was launched by a 13 year old David Dennis, in 1974 [1] [2] which originated the emergence of a new cyberattack still present in nowadays, after more than forty (40) year, being one of the main threats for organizations, due to the fact that new DDoS attacks appear and the constant development, by the attackers, to find vulnerabilities and novel ways to bypass the current deployed defense mechanisms.

Over time, DDoS attacks damaged many organizations with powerful attacks. One of the first major cyberattacks was made to the Yahoo! on February 7 of the year 2000, which utilized a Smurf Attack to take down the Yahoo! for 2 to 3 hours provoking in financial losses from advertising revenue [3] [4]. However, Yahoo! was not the only website targeted, many other ecommerce organizations were affected by DDoS attacks from the same malicious actor, such as Amazon, CNN, and eBay, they called this massive attack as "The MafiaBoy DDoS Attack" [5].

More recent attacks were the DDoS attacks to the consultant Brian Krebs and the French webhost and cloud OVH, in September 2016, and to the service provider Dyn, in October 2016, these attacks peak 1.1 Tbps [6] using the Mirai botnet. Not forgetting the DDoS attacks to GitHub, in February 2018, that reached a 1.35 Tbps from several autonomous systems and to AWS, in February 2020, which lasted for three days and peaked at 2.3 Tbps, however, both attacks were successfully mitigated fast enough that did not made any substantial damage [5] [7].

Cloudflare recently, in August of 2021, automatically detected and mitigated a 17.2 million request-per-second (rps) DDoS attack, this attack was three times larger compared with the previous known attacks and according to Cloudflare [8] the attack was 68% of their second quarter (Q2) average rps rate of legitimate HTTP traffic. The attack was performed from more than 20,000 bots located in 125 countries, in which a big part of the attack originated from Indonesia, India and Brazil. These bots belong to a botnet called Meris [9], formed of infected routers and networking hardware manufactured by the Latvian company MikroTik. The attackers exploit a vulnerability in the router's operating system (RouterOS), with the Common Vulnerabilities and Exposures (CVE) being CVE-2018-14847 [10].

Mirai-variant botnets are still widely used, and they are a huge threat for everyone, such as for organizations or governments. Shortly after the previous attack, in October of 2021, Cloudflare detected and mitigated another DDoS attack peaking just below 2 Tbps from 15.000 bots infected with Mirai code [11].

Similarly, Microsoft mitigated three great dimension attacks, in which two peaked above 2.5 Tbps and the other a tremendous 3.47 Tbps. The 3.47 Tbps attack was reported on November of 2021 and considered to be the largest attack ever reported in the history [12] [13], the origin of this attack came from 10,000 sources distributed by multiple countries, such as China, Russia and India. The huge attack was generated by multiple attack vectors, which were UDP reflection on port 80 using Simple Service Discovery Protocol (SSDP), Connection-less Lightweight Directory Access Protocol (CLDAP), Domain Name System (DNS) and Network Time Protocol (NTP), lasting approximately 15 minutes.

We can verify that the DDoS attacks are evolving, continuously improving their max power and performing more dangerous attacks, where they can, already hit the mark of 2 to 3 Tbps, as well as perpetuate millions of requests per second. Thus, DDoS attacks are a very important subject to constantly explain its procedure, provide the necessary awareness of the dangers of not investing in cybersecurity, produce methodologies to support organizations and make surveys to gather the more recent information from other works together.

Moreover, with the COVID-19 pandemic DDoS attacks had a significant increase in 2020, counting more 1.6 million attacks compared with 2019, according to ENISA Threat Landscape 2021 [14]. Similar trend was verified in the first half of 2021, in which the small DDoS attacks boomed by 233%, as stated by Nexusguard [15], these small attacks can cripple internet service providers (ISP) and communications service providers (CSP) if they do not pay attention and perform additional actions, leaving the detection to threshold or signature-based methods, since the small attacks will not triggers those detection methods. Microsoft also verified an increase of 25% in the average daily number of attack mitigations in period [16].

Therefore, we verified that with the pandemic the number of DDoS attacks increased significantly, being currently a very important topic to consider when defending organizations, being affected by DDoS attacks can lead to severe consequences.

The main scope of this thesis will be denial of service attacks, distributed denial of services attacks and topics related to them, therefore any mention of other attacks that are outside of this scope, will not be described in detail.

1.1. Motivation

DDoS attacks are one of the most common cyberattack and with the COVID-19 pandemic, which led to many people working from home (i.e., remote working), boosted the increase of DDoS attacks, as we can see in the ENISA and Microsoft reports [14] [16]. Thus, with most of the companies maintaining the remote working, DDoS attacks continue to be a major concern.

Currently, there are several DDoS solutions, however these solutions have weaknesses which lead them to not protect against all types of DDoS attacks.

The existing papers present solutions for the problems that they are addressing, that is, the described strategies, methodologies, and techniques for prevention, detection, mitigation and/or tolerance will only resolve specific problems. Therefore, implementing only these solutions will not defend the companies from the vast amount of different DDoS attacks.

Additionally, the presented and described solutions in peer reviewed papers are tested in a closed environment, therefore they cannot and do not reach the dimension (i.e., peaking at Tbps) of a real and advanced DDoS attacks, such as from Advanced Persistent Threats (APTs) groups. For these reasons, organizations cannot take the risk of implementing such solutions, leading them to never being utilized in real world scenarios.

On the other hand, DDoS solutions vendors are the main choice of companies, and these companies trust in the solutions to defend their business, but for some companies relying to much only on these solutions can cause serious consequences, such as reputational damage, since the DDoS commercial solutions cannot mitigate sophisticated DDoS attacks, although they are good at mitigating "*large-but-obvious-to-catch*" DDoS attacks [17].

With these problems in mind, our main motivation for this thesis is to gather and present relevant information about DDoS solutions provided by different vendors, as well as the solutions described in the literature by peer reviewed papers, with the objective that these solutions can be correctly used to support organizations in real environments against a vast number of DDoS attacks. Thus, during the development of this thesis will address and answer the following questions:

1. Can organizations that are targeted by DDoS attacks be helped in the development of their robustness and resilience?
2. Are there techniques, methodologies or frameworks that can guide the organizations in the prevention, detection, mitigation, and tolerance of DDoS attacks?

1.2. Objectives

To be able to answer the questions in the best possible way, it is necessary to complete certain objectives. Thus, it is necessary build an action plan for each question to list those crucial objectives.

The first question is related to the current defense mechanisms used inside an organization, so it is essential to understand how organizations operates to prevent, mitigate, detect, and tolerate DDoS attacks. For these reasons, we need to complete the following action plan, to gather the necessary information:

- Build a questionnaire
- Send the questionnaire to cybersecurity specialists in different companies
- Collect and analyze the gathered information from the questionnaire

While, for the second question, it is required to follow the next, action plan:

- Research for papers, methodologies, or frameworks
- Analyze the findings
- Discard those that are not suitable to use in a real environment
- Development a framework to guide organizations

1.3. Structure of the Document

The following chapters in this document are organized as follows:

- In Chapter 2, we performed a walkthrough of the different cybersecurity concepts, which will allow the readers to better understand the document and provide a detailed explanation of what are DoS and DDoS attacks, as well as the clarification of each steps that the attacker need to complete, so they can execute successfully this cyberattack. The chapter ends with the list of the main motivations that lead the attackers to realize these malicious cyberattacks.

- In Chapter 3, it is described two different ways to classify DDoS attacks, however we choose one between the two classifications, which in our perspective is easier to understand. We classify the 27 (twenty-seven) DoS and DDoS attacks in their respective category and explained the reasons why they are put in those categories.
- In Chapter 4, we presented 3 different categories of DDoS solutions and indicated what solutions they are composed of. With the completion of the description of each category of DDoS solutions, it is presented our proposed framework, which allow companies to follow/choose different paths, in order to decide which DDoS solutions better suits their available resources.
- In Chapter 5, it is performed the detail explanation of how we produced the questionnaire that was sent to multiple cybersecurity agents in different companies and countries. We also described the analyze of the 7 received answers and presented the difficulties we had in collecting answers.
- In Chapter 6, we presented and explained our proposed framework, which can guide companies in the process of choosing the most adequate DDoS solutions for their needs and capabilities.
- Finally, in chapter 7 we present the main conclusions of our work and what are the next steps needed to be done in the future to improve the work.

Chapter 2
Background Concepts

Currently, there are multiple different types of cyberattacks and each different type of cyberattack cause negative effects differently to their victims, but in the end, they all have a common objective to harm their victims.

In this chapter, we will perform a walkthrough of the concepts that led the cyberattacks to be possible, that is, what are vulnerabilities and how malicious actors reach to these vulnerabilities and exploit them. In addition, we will present the different cyberattack types, and explaining in depth the backbone of the cyberattacks that are in the main scope of this thesis.

2.1. Understanding the Cyberattacks Main Concepts

2.1.1. Vulnerability

When we talk about cyberattacks it is important to understand how they are possible. They occur because of the existence of vulnerabilities. Currently, "*vulnerability*" has many definitions from different network security authorities, such as from the National Institute of Standards and Technology (NIST), ISO 27005 and ENISA [18].

Thus, a definition of vulnerability in cybersecurity is a weakness or flaw in an information technology system, system security procedures, internal controls or implementation that can be exploited by a malicious actor to perform a cyberattack successfully.

By attacking a vulnerability, it can cause the systems to stop working, exfiltrate confidential data, disrupt the normal process, or consume their resources.

The OWASP community, which have the objective to improve the security of software [19], is a good place to verify what are the top 10 vulnerabilities related to web applications and IoT devices. With this, the OWASP helps developers, manufacturers, enterprises, and consumers avoiding the described vulnerabilities when building, deploying and managing web application and IoT systems, respectively.

The most recent available OWASP IoT top 10 was published in 2018 [20], while the most recent OWASP Web Application top 10 was published in 2021 [21]. It is important to highlight that the vulnerabilities presented in OWASP top 10 for IoT devices are different from the web application OWASP top 10 vulnerabilities.

We need to have extra careful with IoT devices, because most of vulnerabilities found on IoT devices are no longer possible on laptops and desktops, because over the years security measures in software (e.g., operating systems) and hardware have been implemented. Furthermore, people are more concerned and aware about their security and privacy, but this do not go beyond the "traditional" computers (laptops and desktops), forgetting that IoT devices are also computers, and they are connected to the internet.

According to the article by *Nick G. (2022)* [22], in 2021 was predicted to reach the mark of 46 billion connected IoT devices, which was a 200% increase compared to 2016. Nevertheless, this number of connected IoT devices will continue growing tremendously and by 2030 it is expected to hit 125 billion. The increase of popularity will not only impact the number of devices, but also the entry of new consumers to this market.

Thus, the reasons mentioned above increase the interest of attackers to exploit these devices, attackers which know about the vulnerabilities in the OWASP IoT top 10 [20] and have some knowledge about technology can easily compromise an IoT device, and if the device is connected to the organization network can later result in an information breach or an implementation of a malware that will lead to big financial losses and affect the brand image. For example, this is particularly critical in Industrial IoT (IIoT), by the fact that the disruption of these devices can cause the business operation to stop and inflict significant damage, or in the health area, an exploited vulnerable medical device can affect people's safety [14].

2.1.2. Attack Surface

In addition to the vulnerabilities, it is also important to understand the attack surface of the assets. The attack surface, according to NIST [23], is “the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment”.

In other words, the attack surface of an asset (digital or physical) are all the points where an unauthorized attacker can gain access to the asset. Thus, smaller the attack surface, the easier it is to protect the asset.

There are two categories of attack surface: the digital attack surface and physical attack surface. In brief, the digital attack surface refers to the hardware and software that connect to a company’s network, such as servers, websites, ports, third party software and applications, while physical attack surface consists of all endpoint devices that an attacker can physically access, for example, hard drives, mobile phones, desktops and laptops [24].

Thus, understanding the concept of attack surface, we can indicate that if an asset (digital or physical) has a vulnerability, but that vulnerability does not have an associated attack surface, this means that the attacker cannot exploit the vulnerability, since the current attack surface does not allow the attacker to get to the vulnerability.

2.1.3. Cyberattacks

The cyberattacks are performed in the environment created by interconnected and interdependent network of information systems infrastructures [25], which is called cyberspace, with the purpose to disrupt, disable, destroy, or maliciously control a computing environment/infrastructure; or destroy the integrity of the data or steal controlled information [26].

A set of different types of cyberattacks, not all, are:

- Malware attack – short of “Malicious software”, is software developed by malicious actors with the objective to steal information, damage or destroy computers or computer systems. Virus, Trojans, Worms, Spyware, Adware and ransomware are all types of malwares [27].
- Phishing attack – Cyberattack that attempt to steal users’ sensitive information or credentials masquerading as a trusted entity, through emails or text messages that led the victims to click

in a link, which will ask for their information [28]. Phishing attacks can also be used to deliver other types of cyberattacks, such as malware.

- SQL Injection – this attack is performed when it is asked user input, for example in a website, however the input given by the attacker are queries to the database, leading the attacker to gain access to the information contained in the database, insert new information or delete the database entirely.
- Denial-of-Service (DoS) attack – DoS attack types are when an attacker targets the computer network's bandwidth and/or connectivity. In a network bandwidth attack the malicious actor flood the network with a high volume of traffic consuming all device available resources and preventing legitimate user’s packets to achieve their destination. While connectivity attack is when a target device receives a high number of connections that consume all resources hinder the device to process legitimate user requests.
- Distributed Denial-of Service (DDoS) - A DDoS is a subcategory of DoS attacks [29], in which it differs from a DoS attack by the number of attacking devices, where multiple compromised devices target, in a coordinated way, one or more systems. This kind of attacks are more effective since they can send a much larger traffic volume compared to a single device, leading the target devices to spend more resources.

In this thesis will focus on the DoS and DDoS cyberattacks, thus these cyberattacks will be explained in more detail below, while the further explanation of other attacks is out of the scope.

2.1.4. Denial-of-Service Attacks

The attacks represented in here, are the attack types which can disrupt a target's service with only a single device.

Smurf Attack

The Smurf Attack like ICMP Flood Attack, utilizes the ICMP echo-request to execute the attack. But, in a different way, this attack just needs a single device, being therefore a non-Distributed Denial-of-Service attack.

This attack type is considered an amplification attack, since it uses reflectors where sending a single echo-request message will generate more than one message (i.e., amplifying the attack). This attack utilizes the IP broadcast functionality, in which an echo-request message is sent to every host in the broadcast network, leading to each host (i.e., reflectors) to respond to the ping with echo-reply. Thus, the attack starts with the generation of an ICMP echo-request message with a spoofed source IP address (i.e., the victim IP address), in which will be send it to an IP broadcast address of a router or firewall. After, the request messages will be sent to all hosts inside the broadcast network and each host that received the request will respond with an echo-reply, with this the number of replies to the spoof IP address is increased. Eventually, the victim will be flooded with a higher number of reply that it can support, resulting in disruption of the services provided by the target. The representation of the attack can be seen in the Figure A.1, Appendix A.

Nowadays, this attack type is already solved and obsolete since firewalls block all ICMP protocol messages [30] [31].

Fraggle Attack

The Fraggle attack was developed to bypass the firewalls rules that block ICMP messages. This attack procedure is similar to Smurf Attack, but instead this attack uses spoofed UDP packets directed to port 7 (Echo service) and port 19 (Chargen service). As well as ICMP messages in the Smurf Attack, datagrams are also sent to a broadcast IP address which will forward to all host in the network and replying to the spoofed IP address, flooding the victim with unwanted responses.

This attack, as well as Smurf attack are already prevented by protection mechanisms [32].

Local Area Network Denial (LAND) Attack

This attack is considered a denial-of-service (DoS) attack, since it does not need multiple devices, simultaneously, to disrupt and/or shut down services. In this attack type, the attacker sends a TCP SYN packet with spoofed source and destination IP address, which are the IP address of the victim. When the victim receives the packet and tries to reply, it will create an infinite loop and eventually crashes the victims' device. This happens because the system will repeatedly be sending replies to itself.

Ping of Death Attack

The Ping of Death Attack consists of sending an intentionally malformed data packet (i.e., ICMP packet) that exceeds the maximum packet size, leading to the victim crash, reboot, or freeze. The ICMP packet need to be larger than 65,536 bytes [31] to cause the mentioned consequences at the victim. The Figure A.2, in Appendix A, present this attack flow.

Currently, this attack type is already protected by host systems.

The denial-of-service can be successfully executed only by a single attacker, hence it is not necessary the utilization of a botnet, hence this attack is classified as a DoS.

Teardrop Attack

Another DoS attack is Teardrop Attack [33], where the attacker manipulates the offset value (i.e., number and location) of fragmented packets which will generate errors when re-build/reassemble those packets, exploiting the vulnerability in TCP/IP fragmentation. Therefore, the attacker is sending fragmented packets with overlapping offsets, this will result in invalid reassembled packets and consequently the target system will crash or reboot.

R U Dead Yet? (R.U.D.Y) Attack

The R.U.D.Y is an attack tool that aims to denial the victims service to valid users, also called **Slowpost** or **slow request attack** [34], is another attack type characterized as a slow attack, focusing on exploiting the form submission field of the websites through HTTP POST requests, therefore it attacks the application layer. The attacker utilizes the R.U.D.Y tool to scan for a form field within the victims website, once it is found the tool creates and submits HTTP POST requests, but those requests packets are cut into small sized packets (i.e., 1 byte [34] [35]) and sent at randomized intervals (i.e., the packets are sent very slowly). With this the attacker can maintain the connection open with the server for very long time, consequently degrading the normal operations. Additionally, it is possible to create simultaneously multiple connections aiming to overload the victim server's connection table, resulting on the hinder of new connections, such as from legitimate users, hence preventing the website to provide their service.

Slowloris Attack

The Slowloris is a specific attack tool and attacks the application layer, with the main idea of using only a single device to shut down a server. Initially, the attacker sends a large number of partial HTTP requests and for each requests the target server opens a connection. Normally, when the server does not get any message for a period, its timeouts to free the socket for a new connection. But, in order to keep the connection as long as possible the attacker send partial HTTP requests at a regular interval, to inform the server that the attacker device still there and is just slow (e.g., saying "I'm still here! I'm just slow, please wait for me." [36]). Consequently, the server will never release the occupied sockets and, eventually, all available sockets will be filled, resulting in the impossibility of opening new connections and, hence, the application server is unable to respond to legitimate users. Such as, HTTP Fragmentation Attack and R.U.D.Y Attack, Slowloris is a slow attack.

Slowloris attack is represented in Figure A.3, Appendix A.

2.1.5. Distributed Denial-of-Service Attacks

The distributed denial-of-service attacks utilizes more than a single device to overwhelm and disrupt a victim's service.

It is very important to highlight the difference between a reflection attack and an amplification attack. The reflection attacks means that the attacker uses other devices as a reflector to send a message to a victim, hence the number of requests received by the reflector is the same to the responses sent. While an amplification attack is a reflection attack, but the reflector generates a response significantly larger (i.e., more information in the message or/and messages) than the original request sent by the attacker. Thus, attacks that are amplification, are also reflection, but in the other way is not true, that is, reflection attack is not always an amplification attack.

The attacks that are named amplification, they are also reflection, but since amplification is the most dangerous form of reflection attacks and the difference between them was already explained, they will be only named amplification.

ICMP Flood Attack

The ICMP Flood Attack, also known as Ping Flood Attack, exploit one of the most important network layer (i.e., from seven layers OSI model [37]) ICMP through the utilization of ICMP echo-request, with the objective to overwhelm the victim, consequently disrupt the ability to respond to the high number of requests and overload the network with a high traffic volume. The ICMP messages (echo-request and echo-reply) are used to ping a network device to verify if it is available or reachable by the sender. To execute this attack, the malicious actor orders their botnet to send ICMP echo-request to a single victim, in which will reply to those echo-requests with an ICMP echo-reply, the greater the number of bots within the botnet sending messages, faster will be the consumption of the victim available bandwidth. Thus, the amount of received message from the target device will be the sum of the messages sent by each bot. We can see this attack flow in Figure A.4, Appendix A.

Previously, the attacker would spoof the source IP address to mask the sending device, but currently with the increased number of botnet and bots, attacker rarely hides their bots IP address and rely only on the capacity of the bots to saturate the bandwidth of the victim [38].

UDP Flood Attack

The UDP Flood Attack has the identical objective as the ICMP Flood Attack which is to flood the victim with a high volume of traffic. The attacker utilizes their botnet to execute this attack, sending UDP packets (i.e., datagrams) with a spoofed IP address to specific or random ports on the target system, using UDP is easy to spoof the IP address of the attacker since it is "connectionless" and does not need a handshake mechanism or session [39].

On the victim side, when it receives the UDP packet checks the specified port to identify and confirm if exists any listening applications, generally, no application will be listening and the system need to inform the sender, in this case reply to the spoofed IP address with an ICMP "destination unreachable" message. However, since the IP address specified in the packet is not the IP address of the attacker, these messages will be sent to an unknown device. With the great volume of datagrams sent through the botnet, eventually, the victims’ available bandwidth will be consumed and disrupting the normal operation, preventing legitimate communication.

This attack type is already known for decades, but still very popular and growing trend these days, in which UDP Flood attacks is the most used attack with 33% of total attack types occurred, between July 2020 to June 2021, presented by *Microsoft Digital Defense Report* [16].

DNS Amplification Attack

The DNS Amplification Attack, as well as the DNS Flood Attack uses the domain name servers, but in a different way. While DNS Flood Attack directly overwhelms the domain name servers, DNS Amplification Attack utilizes the domain name servers as an intermediary (i.e., as a reflector) to amplify the attack to the real victim.

The attackers, firstly, send a DNS name lookup request to a publicly accessible and unsecured open DNS servers with spoofed source IP address, which will be the victim's IP address, leading the domain name servers to send the response to the target. Typically, the attacker sends small requests that result in large responses, with this is possible to generate bigger messages with tiny requests increasing the attack power, hence bots with small bandwidth (e.g., some small IoT devices) can execute this attack without worrying about their available resources. By leveraging a botnet to send a large amount of spoofed DNS queries, it is possible to create a high traffic volume, overwhelming the victim network bandwidth and resources, disrupting their normal functioning.

An example, according to US-CERT, the attacks observed by them mainly use DNS "ANY" request, in which returns all possible known information about a specific DNS zone with only a single request, therefore the response to the victims will be much larger than the request.

Furthermore, the responses received by the victim are legitimate, they come from legitimate servers, making it extremely difficult to prevent and stop these types of attacks [40].

NTP Amplification Attack

Network Time Protocol (NTP) is an application later protocol utilized to synchronize computer clocks between multiple device systems [41].

This attack type works similarly to DNS Amplification Attack, but instead this exploits NTP servers which have the *monlist* command enabled, this command allows to retrieve information about the hosts with which the NTP servers communicated recently, consequently the traffic sent by the NTP servers will be larger than the message sent by the attacker. In other words, the packets sent by the attacker will be amplified into larger packets.

The attack starts with the malicious actor sending UDP packets with spoofed IP address, through the botnet, to NTP servers with *monlist* command enabled. The UDP packets makes requests to the NTP servers to use *monlist* command, which generate a large response. After receiving the datagram, the server will reply with the results of *monlist* command to the spoofed address, this means, replying to the real victim IP address. Thus, the victim will be flooded by a high traffic of large packets, overwhelming the victims' resources, such as bandwidth and CPU, and resulting in denial-of-service. In addition, this attack is hard to block and filtrate, since the malicious packets are sent by legitimate and valid servers, similarly to DNS Amplification Attack.

In 2014, Cloudflare was attacked by a NTP Amplification Attack, in which the attacker traffic peaked at over 400Gbps [5] [42].

CHARGEN Attack

This attack exploits the character generator protocol (CHARGEN), a very old protocol, but still in use on some connected devices such as printers and photocopiers. The CHARGEN Attack is an amplification attack, in which the attack is executed by sending small packets with spoofed IP address of the victim to internet devices that have CHARGEN enabled. After this, CHARGEN enabled devices that received the packets, will respond with UDP packets to the victim, which had the IP address spoofed, on port 19. Consequently, the target will be flooded with a large number of bogus UDP packets and, eventually, consuming all available resources, leading the victim to be unreachable for legitimate messages [43].

SNMP Amplification Attack

This attack type utilizes the Simple Network Management Protocol (SNMP), which is an Internet protocol for exchange management information between network devices, such as routers, servers, printers, and switches on the port 161. The cybercriminals send a large number of SNMP queries. with the botnet, to devices that have the protocol, but these queries have the source IP address forged with the IP address of the victim, so whenever the connected devices receive the query, they will reply with the response to the victims IP address. However, it is possible, to send small SNMP queries, such as *GetBulkRequest* [44], that will result in larger responses amplifying the attack, in which these responses will be forwarded and flooding the victim with a high traffic of SNMP responses, disrupting the victims normal operation. Additionally, this attack does not generate large or unusual traffic from the bots making it difficult to detect and identify that the devices of end users are participating in illicit attacks to other entities.

According to Cloudflare report of fourth quarter of 2021 [45], SNMP Amplification Attack is the primary emerging attack vector that attackers are using to produce DDoS attacks, where it was possible to observe an increase of 5796% comparing with the previous quarter.

MSSQL Amplification Attack

The Microsoft SQL (MSSQL) Amplification Attack utilize Microsoft (MS) SQL Servers to reflect their responses to the victim by abusing of the Microsoft SQL Server Resolution Protocol (MC-SQLR). MC-SQLR, in which is listening on port 1434, allows clients to identify the database instance with which they are trying to communicate when connection to a database server. Thus, the MC-SQLR can be used whenever clients need to acquire information about the MS SQL servers on the network [46] [47]. Thus, the attacker through the execution of scripted requests with the source IP spoofed with the victims IP address, lead to the MS SQL servers to send their responses to the victim. The size of the amplification will vary, depending in the number of instances present in the abused MS SQL servers.

According to Akamai [47], the attack can produce an amplification factor of nearly 25 times bigger than the request size and its replication does not require a high level of technical skill. Therefore, this DDoS attack type being the one of the emerging threats in the fourth quarter on the year of 2021 [45], with the increase of 1607% compared with the previous quarter of 2021.

SSDP Amplification Attack

The Simple Service Discovery Protocol (SSDP) is a network protocol and is part of Universal Plug and Play (UPnP), which is used to discover services available on a network, such as Plug & Play (PnP) devices, in other words, to find and communicate with other devices that only need to be on and connected to the network, without the need of complex configurations by the owner. For example, a new printer that connects to your network does not need further configurations to be detected by other devices in the same network, thanks to this protocol. SSDP uses HTTP and multicast over UDP port 1900 [48] and works with *NOTIFY* and *M-SEARCH* methods [49]. Thus, whenever a PnP device connects to the network it sends a message to the IP address of the multicast, which will inform all other devices, such as computers, on the network about the new device. Once a computer receives the message sent by the multicast address, it can send a message directly to the new device requesting the complete description of its services, which will be responded with the list of all available services provided by the device.

This is an amplification attack, since it uses PnP devices to reflect and amplify the data sent to the victim. Initially, the attacker needs to discover PnP devices in the network to be used in the attack, this can be done through the *M-SEARCH* request, this method search for devices on a network, in which those devices that receive the request will respond to the source device. With the responses the attacker can gather the information of which devices are available. Thus, the attacker can send *M-SEARCH* packets with the source IP spoofed with the victims address to those devices, requesting much data as possible, especially with *ssdp:all* (i.e., find all PnP devices on the network) and *MX* value equal to 1 (i.e., max amount of time for the device to respond) [48]. Consequently, the PnP devices will reply to the target victim with more data than the data sent by the attacker bots, because the response message generates more than one message by the fact each device is expected to have at least one service [48], resulting in the victim being flooded by all PnP devices and eventually preventing the victim to provide the service correctly.

LDAP Amplification Attack

The Lightweight Directory Access Protocol (LDAP) is used to access and manage directory services on corporate networks. The LDAP operates over TCP/IP stack and is based on the client-server model. A LDAP client to retrieve data stored in a database, it needs to communicate with a LDAP server to access the data. Additionally, should be used authentication mechanisms when LDAP clients access LDAP servers [50]. The LDAP servers which are vulnerable and exposed to the Internet will be used to execute this attack type.

Similarly with the other amplification attacks, the attacker sends requests with the source address spoofed with the victims IP address to LDAP servers with open TCP port 389, which will retrieve the requested information, it is expected to be larger than the request message, hence amplifying the attack. After the LDAP server processed the request, it will reply to the request source IP address which in this case will be the victim. Consequently, the victim will be overwhelmed with large traffic of big messages and eventually hinder the availability of the victim’s service.

CLDAP Amplification Attack

The Connection-less Lightweight Directory Access Protocol (CLDAP) is a version of LDAP, previously described, the difference is that CLDAP operates with UDP at port 389 instead of TCP, hence is not needed the three-way handshake. In Figure A.5, Appendix A, it is presented the how this attack is performed.

The CLDAP Amplification Attack was identified and mitigated by Akamai Security Intelligence Response Team [51], in 2016, which, at that time, it was a new attack type. According with the Akamai report, on January 7, 2017, has been observed the largest DDoS attack using only CLDAP Amplification Attack peaking 24 GBps, with a rate of 2 million packets per second [51].

The attacks procedure is similar to LDAP Amplification attack, with the difference between both attacks being the transport protocol and the servers used as reflectors, one the attacker utilizes a list of CLDAP servers and in the other a list of LDAP servers.

The AWS DDoS attack in 2020 was targeted by this attack type [5].

SYN Flood Attack

An attacker using the SYN Flood Attack takes advantage of the vulnerability in the three-way handshake mechanism of TCP's connection establishment process. To create a connection between two parties (e.g., client and server) is needed to complete a three-way handshake process, where multiple acknowledgements between them are exchanged.

In the three-way handshake, the client sends the first packet, the SYN packet, to a server. This means that the client requests the server to create a connection between them. Upon receiving the SYN packet from the client, the server responds with a SYN/ACK packet, this confirm that the server successfully receives the SYN packet and acknowledge the connection with the client. Finally, the client replies to this last packet with an ACK packet which completes the handshaking process and establish the TCP connection between them. The server stores in memory all states used during the three-way handshake process until it establishes, or the time-out occurs due to the missing responses on the part of the client. SYN Flood Attack exploits this feature and floods the server's memory, when the memory reaches its limit, the next connection requests will be rejected from legitimate clients, preventing the communication of legitimate users with the server.

To accomplish the objective of flooding the server's memory, the attacker does not complete the three-way handshake by not replying with the last ACK packet, thus this will create a huge number of incomplete connections.

In order to conduct successfully this SYN Flood Attack, the malicious actor spoofs the source IP of the SYN packet with one that does not exist. Therefore, when the server replies with SYN/ACK packet to that source IP address, it will never receive the last ACK packet from the source. Nevertheless, the server waits for the ACK packets which eventually will fulfill its memory and hence preventing legitimate users of communicating with the server.

It is also possible execute this attack using a real IP address from a device, but here the device ignores the received SYN/ACK packets from the victim and thus it is possible to successfully execute the denial-of-service attack.

It is worth to note that exists multiple flood attacks that play with TCP flags, they are slightly different, but with the same objective to overwhelm and disrupt a targeted victims' normal operations by consuming the available resources through the process of the packets, such as SYN/ACK Flood, RST Flood, FIN Flood, XMAS Flood (i.e., all TCP flags are set to 1 in the packet), ACK Flood and ACK/PSH Flood. Thus, only SYN/ACK Flood Attack and ACK Flood Attack will be described below, while the remaining flood attacks will not be address, since their process of overwhelming the victims are very similar, resulting in redundant definitions, but this does not mean that those attacks are not important to follow and to understand by cybersecurity agents.

The SYN Flood Attack can be seen in Figure A.6, Appendix A.

SYN/ACK Flood Attack

In this attack type, the threat actor floods a victim with SYN/ACK packets, that are used in the second step of the three-way handshake mechanism, with the objective to disrupt the victim normal operations. These SYN/ACK packets sent by the attacker are not part of three-way handshake, but even so the server needs to process each packet to understand why it is receiving such packets out-of-order, with this will lead the server to waste resources to handle those packets and denying legitimate traffic and therefore valid users cannot access to the service.

ACK Flood Attack

The ACK Flood Attack is slightly different from SYN/ACK Flood Attack, in there the TCP ACK packet is used to overwhelm the victim with a huge number of these packets which do not belong to any open session on the server's list, with the goal to deny the provided service to other users. The victim's server needs to process each packet received, similar to SYN/ACK Flood Attack, to verify to which message the ACK packet came from, resulting in a great consumption of computing power. Thus, being flooded with ACK packets will consume all available resources from the victim leading it to drop legitimate packets and disrupting the normal performance.

UDP Fragmentation Flood Attack

The UDP Fragment Flood Attack is a more specific UDP Flood attack, the different feature is that UDP Fragment Flood Attack uses large fragmented packets with the objective to exhaust victims' resources with as fewer packets as possible. For this reason, that the fragment is maliciously fabricated, reassembly those fragments will not create a real data. Thus, eventually the victims' resources, such as CPU and memory, will be consumed, because these resources will be reserved in order to re-build the non-existent data, preventing communication with legitimate users [52].

In 2015, Radware recorded many of these attack types against customers in the financial services sector [53].

QUIC Flood Attack

QUIC is a new transport protocol designed to improve performance for HTTPS traffic, that is, sending data faster, more efficient, and more secure than the other transport protocol, such as TCP and UDP. The QUIC uses UDP packets to increase the delivery speed and to solve the drawbacks of UDP packet loss, its utilized multiplexing, to send several streams of requests/responses. Also, uses authentication and encryption to prevent modification and limiting ossification of the protocol by middleboxes. It's estimated that 7% of Internet traffic is now using QUIC [54]. The extensive explanation of how the protocol works is out of the scope of this thesis, but the detailed description can be found at *Langley et al. (2017)* [54].

The QUIC Flood Attack is carried out by the attacker flooding a victim with messages sent over QUIC. Thus, the victim's server will need to process all the QUIC messages it receives, consuming available resources and consequently slowing the service provided or, in the worst case, denying it completely.

DNS Flood Attack

The domain name servers are a crucial Internet service, since the servers automatically translates domain names to IP addresses. On the Internet it is necessary to use domain names, because they are easiest to remember compared to a long string of numbers (i.e., IP addresses). For this reason, this attack type focus on these servers to hamper the translations.

The DNS Flood Attack is an application-specific variant of a UDP Flood, since DNS servers use UDP traffic for name resolution.

The attacker sends a large number of packets, through the utilization of their botnet, with the intention to overwhelm one or more Domain Name System (DNS) servers' resources belonging to a specific location/zone, disrupting the normal operation of those servers (i.e., preventing the resolution of domain names) of that zone and its sub-zones. Thus, legitimate users that communicate with the DNS server will be blocked, hinder the users to access the provider's DNS servers [55] [56].

The Figure A.7, Appendix A, presents how this attack is performed by malicious actors.

NTP Flood Attack

In this attack, the NTP servers are the primary targets, in which the attacker floods those servers, with NTP packets using their botnet, to exhaust the available resources and disrupt the provided services.

The attack procedure is similar to DNS Flood Attack, hence the detailed explanation of this attack will be redundant [57].

Additionally, this attack type exists and is possible to execute, but the damage that it does is not very catastrophic (i.e., multiple devices will not have synchronized clocks) and for this reason is not often used, except for some cases where it is necessary that the devices have their clocks synchronized. Thus, the NTP Amplification Attack is frequently used and had a greater impact, as we demonstrated previously.

HTTP Flood Attack

The HyperText Transfer (or Transport) Protocol (HTTP) is the protocol used on the Internet to transfer data over the web, for example, transferring web pages between clients and servers through requests and responses.

In the HTTP Flood Attack [58], is designed to flood a victim's server by manipulating HTTP requests. Here the concept is the same as the previous attacks, that is, flooding the victims' resources in order to disrupt the web server to prevent legitimate users to communicate with it. Firstly, the attacker needs to set up TCP connections with the web server using the valid IP addresses of the bots. There are two varieties of HTTP Flood Attacks, which are HTTP GET and HTTP POST.

With the HTTP GET attack, the attacker executes a HTTP GET requests to retrieve very large images, files, or some other asset from the victim. However, each bot in the botnet sends a request and each of these requests need to be processed by the server through multiple actions to reply correctly. Thus, the server is required to read the asset requested from the back-end storage (i.e., database) and divide the asset into multiple packets to send it to the respective bots, this will overwhelm and consume all available resources (i.e., CPU and bandwidth) on the victim's server, hindering to respond to valid users.

While, with the HTTP POST attack, the attacker typically submits a form on a website, in which the server needs to process the incoming request and store the data into a back-end storage (i.e., database). The process of managing the received data and the execution of the necessary database commands utilize a larger number of resources, in this case processing power and bandwidth. Thus, flooding a victim server with a huge number of HTTP POST requests, using the botnet, will exhaust the available resources making the victim unable to process and communicate with legitimate users.

Both HTTP Flood Attacks (GET and POST) are similar, since they consume processing power, by the necessity of execution of some actions on server side, and bandwidth because of the high volume of incoming requests sent by the bots and the larger responses sent by the server. Additionally, the HTTP requests sent by the attacker consume significantly less resources compared with the resources exhausted by the server.

In Figure A.8, Appendix A, it is demonstrated how both HTTP Flood Attacks are performed by malicious actors.

The advanced and secure form of HTTP, HyperText Transfer Protocol Secure (HTTPS), that allows encrypting the entire communication with SSL/TLS can be also used to execute this attack, in which he attacker instead of using HTTP, use HTTPS to flood the victim. In addition, using HTTPS can also saturate the victim due the need to perform the asymmetric encryption, resulting on the consumption of more resources [59].

HTTP Fragmentation Attack

In the HTTP Fragmentation Attack, as well as the HTTP Flood Attack, the attackers' bots establish a valid connection with the victim's server, but instead of sending a HTTP GET or a HTTP POST to consume the victim's resources, the threat actor cut the packet in small fragments and sends them slowly as possible, that is, before the servers' times out the connection. The reason behind this method of sending the tiny fragments slowly is to keep the connections active for a long period, Thus, continuously making connection with the victim and keeping those connections active will, eventually, cause exhaustion to the server's connection table, preventing it to create more connection with valid users and resulting in a denial-of-service. This attack flow is presented in the Figure A.9, Appendix A.

The attack works because some web servers, such as Apache, have inefficient timeout mechanisms, allowing malicious users to keep long sessions [60] [61].

This attack type is characterized as a slow attack, in which is require little bandwidth and the requests sent are slow, not generating suspicious traffic hence being very difficult to distinguish from normal traffic and undetected for long periods of time. Thus, they are different from floods attack, since these make a huge traffic volume and are easily detected [34] [62].

SIP Flood Attack

The Session Initiation Protocol (SIP) is an application-layer protocol that permit to establish, manage, and terminate real-time communications, such as voice and video calls, known as Voice over Internet (VoIP) calls.

An attack can be executed using different types of SIP methods, such as SIP REQUEST, SIP INVITE, SIP NOTIFY and SIP INFO [34].

In the SIP Flood Attack the objective is to flood the SIP registration server (SIP REGISTRAR) to consume all available resources, since the server need to store the information of the user agents, resulting in outage of its services and legitimate users cannot reach the server.

Ransom DDoS Attack

In the Ransom DDoS (RDDoS) Attack the malicious actors extort money from organizations by threatening them with a distributed denial-of-service attack (DDoS). These attacks are been a new increasing trend, since 2020, they seem to be lucrative for the malicious actors going by the names of well-known advanced persistent threat (APT) groups, such as "Fancy Bear", "Armada Collective" or "Lazarus Group" [14] [63] [64]. Any DDoS attack type mention previously in this chapter can be used to disrupt the victims' services and leading the attacker to ask for a monetary value to stop the attack.

The RDDoS attack executed by the mentioned threat groups initiate by sending a letter to a victim (i.e., an organization) warning that the organization's network will be targeted with a DDoS attack that will peak over 2 Tbps, starting a week later the sending of the respective letter. To stop this attack of occurring the organization is demanded to pay a 20 BTC (Bitcoin), plus 10 BTC for each day not paid when the attack is already in execution, to a mentioned wallet address in the letter. In addition, on the date that the letters are sent the extortionists execute a small attack, in order to prove the legitimacy of the threat.

However, the RDDoS Attack can be performed in two different ways, one was already described in the previous paragraph, in which the attacker sends a letter before carrying out the DDoS attack. While the other way the threat actor starts the DDoS attack and sends a ransom letter demanding a payment to stop the attack.

Zero-day DDoS Attack

The Zero-day DDoS Attack is used to describe attacks that exploits new vulnerabilities, these vulnerabilities are unknown, as well as the impact and damage originated by these attacks.

When we say that the vulnerabilities in Zero-day attacks are unknown, we are referring that they are unknown by the community in general. However, these vulnerabilities can be known by a strict group of persons, including the attacker, which found them through research of the system, flaws in recent patch made by a company, and many other ways.

Thus, even if a certain number of people found a vulnerability, this does not mean that the vulnerability will be known by everyone, since a person with malicious intentions will not disclosure that precious information and will use it for their own benefits.

Currently, for Zero-day DDoS Attacks there is no effective defensive mechanisms neither efficacious mitigation plans [65] [66].

Blended Attack

The Blended Attack is an attack method that the attackers use. Speaking specifically in DDoS attacks, Blended Attacks refers to the idea of utilizing mixed attack types to exploit different weaknesses present in web applications or protocols, to disrupt a victim. An example of this attack is use one volume-based attack type (e.g., UDP Flood Attack) to consume significant bandwidth and complementing it with an application attack (e.g., HTTP Flood Attack) to consume server resources, maximizing the damage done to the target [67].

Is important to mention that the attacker may not use only DDoS, they can combine with another sophisticated attacks, such as phishing or malware.

2.1.6. Emerging DDoS attacks

Attackers are always trying to exploit new vulnerabilities, that is, novel methods that can bypass the security measures of organizations and fulfill their goals of denying services. Security agents need to be aware of emerging DDoS Attacks so they can in advance implement security measures and prevent the attack to hit their business or, if the attack cannot be prevented, having already a set of mitigation measures. With threat intelligence of new emerging DDoS attacks, organizations are not caught off guard.

Here, we will present one attack that uses a novel DDoS attack method, to can carry massive attacks and disrupt any company *status quo*.

TCP Middlebox Reflection

The DDoS attack using TCP Middleboxes for reflection was described first by researchers from the University of Maryland and the University of Colorado in the paper “*Weaponizing Middleboxes for TCP Reflected Amplification*” [68]. But only in 2022 that these attacks are found in the real-world scenario, where Akamai Security Researchers detected and analyzed a huge numbers of TCP reflection attacks, peaking at 11 Gbps at 1.5 million packets per second (Mpps) [69].

In this DDoS attack it is used a new attack vector, middleboxes. Middleboxes is an in-network device sitting between two end-hosts with the purpose of transform, monitor or filter packets streams in-flight. The main difference of middleboxes and traditional network devices, such as routers and switches, is that middleboxes operate with the packet’s headers and with their payload, as well.

The attacker uses middleboxes as reflectors with the objective to amplify their attacks, by abusing the middleboxes that have the objective to block the access to certain websites (i.e., content filtering) and do not take in consideration the TCP states, therefore can respond to out-of-state TCP packets. When users try to access a blocked website and the packets are received by the middlebox, it will respond by sending, typically, HTTP headers and in some cases entire HTML pages. With these messages attacker see an opportunity window for a significant amplification attack.

Currently, the attack traffic in relatively small just peaking at 11 Gbps, but according with Akamai report it is expected that the attack will grow in the future, since it offers a significant amplification of the attack [69] and the existence of a large number of vulnerable middleboxes that can be exploited, in which 337 million IP addresses are found by the researchers of University of Maryland and University of Colorado [68].

2.2. Related Work

Nowadays, there are in the literature a large number of surveys regarding DDoS attacks and defense mechanisms. But most of the recent ones focus mainly in a specific attacked area, such as IoT and cloud environments, by the fact that they are new and have numerous different subjects to tackle.

Zargar et al. (2013) [4] presented a survey in which is described and classified DDoS flooding attack types, as well as the defense mechanisms, where they divided in four categories Source-based DDoS Defense Mechanisms, Network-based DDoS Defense Mechanisms, Destination-based DDoS Defense Mechanisms and Hybrid DDoS Defense Mechanisms. However, this paper lacks new DDoS attack types compared with out thesis and the defense mechanisms described are traditional and old methods, good to understand how previously the DDoS attacks are defended, but with the emergence of newer and sophisticated software the feasibility of using those mechanism will be less.

Prasad et al. (2014) [70] explain how DDoS attacks work and the attacker motivation, but it is not provided any definition or classification of DDoS attacks. The authors presented a survey from multiple papers, in which for each DDoS detection strategy, in this case are statistical, soft computing, knowledge, and datamining and device learning, is represented a table that demonstrate how the paper contributed to defend from DDoS attacks.

In *Mahjabin et al. (2017)* [34] survey the actors started with the explanation of how the DDoS attacks work and going deeper, providing the information about the motivations of the attackers. After that, they described multiple DDoS attack types and classified them in resource depletion, bandwidth depletion or both, pointing a different perspective compared with our thesis. They also presented different defense mechanisms to prevent and mitigate DDoS attacks. However, the description of the more sophisticated software's used to and by organizations to protect them from DDoS attacks, are not performed. Also, techniques present in the literature, produced by researchers, which can be viable in the real-world environment are not mentioned. This thesis fulfills the gap left attacking those points.

With the increase utilization of IoT devices, coming from the popularity of those devices which helps in day-to-day tasks, but are sold insecure, for example, with weak passwords and the nonexistence awareness led to those devices to remain vulnerable, therefore, DDoS attacks from IoT devices became a huge threat to everyone. In *Vishwakarma and Jain (2019)* [71] paper it is presented a survey of DDoS attack, but with the main focus in the IoT world. The paper performs the taxonomy of DDoS attacks, explaining some attack types. The defense mechanisms provided by the authors, some are specifically designed to protect IoT devices, on the other hand, some can be used in general to protect and defend organizations.

The work from *Salim et al. (2019)* [72] makes a survey of DDoS attacks in IoT. The paper discusses the motivations why attacker choose IoT devices, as well as the motivations why attacker precede to do DDoS attacks. It also describes some DDoS attack types. and DDoS attack tools. The authors provide a deep description of DDoS defense mechanisms, in which they divide in three categories: prevention, detection and mitigation. To help visually it is demonstrated a table with all defense mechanisms and DDoS attacks type, presented in the paper, in which those attacks that are protected by the defense mechanism are marked, therefore is easily visualized which attacks are defended with which mechanisms.

The papers from the authors *Yan et al. (2015)* [73], *Dong et al. (2019)* [74] and *Singh & Behal (2020)* [75] describe DDoS attack that target specifically software-defined networks (SDN) in cloud computing environments. Both described and classified what is a DDoS attacks, introduced the existent problems in the SDN and cloud computing, and present surveys where they compared the defense mechanisms in literature, that existed at the time that they wrote the paper.

Other papers that describe DDoS attacks and provide defense mechanisms are from *Kamboj et al. (2017)* [76] and *Mallikarjunan et al. (2016)* [77], these are small papers with 5-6 pages that gives a good insight about some DDoS attacks and existing defense mechanisms (i.e., solutions), but they lack novel solutions compared with the other papers, already mentioned, and our thesis.

The authors *Bhardwaj et al. (2021)* in their paper [78] presented the state-of-the-art of the DDoS attacks in the cloud. They mentioned the DDoS incidents which occurred since 2014, with the objective to demonstrate how DDoS attacks can targeted cloud platforms and consequently the importance of implementing and evolving DDoS solutions. They also described the different types of DDoS attacks that can be performed on cloud infrastructures, cloud services and cloud costumers.

This was the only the peer reviewed paper, that we found in the literature, that performed a description of the different DDoS commercial solutions (total of 14 commercial solutions). Additionally, they presented a survey of anomaly-based techniques to detect DDoS attacks, in which they mentioned multiple papers that propose solutions to detect DDoS attacks grouped in the following categories: anomaly-based supervised machine learning methods for DDoS detection, anomaly-based unsupervised machine learning methods for DDoS detection, anomaly-based statistical methods for DDoS detection and anomaly-based hybrid methods for DDoS detection.

None of the above-mentioned papers had described the viability or how the defense mechanisms are used by cybersecurity agents and suited in a real-world attack. Neither a framework to guide organizations to protect themselves from DDoS attacks.

Therefore, this means, that the papers that we found, propose their solutions to combat DDoS attacks or perform a survey of the current DDoS defense mechanisms, however, even if the solution are tested with dataset with DDoS attacks, such as CAIDA [79], it is not enough to ensure that the solution provides a high level of effectiveness and efficiency in real-world environments, leading to companies to not take the risk of implementing them and resort to DDoS commercial solutions where they have some guarantees through the service level agreements (SLA) between the DDoS commercial vendor and the company.

2.3. Architecture of DDoS Attacks

In this section, we will explain in detail the different phases used in DDoS attacks, since the recruitment phase until the unleash of the attack by the botnet targeting the victims. The word botnet is derived from "robot networks". For further detailed definition of what is a denial-of-service (DoS) attack, it is present in the following works of *Mirkovic & Reiher (2004)* [80] and *Douligeris & Mitrokotsa (2004)* [81].

After many years, since 2004, these papers still have the definition viable and characterize what is a DoS attack. A DoS attack can be described as a cyberattack in which a malicious actor has the intention to render a computer or any type of network device unavailable of providing their services correctly and preventing their normal functioning.

DoS attacks are composed of only one machine and this machine is in charge of performing every stage of an attack, while the architecture in typical distributed denial-of-service attacks is constituted by four main elements [81] [82], which are:

- The **real attacker** or **botmaster** is the malicious actor that executes the attack.
- The **handlers**, **masters** or **Command and Control** (**C&C**) servers, they are compromised hosts with the program to control multiple agents, through handlers the attacker can verify which agents are available and attack parameters.
- The **agents**, also called bots, zombies, and slaves. They are compromised devices that receive the orders from handler’s devices and execute the attack. A set of agents is called a botnet.
- The target **victim**, the service or host that will suffer the denial-of-service attack.

DDoS attacks to be successfully executed by the attackers, need to go through four phases, which are *Recruitment*, *Exploitation & Infection*, *Communication* and *Attack* [83]. The definition of each phase is represented as follows:

1. **Recruitment:** In this phase, the attacker utilizes different strategies to scan for new vulnerable devices, which will be later used to perform the DDoS attack to the real victim.
2. **Exploitation & Infection:** The vulnerable devices that have been discovered through the scans of the *Recruitment* phase are exploited and the attack code is injected or downloaded using propagation mechanisms. Completing this phase, the devices with the attack code are considered infected.
3. **Communication:** The attacker through handlers or the Internet Relay Chat (IRC) channels identify which agents are available to execute the DDoS attack and if it is necessary to transmit modifications or upgrades to the attack code. Handlers and IRC channels are the link of communication between the attacker and their botnet.
4. **Attack:** This is the last phase, where the attacker commands the botnet to onset the DDoS attack and the botnet members will start to send malicious packets. The attacker transmits the attack parameters, such as victim's IP address, attack duration, attack type and other necessary information.

Over the years, botnets, which are a crucial piece in the realization of DDoS attack, have evolved to be more sophisticated and complex, making it harder to find the infected devices. Thus, further in this chapter we will present the current botnet structures used by malicious agents.

In the Figure 2.1, it is demonstrated the flow of how the different phases are used to reach the malicious actor final objective, that is, the attack to the victim, and the main functions of each element of the DDoS attacks. A detailed description of the Figure 2.1 flow will be done below.

In the first phase of DDoS attacks, the attacker utilizes scan techniques to discover new devices, with the objective to add them to the botnet. However, the new discovered devices might be vulnerable or not. Here comes the second phase, where the attacker exploits and infects the devices that are vulnerable (i.e., the devices have a specific vulnerability that an attacker is able to exploit and then infect it), whereas the devices that do not have the specific vulnerability that the attacker is looking for will not be exploited and infected.

When infected, devices become agents of the attacker botnet and now can be ordered to start/perform a DDoS attack.

The flow between attacker/handler and handler/agents, is the to demonstrate how the attacker communicates with their botnet, which is through the handler. With this flow, the attacker can verify the state of the botnet, transmit upgrades and/or modification to the agents and start DDoS attacks.

In further Sections, will be described in detail the techniques used in each phase of a DDoS attack.

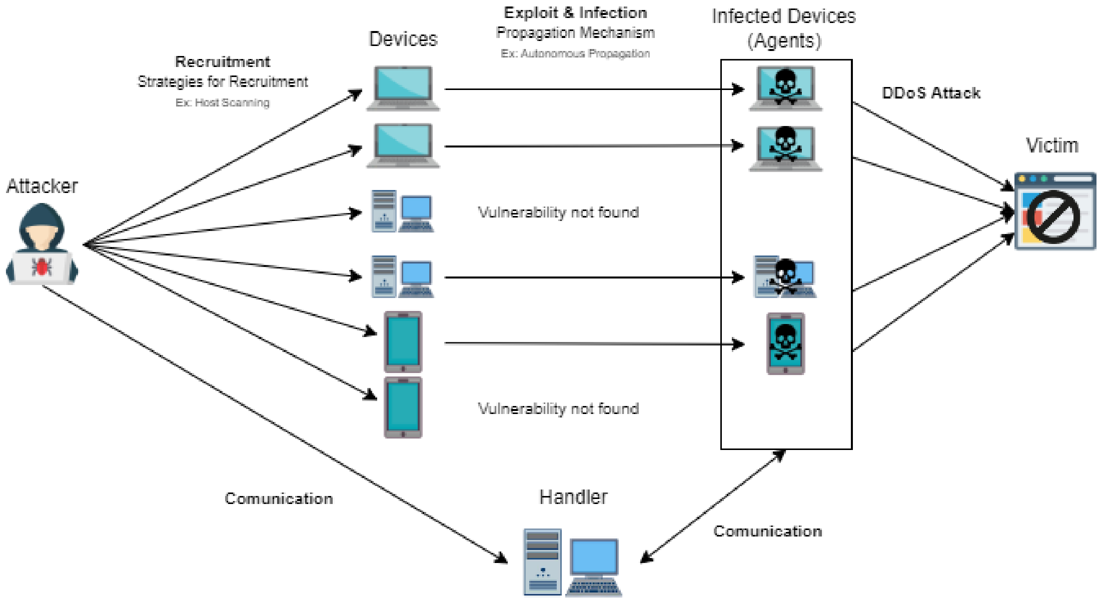


Figure 2.1. Architecture and Phases of DDoS Attacks

2.4. Level of Automation of DDoS Attacks

Each attack can have different levels of automation in different phases of DDoS attacks, that is, when scanning for new devices and recruiting them for the botnet, infecting these devices and commanding the botnet to start an attack. The levels are Manual, Semi-automatic and Automatic [80] [81] [84] [34] [85].

2.4.1. Manual

In the Manual level of automation, the attacker manually scans for vulnerable devices, breaking into and infecting them with the program that contains the code that will run the DDoS attack, that is, the malicious code. The attacker needs to manually start the attack, by running the installed program. This means that the attacker need do to all the work to execute the attack.

Even if there is no study to prove the most common level of automation of DDoS attacks, currently, we can forecast that semi-automated and automated levels of automation will continue to grow in usage and became dominant than manual automation level. This will happen is because automating processes/phases will bring benefits, such as less workload to the attacker in scanning, exploiting, infecting devices and/or perform DDoS attacks. Another crucial reason is the disclosure of the source codes, so everyone can have access to it, like what happen with the Mirai source code, this will allow script kiddies (i.e., unskilled personnel who used scripts and/or programs [86]) and other individuals to use semi-automatic and automatic DDoS attacks.

2.4.2. Semi-automatic

The semi-automatic DDoS attacks are represented in an agent-handler attack model, this model elements were already described, previously, in Section 2.2.

In this level of automation, the attacker automatically scans for new vulnerable devices, compromise and infect them. After these phases the attacker, through the handler device, specify the attack type, the victim's address, duration, and the onset of the attack. The handler's job is to broadcast the specifications to all agents in which on the other hand these will send the packets to the victim, realizing the DDoS attack. An example of this kind of semi-automatic attack is the Mirai Botnet [6] [87], the detailed description of Mirai is presented in Section 2.9.1.

The semi-automatic can be classified into two different types, which depends on the type of communication between handlers and agents. It can be *direct communication* or *indirect communication*, the definition of each type will be demonstrated below:

Direct Communication: In the direct communication, a handler and an agent know each other IP addresses, so they can communicate directly between them when necessary. Therefore, is necessary to transmit the IP address of the handler, this is done through the attack code which will have the handler's IP address hard coded. So, when the compromised agent receives the attack code with a propagation mechanism, it will also obtain the IP address. After getting the IP address the agents will inform the handler of their readiness, who will store each agent IP address for later communication. However, the main downside of this approach is the fact of discovering a comprised/infected device will be possible to expose all devices within the DDoS network through backtracking.

Indirect Communication: In the indirect communication, it is utilized communication services available on the Internet, such as the Internet Relay Chat (IRC), to control and synchronize agent actions. The IRC allows real-time communication with multiple people around the world within the same channel as well as between only two persons, through a text-based chat. This surpasses the drawback of the direct communication since IRC channels provides anonymity to the attacker and difficult the detection malicious communication between the legitimate packets. Also, the distributed nature of the IRC hinders the investigation of the communication making harder to find and expose the root of the attack, that is, discovering a single agent may result only in the identification of one or more IRC servers and channels used by the DDoS network.

However, over the years the number of users using IRC had a significant decline, where it is possible to verify in *Netsplit* [88], which show the number of users, channels and servers from the Top 10 IRC networks, since 1998 to 2021. The attacker can avail from this type of communication through other legitimate services similar to IRC.

2.4.3. Automatic

The automatic DDoS attacks, every phase of the scanning for new devices, exploiting, infecting and execution of the attack are automated. Therefore, the attacker does not need to establish a communication between the handlers and agents to perform an attack. The execution of the attack only requires a single command at the beginning of the recruitment phase, leading to the malicious actor having little exposure and being harder to reveal their identity.

In this level, the necessary information is already coded in the attack code, for example the start time of the attack, the type of attack, the duration and the victim's IP address. Nevertheless, the backdoor created during the propagation of the attack code will remain open, which can be further used to modify the existing attack code.

An example to execute this degree of attack is using computer worms [89], since they can replicate and spread quickly, infecting hundreds of thousands of devices and add them to a botnet, having the specific targets and the other parameters built in the worm code.

2.5. Strategies for Recruitment

The recruitment of new devices for a bot army is the first phase that malicious actors need to perform to successfully execute the DDoS attack. For this purpose, it is necessary to utilize different strategies to find new devices with some flaw to be exploited and add it to the attacker botnet.
A method that attackers mainly use is the port scanning, which is an information gathering technique, with this it is possible to gather information about the scanned devices, since they can gain information about available and responding devices as well as which ports are open.

The strategies have been evolving over time, mainly on the emergence of Internet of Things (IoT) devices, *Al-Alami et al. (2017)* [90] and *Markowsky & Markowsky (2015)* [91] demonstrate strategies to scan for vulnerabilities in IoT devices using different tools like Shodan, Nmap and Masscan.

The scan strategies can be divided in *Host Scanning*, in which the goal is to choose addresses of potentially vulnerable devices to scan, and *Vulnerability Scanning*, where we already have a built list with multiple addresses, and it goes through that list scanning each IP address one by one checking if it has any vulnerability. These strategies are used in semi-automatic and automatic levels, where we have some kind of automation. In this section, will be explained how attackers, automatically, scan for new, potentially vulnerable, devices with the objective of increasing the number of bots in their army. The *host scanning strategy* can be differentiated between *random scanning*, *hitlist scanning*, *signpost scanning*, *permutation scanning* and *local subnet scanning*. While *vulnerability scanning strategy* can be divided between *horizontal scanning*, *vertical scanning*, *coordinated scanning* and *stealthy scanning* [80] [83] [34] [92] [93].

2.5.1. Host Scanning

Random Scanning

A random scanning is when each compromised device probes random IP addresses, starting the scanning with a different seed. However, scanning randomly for new devices can lead to an increase of traffic volume and generate duplicate probes to the same IP addresses, because does not exist synchronization between the different compromised hosts. The automatic infection of this type of scanning can reach a saturation point, in which a high percentage of vulnerable devices are already infected.

A drawback is the high traffic volume may have the consequence of facilitating the attack detection.

Hitlist Scanning

Is performed by an infected computer that probes all IP addresses from an externally supplied and already build list with multiple potentially vulnerable IP addresses. This type of scanning allows a fast propagation and no collisions during the scanning phase since it sends a portion of the initial list to the vulnerable and infected device and keeps the rest.

The disadvantage is that the attacker needs to build the hitlist, previously. The information of vulnerable devices IP addresses can be collected through public information or other types of scanning strategies like stealthy scanning and distributed scanning, in the last one the already compromised devices are used to build the hitlist. Another drawback is the size of the hitlist, bigger the list, bigger the traffic volume transmitted, which in turn will facilitate the detection by cybersecurity agents.

Signpost Scanning

This scanning strategy, can be also called *Topological Scanning*, utilize information on the compromised devices to select new targets. An example is a Webserver based worm which could spread by infecting other vulnerable devices, simply by clients clicking or accessing the infected website.

The advantage when using this strategy is the low generation of traffic and therefore reduces the chances of attack detection. However, the downside is that the identification speed of new devices depends on the client's behavior and hence it is not controllable by the malicious actor, existing the probability of slower recruitment.

Permutation Scanning

The permutation scanning starts with a precompiled hitlist, how this list can be compiled was previously explained, in the definition of **Hitlist Scanning**. The initial set of compromised devices share a common pseudo-random permutation of the IP addresses, called *permutation ring*, each IP address is mapped to an index of the permutation and where each of them will scan the IP addresses one-by-one, starting in a random location, on the permutation ring.

To prevent scanning the same addresses, new infected devices will choose a random location in the permutation ring to start, ahead of their IP address, if it finds a device that has already been infected a new starting point is chosen. The reason why this occurs is to not collide with already scanned IP addresses by other infected devices, avoiding duplication of scans.

Whenever an infected host reach a threshold of already scanned devices it will become dormant to prevent further collisions.

A benefit of permutation scanning is his stealth since it does not flood the network with multiple packets to the same IP addresses (e.g., duplicate scans) and all infected devices can scan at low rate, hindering attack detection.

In the paper of *Manna et al. (2009)* [94] it is presented an extensive definition and characterization of how this scanning strategy works.

Local Subnet Scanning

The local subnet scanning can be used with the others, previously, described scanning strategies, here the difference is that the scanning is performed to find vulnerable devices in the same network as the infected device, with the main goal to infect as many devices as possible in the sub-network. Within the same sub-network, it is possible to infected multiple vulnerable devices protected by a firewall, since some firewalls only protect the traffic delivered from an external source, not giving any defense from attacks inside the network.

2.5.2. Vulnerability Scanning

Horizontal Scanning

To scan devices, the horizontal scanning focus only in a specific destination port, looking for a specific vulnerability, on all devices from a given list or using a host scanning strategy. An example is scanning the SSH port (port 22) and verify if it is open, with that information the malicious actor can then prepare, and attack known vulnerabilities in that port.

Vertical Scanning

The vertical scanning is when the infected devices scan for multiple ports on a single device. The *nmap* [95] tool can be used to perform this type of scanning, which we can retrieve the information of what ports are open in a specific IP address or target [96].

Box Scanning

Malicious attacker can combine both, horizontal and vertical scanning. Using this strategy is possible to increase the range of scanning, since it will be scanning multiple ports on several devices. Another scanning tool, besides *nmap,* that can do this scanning strategy is *Nessus* [97] where it is possible to scan multiple ports in a wide range of hosts [98].

Coordinated Scanning

This type of scan is done by multiple scanning devices with the purpose to scan for vulnerabilities in same destination port(s) of various devices within a particular local subnet (e.g., a /24 subnet). Doing this the attacker can have the knowledge of the most common vulnerabilities found within a given network and prepare a more direct attack to those vulnerabilities.

Stealthy Scanning

The main goal of this scan strategy is to avoid detection by intrusion detection systems (IDSs). The previous scans (horizontal, vertical, and coordinated) may also be stealthy through the realization of slowly scan, preventing abnormal number of traffic volume. Furthermore, modify packets can make it harder for security tools to detected uncommon traffic, for example, modify the TCP packets to utilize the FIN (FIN Scan attack) and/or NULL flags (NULL Scan attack) [95] [99], however, nowadays the IDSs can easily detect the existence of abnormal traffic when it is performed with these different types of modified TCP packets scans (e.g., NULL Scan, FIN Scan and Xmas Scan), since they are already well known by the community, cybersecurity agents and tools.

2.6. Propagation Mechanism

After completing the recruitment (i.e., identification of new vulnerable devices) is necessary to exploitation and infect them through the propagation of the attack code. By completing this step, the vulnerable devices are infected and become bots, being subsequently integrated in the botnet. Thus, whenever the attacker intends to carry out a DDoS attack it only needs to communicate through the handlers, as it is represented in the Figure 2.1.

There are three attack code propagation mechanism when infecting a device, which are called *central source propagation*, *back-chaining propagation* and *autonomous propagation*. The following papers explain in detail these three mechanisms [80] [83].

Central Source Propagation

In the central source propagation, the attack code is stored on a central server or set of servers, when an agent device is compromised, the attack code is downloaded from the central server(s) through a file transfer mechanism (e.g., *wget,* which is a software for retrieving files using HTTP, HTTPS, FTP and FTPS [100]). This propagation approach applies great burden on the central server, generating high traffic volume increasing the probability of attack discovery. Also, the central server is a single point of failure, if it is not available the transference of the attack code will be impossible. Blocking the communication between the central server(s) and the agent devices will prevent the increase of the botnet and the DDoS attack power.

Back-Chaining Propagation

When using this propagation mechanism, the attack code is propagated through the malicious device, this is the device that performed the exploitation, on the agent device. The Trivial File Transfer Protocol (TFTP) can be used to transfer the file with the attack code to the agent device. After downloading the attack code, the infected device will become the source of the next propagation step. Contrary to central source propagation mechanism, this propagation does not have a single point of failure (i.e., central server) and for this reason is more resistant to security techniques.

Autonomous Propagation

With the autonomous propagation, the agent device does not need to download the attack code, this is avoided by the attacker device directly injecting the code during the exploitation. This approach reduces the traffic volume, since is not needed the additional step of downloading the attack code, hence also reduces the probability of attack detection.

2.7. Malicious Software

The malicious software, also called **Malware**, refers to all code written with the goal to harm devices. In relation to DDoS attacks, the malware is used to infect devices with the objective to gain unauthorized access of a device, for it to be integrated in a botnet and utilized in DDoS attacks. Examples of types of malwares include *Viruses, Worms, Trojans, Ransomware, Spyware and Adware*. Nevertheless, not all the different malware types are used to add new agents to the botnet. For our work, the malware types with more relevance are *Viruses, Worms* and *Trojans*. The definition of these three types of malwares are as follows:

Virus

A computer virus is a malicious software, the primary characteristic of viruses is that they are almost always attached to an executable file, hence the virus may exist on a system but will stay dormant until the hosted executable file is executed, activating it. Once activated, the virus will propagate by inserting a copy of itself into other programs. Thus, the viruses spreads whenever this infected programs are transferred to other devices and are executed through the network, file sharing or email attachments [101] [102] [103].

Worms

Computer worms are similar to virus, in which they replicate copies of themselves and can cause harm to the infected devices.

However, the difference between worms and virus, is that virus can only spreads to another devices if the infected executable file is transferred to those devices. While worms are standalone software, therefore they do not require a host file and its execution to propagate to another devices [101] [102].

Since worms does not need a host file to be transfer to other devices to infect them, they spread through network connections, exploitation of vulnerabilities on the target system and/or a downloaded of an infected file.

Trojans

A Trojan malware is a malicious software that looks like a legitimate software, consequently, leads users to execute it on their systems. Once it is activated, is possible to achieve a large of attacks, such as *backdoor Trojans*, *dropper Trojans, banking Trojans* and many others [104].

The backdoor Trojan are often used to help malicious actors to gain unauthorized access the infected devices, hence being the Trojan type mostly used to integrate new agents to the botnets. Unlike virus and worms, Trojans do not self-replicate.

The previous described malware can be injected by the malicious actors, after exploiting the vulnerabilities present on the devices, or they can be downloaded by the users through email attachments (i.e., phishing campaigns), flash drives, vulnerable websites and drive-by download [105].

In recent years, we had a huge increase in the utilization of IoT devices, but these devices have a weak security, hence being an easy target for attackers. An example is the utilization of computer worms to infect a large number of IoT devices, in which it is referred by *Molesky and Cameron (2019)* [106].

We can conclude that computer virus and worms are powerful tools for the malicious actors to automatically infect new devices and carry out DDoS attacks. While Trojans allows the opening of backdoors, where there should not be, leading the attackers to bypass security mechanism and gain unauthorized access to the device. Thus, these malwares amplify the attack surface from where the devices can be infected, that is, when is not possible to find and exploit vulnerabilities, it can be done through social engineering that will lead the users to execute the malware for helping the attackers.

2.8. Botnet Topology

The previous strategies and techniques described in this chapter are utilized to create or increase the malicious actors and botnets, so they can perform DDoS attacks that will have a greater impact on specific victims. Thus, botnets are a crucial component in DDoS attack realm.

A botnet consists of several infected devices (i.e., bots), which are controlled by a botmaster. The botmaster is the entity that orders the botnet to execute the given instructions to carry out the malicious activities, like DDoS attacks.

The botnet allows the attackers to use several infected devices and utilizing as many bots as possible the attack size and power will increase tremendously, as well as the difficulty to mitigate the attacks, since is hard to determine which are the malicious packets of those who are from legitimate users. Thus, working with botnets are more beneficial for attacker than using just a single device to carry out the attack. It's worth noting that for the majority of the DoS attacks the host systems have already implemented mechanisms to prevent those attacks to occur.

Other reason why the botnet is more used these days by the attackers is the ease of compromising and infecting IoT devices and creation of botnet with only infected IoT devices.

The attackers to control the botnet need a *Command and Control* (C&C) server which have the objective to communicate to bots the updated instructions to carry out an attack. This ability to communicate with the infected devices in the botnet allows the attacker to modify the attack type, change the target IP address, and other crucial actions.

Botnet structure can vary, but its communication between the C&C server and the bots can be performed in three different ways: centralized, decentralized and hybrid, which is a combination of centralized and decentralized topologies [107] [108].

In general, botnets can be used for non-malicious activities, such as sending advertising spam or doing several repetitive tasks, and for malicious activities, such as DDoS attacks and brute force attacks. In this thesis, we will only focus on botnets that perform distributed denial-of-service attacks.

Centralized C&C

The centralized C&C topology have a dedicated central command and control server, in which every bot in the botnet is connected to this central server. The function of the central C&C server is to disseminate new or update the current information by all infected devices.

The C&C server is an essential piece of the botnet, it is with this server that the real attackers can control their botnets, for example sending the information about the new victim's IP address and the attack type or check the information about the availability of each bot and track their activity. Therefore, the attacker must be connected to the C&C server to execute the commands and control the botnet.

This kind of topology have advantages, one of them is the low latency since the bots are directly connected with the C&C server. Another benefit is the simple network structure, allowing high scalability and making it easy to create and manage a botnet with this topology. However, those advantages come with drawbacks, which is the low robustness, this is because the C&C server is a single point of failure. Thus, in order to dismantle the whole botnet using a centralized command and control server, it is only necessary to bring down this server. Another disadvantage is that the IP address of C&C server need to be hardcoded in the malicious code when infecting a vulnerable device, In addition, observing the network traffic of a bot is possible to detect and find the command and control server [107] [108].

To address the mentioned disadvantages some mitigation measures have been mentioned in the literature, one of those solutions is the *fast-flux* network. These mechanisms assign multiple IP addresses to the same domain name, through DNS, thus enabling different bots to be linked with a single web page.

The bots associated to the web page can be used as an intermediate point, relaying the data to the C&C server, hence only those proxy bots know the real C&C server giving an additional layer of protection to the botnet. Since registering and de-registering bots from a domain name can be done at any time, this can be used to change IP addresses linked to the domain name rapidly, increasing the complexity to take down a botnet. In addition, utilizing the *fast-flux* method transfers the single point of failure to the DNS server [108] [109]. Further information about centralized botnet improvements and their definition are out of the scope of this thesis, but those information can be found in the papers of *Vormayr, Zseby & Fabini (2017)* [108] and *Ollmann (2009)* [109].

The centralized topology uses the following communication protocols to disseminate the information to the botnet:

- **Internet Relay Chat (IRC):** This communication protocol was mostly used in the past. The botmasters utilize the channels to broadcast the commands and control their botnet in real-time, thus each bot needs to establish a connection with the IRC server. With this protocol the bots follow the *PUSH* approach, which means that when a bot connects to an IRC channel, it will remain connected and wait for the commands [107].
- **Hypertext Transfer Protocol (HTTP):** In this technique, bots will connect to a specific web server through an URL or IP address which will be an intermediate bot or the C&C server. The botmasters will post commands on those web servers and the bots will periodically connect to them to update their information or get new commands. Therefore, bots adopt a *PULL* approach, different from the approach followed by IRC bots, in which the bots do not remain connected to the web server and connect to it several times, at regular intervals defined by the botmaster [107].

Over the years, many topologies inside the centralized topology have been observed, such as *Star Topology*, *Multi Server Topology* and *Hierarchical Topology* [109] [110].

The *Star Topology* is the simplest topology, here every bot is directly connected with a single C&C server. Most of the characteristics of this topology have already been mentioned before, for instance single point of failure.

The *Multi Server Topology* is an evolution of the *Star Topology*, thus they are similar, but instead of a single C&C server, multiple C&C servers are used to provide the command-and-control functions. These C&C servers must communicate with each other to correctly manage the botnet. If one server fails or is permanently removed, the remain C&C servers can maintain and control the botnet. An advantage of having multiple servers is they can be distributed wisely amongst different geographical locations allowing a faster communication between them and the bots.

In the *Hierarchical Topology,* bots work as a proxy, they can propagate the commands communicated from the C&C server to the others, hence the C&C is not directly connected with the bots and depending on the hierarchy depth the latency can be very high, being hard to be use in real-time activities. A single bot does not have the perception of the entire botnet, making it difficult for cybersecurity agents to estimate the botnet size.

A recent example of a centralized botnet is the Mirai botnet. This botnet is comprised with four major components: the bot, the C&C server, the *loader* and the *report* server. How the bot and the C&C server work has already been described previously. Usually, for the C&C communicate anonymously with the other parts of the infrastructure through the usage of the Tor network. The role of the *loader* is to help in the dissemination of the malicious code targeting different platforms (total of 18, including ARM and x86). While the function of the *report* server is to maintain a database with the crucial information about all devices in the botnet, this server allows the botmaster through the C&C server to check the current status of the botnet (i.e., which bots are available). The article of *Kolias et al. (2017)* [6] demonstrate a deep walkthrough about the Mirai botnet and their activity.

Decentralized C&C

In this decentralized model, each infected device in the botnet behaves like a bot and a C&C server at the same time, thus each bot transmits the received commands to its neighboring bots [107]. So, we can conclude that a Decentralized C&C topology is based on a peer-to-peer (P2P) network model. Defining in a simple way the flow of this model, the botmaster sends the new or updated commands to one or multiple bots and those bots that received the information will broadcast it to the other bots. This procedure will be repeated for every bot that receive a new command, leading the botnet to a consistent state where every bot has the new information.

An example of a P2P botnet is a fully meshed botnet, in which every bot is connected to every other bot. By the fact that every bot is connected this will ensure a low communication latency, since it does not need to be transmitted through additional bots in order to every bot receive the message. Another advantage of meshed botnets is that they have a high robustness because removing an arbitrary number of bots will not take down the botnet and it will continue working correctly. But a downside is when adding and removing a bot will lead to a high number of messages due to the required changes for the botnet to be in the correct state [108].

Differently from Centralized C&C topology, the Decentralized C&C is harder to implement since it will inherit the problems of distributed systems, such as reliably deliver commands because of the unreliable network [107] [108].

Hybrid C&C

As described above, Centralized C&C and Decentralized C&C exhibit weaknesses, thus the Hybrid C&C topology combine both models to overcome those weaknesses and get the benefit of both worlds [108].

In the Hybrid C&C, there are three main components: C&C server, proxy bots and worker bots. The C&C server is a centralized server used to send commands and control the botnet, but instead of bot be directly connected to it, only the proxy bots are connected to the server, creating a new proxy layer and they are connected to each other proxy bots, being a P2P topology. The layer of the worker bots consists of the bots that will execute the tasks of the botnet, such as execute the DDoS attack. The Hybrid C&C model is very similar to the *Hierarchical Topology* of the Centralized C&C, with the difference being the P2P network between the proxy servers.

2.9. Recent Famous Botnets

We will describe four botnets, briefly, that used to carry out DDoS attacks, hence the following botnets performed at least one DDoS attack.

As already presented in the Section 2.8, botnets are a set of infected devices controlled by a botmaster to perform a wide range of tasks. The tasks are not necessarily malicious, they can be legal, such as performing a repetitive task or running non malicious scripts.

2.9.1. Mirai Botnet

The Mirai Botnet [6] is composed of four crucial components which allows it to perform efficiently. The components and their description are as follows:

- **The Bots**, which are the devices already compromised with the malware code. These bots in Mirai have two objectives, propagate the infection to other vulnerable/misconfigured devices through brute force attacks and to launch attacks to specific victim when it receives the order from the person that control the botnet, that is, the botmaster.
- **The Command and Control (C&C) server**, which allows the botmaster to control and manage centrally the whole botnet, hence, the C&C provide the information of the current state of the botnet and broadcast the changes made to the DDoS attack to the bots connected to the server. The communication to the other members of the botnet is, usually, transmitted via the anonymous Tor network [6].
- **The Report server**, is the server used to maintain a database with the details of all compromised devices in the botnet. When a new device is infected, it will directly communicate with this server.
- **The Loader**, which is the server that facilitates the dissemination of executables targeting different platforms, according to the paper of *Kolias et al. (2017)* [6] it is 18 different platforms in total. This server is used to inject the malicious binary to the victim, with the objective of infecting it.

The bots perform brute-force attacks on new IoT victims to discover the default credential through a list of 62 combinations of username-password, this full list can be checked in the Imperva report [111]. After discovering the credentials and have access to a command line, it sends various device characteristics to the report server which will be further observed by the botmaster through the C&C server. The botmaster than can issue an infect command to the loader containing all necessary details, with this, the loader will connect to the victim and instruct it to download and execute the malicious binary. Finishing this step, the botnet got a newly recruited bot that can communicate with the C&C server to receive attack commands.

To onset a DDoS attack the botmaster just need to send a command through C&C server ordering all bots to start an attack against a specific target.

In the Figure 2.2, we can see the attack flow of Mirai botnet and how the different components work together to successfully shutting down a victim. The attack flow of Mirai presented in the Figure 2.2 will be described below.

The flow 0 between the attacker and the C&C server means that the attacker utilizes the C&C server to communicate with the botnet (i.e., check the status of the botnet, perform updates, and command an attack). This flow is similar in all botnets.

The Mirai attack flow starts in flow 1, where the current bots realize brute force attacks through the usage of username/password combinations to other devices. In case the victim device is vulnerable to the brute force attack, the bots will gain access and gather information from the victim's system and send it to the Report server (flow 2). The devices that are exploit by the bots through the brute force attacks will have their system characteristics stored in the Report server.

The attacker, then check the Report server, through the C&C server, for any new information about the devices exploited by their bots, flow 3. After that, the attacker sends the malicious command to the Loader server, which will convert the malicious command in binary and relay the command to the victim (flow 4 and 5). The victim upon receiving and executing the malicious command will become a bot and being part of the attacker botnet, consequently the new bot will establish a communication tunnel with the C&C server, allowing it to receive commands directly from the C&C server (i.e., the attacker).

Finally, the attacker can onset a DDoS attack by sending the attack command to their bots through the C&C server, leading the bots to execute a DDoS attack to the victim chosen by the attacker, as we can see in flow 6 and 7.

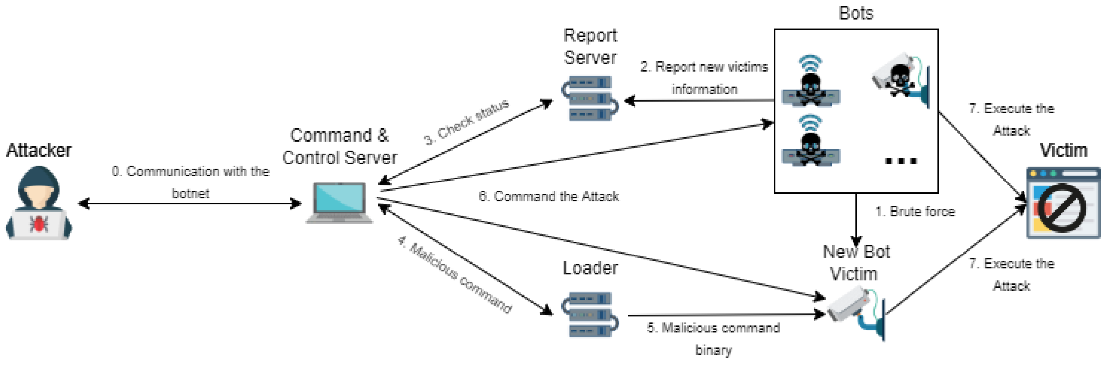


Figure 2.2. Mirai botnet attack flow

2.9.2. WireX Botnet

The WireX Botnet primarily targets were Android devices because the source of the infections came from approximately 300 mobile applications, which were available for download on the Google Play Store [112]. Security experts identified that from those 300 applications, many of them, belong to the following categories: file managers, media/video players or ringtones [113] [114]. With the application(s) installed and launching it, the malicious components embedded starts by communicating with the remote command & control server to get the attack commands. When attack commands are received, the parsing service module inspects the commands and invokes the attacking module to onset the attack with the extracted parameters.

2.9.3. Meris Botnet

The Meris Botnet is formed of infected routers and networking hardware manufactured by the company MikroTik. The attacker exploited the vulnerability in the device's operating system (RouterOS) that allows attackers to gain unauthorized remote access to read and write arbitrary files.

The vulnerability has been patched in 2018, but those devices that did not patched the RouterOS versions are still being exploited. Thus, in the newer versions of RouterOS it is no longer possible to exploit these devices, left the attacker only with the exploitation through the utilization of default usernames and passwords [115].

2.9.4. Mozi Botnet

The Mozi Botnet is a new peer-to-peer (P2P) botnet which relies on the Distributed Hash Table (DHT) protocol to build the network. The botnet spreads to multiple devices, including IoT, through two different methods, via Telnet with weak passwords and exploiting know vulnerabilities (the detailed list of vulnerabilities can be seen here [116]). After the new infected device joins the Mozi P2P network it will continue to infect other devices.

The execution of commands is done by each Mozi bot through a payload issued by the botnet master. In which, the main commands are DDoS attacks, collecting bot information, execute the payload of the specified URL, update the sample from the specified URL and execute system or custom commands.

2.10. DDoS-as-a-Service

The Cybercrime-as-a-Service open the door to a wider population of attackers, by making criminal services as tools such as any type of malware and DDoS attacks available and accessible to everyone even if they do not have the technological expertise required to perform these attacks/crimes [117].

The services are offered online, often on the dark web, but also on the clear web and are paid more often with cryptocurrencies. Currently, dark web users are adopting anonymous cryptocurrencies such as Monero [118], with this their digital footprint will be harder to track and consequently prevent the authorities to find their identities.

DDoS-as-a-Service are provided by cybercriminals, in which the criminals use their botnets to perform attacks in exchange of monetary payments. Thus, when a person with bad intentions pays for a DDoS attack service, will result in the launch of the DDoS attack targeting the indicated victim. The existence of these DDoS-as-a-Service attacks reduce the effort of other entities to manage large botnets, high-volume and complex attacks, in addition of the already mentioned benefits of these services.

The DDoS-as-a-Service provided in the dark web are much more powerful, but in the clear web (i.e., in websites accessible with a normal browser, such as Google Chrome and Firefox) we can also find these services available and accessible for everyone, DDoS-as-a-Service offered by criminals are called *Booters* [119].

An IP *stresser* differs from a *Booter*, in which an IP *stresser* is a tool utilize to test the robustness of a network or server. Thus, a website administrator can use these tools to verify if their resources are sufficient, such as bandwidth and CPU, for their business. IP *stressers* are used legitimately to test an owned website. While *Booters* are the illegitimate use of IP *stressers* [120].

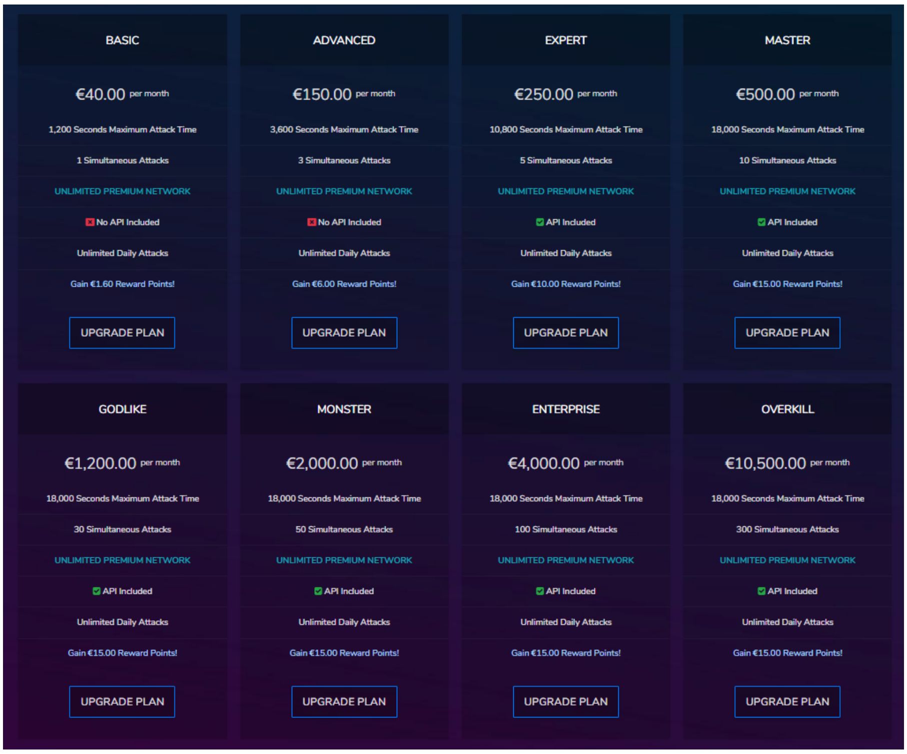
The *Booters* offers a user-friendly interface, therefore, people without any knowledge about DDoS attacks can easily order one. Additionally, *Booters* are not restricted to one type of DDoS attacks and allows the clients to choose what type of attack they want to see to be performed to their target.

In Figure 2.3 shows a price table of a Booter website, in which we can observe that the cheaper attack goes for 40€ a month, an attacker can run a twenty (20) minute attack, with an attack volume of 20 Gbps (the information about the attack volume can be seen in the highlighted box of the Figure 2.4). However, it is also possible to choose better plans, going up to as much as 10,500.00€ a month with increased benefits, which are 5 hours of attack time to 300 targets simultaneously, but with the same attack volume, 20 Gbps, as we can see in the Figure 2.5. In Figure 2.4 and Figure 2.5 are possible to verify that the vendor accepts cryptocurrencies, such as Bitcoin, and credit cards. However, currently, most of the *Booters* vendors only accept cryptocurrencies and only a few also accept PayPal [121].

Most of the DDoS attacks provided in the clear web have a low attack volume compared with the scale of the attacks mentioned throughout the work, for example the 1.1 Tbps attack to the webhost and cloud OVH [6], in 2016, or the attack of 2.3 Tbps to AWS, in 2020. Thus, organizations with some mitigation mechanism can easily automatically prevent these types of attacks from *Booters*.

We can verify the ease that anyone have in making a purchase for a DDoS-as-a-Service, since these services are not only in the dark web, but also in the clear web. Consequently, it is not necessary a great effort to find them (i.e., it is not needed a specific browser and the research is faster), comparing with the effort required to find them in the dark web.

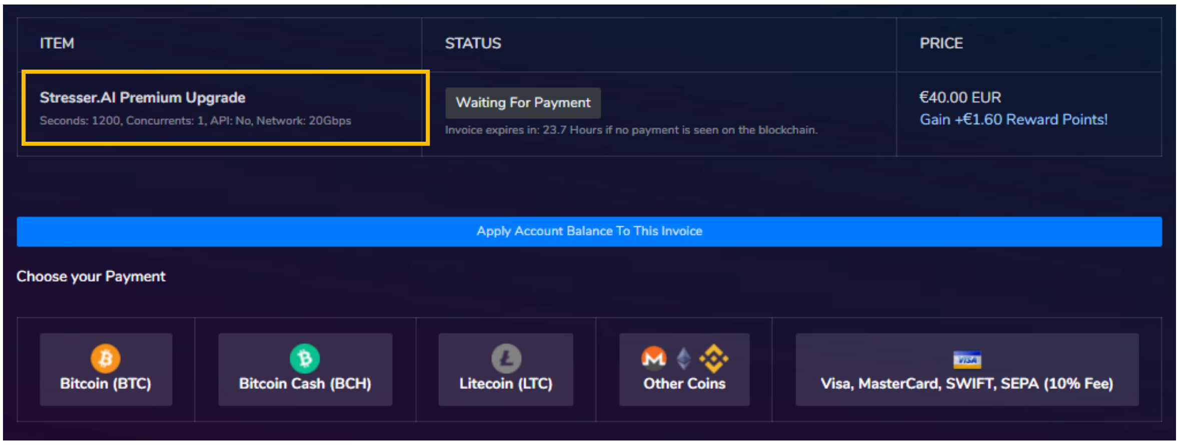
Is important to note, that Figure 2.3, Figure 2.4 and Figure 2.5, are solely for educational and exemplification purpose we do not incentive the utilization of these services against any entity without their permission.



BASIC	ADVANCED	EXPERT	MASTER
€40.00 per month	€150.00 per month	€250.00 per month	€500.00 per month
1,200 Seconds Maximum Attack Time	3,600 Seconds Maximum Attack Time	10,800 Seconds Maximum Attack Time	18,000 Seconds Maximum Attack Time
1 Simultaneous Attacks	3 Simultaneous Attacks	5 Simultaneous Attacks	10 Simultaneous Attacks
UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK
☒ No API Included	☒ No API Included	☑ API Included	☑ API Included
Unlimited Daily Attacks	Unlimited Daily Attacks	Unlimited Daily Attacks	Unlimited Daily Attacks
Gain €1.60 Reward Points!	Gain €6.00 Reward Points!	Gain €10.00 Reward Points!	Gain €15.00 Reward Points!
UPGRADE PLAN	UPGRADE PLAN	UPGRADE PLAN	UPGRADE PLAN

GODLIKE	MONSTER	ENTERPRISE	OVERKILL
€1,200.00 per month	€2,000.00 per month	€4,000.00 per month	€10,500.00 per month
18,000 Seconds Maximum Attack Time	18,000 Seconds Maximum Attack Time	18,000 Seconds Maximum Attack Time	18,000 Seconds Maximum Attack Time
30 Simultaneous Attacks	50 Simultaneous Attacks	100 Simultaneous Attacks	300 Simultaneous Attacks
UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK
☑ API Included	☑ API Included	☑ API Included	☑ API Included
Unlimited Daily Attacks	Unlimited Daily Attacks	Unlimited Daily Attacks	Unlimited Daily Attacks
Gain €15.00 Reward Points!	Gain €15.00 Reward Points!	Gain €15.00 Reward Points!	Gain €15.00 Reward Points!
UPGRADE PLAN	UPGRADE PLAN	UPGRADE PLAN	UPGRADE PLAN

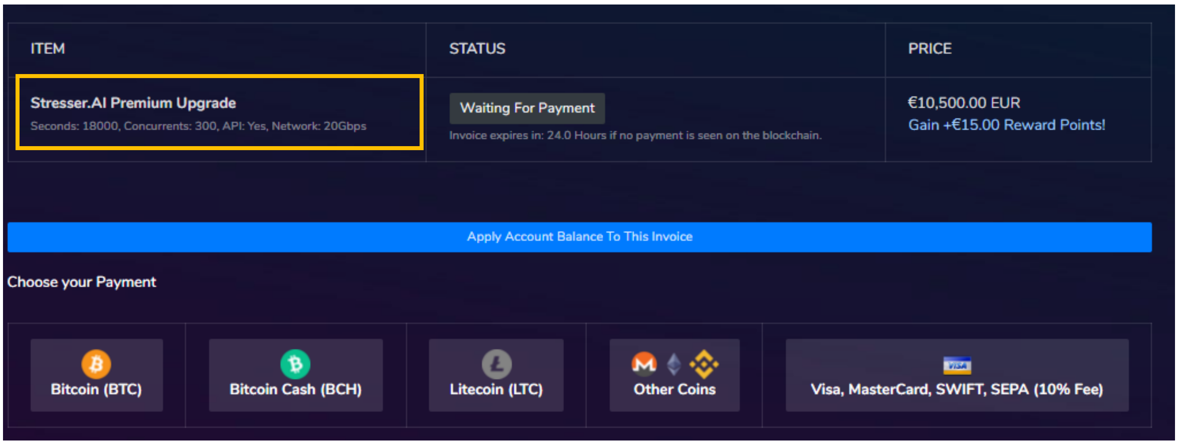
Figure 2.3. Booter Pricing Table from stresser.ai website [110]



ITEM	STATUS	PRICE
Stresser.AI Premium Upgrade Seconds: 1200, Concurrents: 1, API: No, Network: 20Gbps	Waiting For Payment Invoice expires in: 23.7 Hours if no payment is seen on the blockchain.	€40.00 EUR Gain +€1.60 Reward Points!

Apply Account Balance To This Invoice
Choose your Payment
Bitcoin (BTC)
Bitcoin Cash (BCH)
Litecoin (LTC)
Other Coins
Visa, MasterCard, SWIFT, SEPA (10% Fee)

Figure 2.4. Payment Options for the cheaper booter from stresser.ai website [110]



ITEM	STATUS	PRICE
Stresser.AI Premium Upgrade Seconds: 18000, Concurrents: 300, API: Yes, Network: 20Gbps	Waiting For Payment Invoice expires in: 24.0 Hours if no payment is seen on the blockchain.	€10,500.00 EUR Gain +€15.00 Reward Points!

Apply Account Balance To This Invoice
Choose your Payment
Bitcoin (BTC)
Bitcoin Cash (BCH)
Litecoin (LTC)
Other Coins
Visa, MasterCard, SWIFT, SEPA (10% Fee)

Figure 2.5. Payment Options for the most expensive booter from stresser.ai website [110]

2.11. Motivations of DDoS Attacks

The NetScout, the owner company of Arbor Network, which provides DDoS protection services and considered the global DDoS mitigation market leader in 2017 [122] provides a real-time DDoS attack map, called NETSCOUT Omnis Threat Horizon [123]. Similarly, Cloudflare have the Cloudflare Radar [124], which exhibit multiple graphic that shows the attacks occurred in the following intervals 24 hours, 7 days, 14 days, and 30 days. With these two tools we can verify that daily exists multiple active attacks and their dimensions. Thus, it is important to describe why malicious actors perform DDoS attacks.

The targets of these DDoS attacks can vary from smaller victims like home users or small websites to bigger and harder to attack like a country government. Moreover, the attackers have different motivations to execute the DDoS attacks to their victims, since a malicious actor attacking a small e-commerce site have different intentions and purpose that a hacker trying to break the website of a government.

The most attractive industries targeted by DDoS attacks in the second quarter of 2021 observed from Cloudflare DDoS report [125], are Consumer Services, Government Administration and Marketing & Advertising. While the most attractive targets of DDoS attacks presented in Microsoft Digital Defense Report of 2021 [16] are the Online gaming and gaming vertical.

The reasons and/or motivations for the DDoS attacks can be multiple. Below will be identified and described six different categories to provide a deep understanding of motivations behind DDoS attacks.

2.11.1. Financial gain or economic benefit

The attackers motivated by financial profit are considered the most dangerous, by the fact that they are guided by the objective of achieve financial benefits.

The Ransom Denial-of-Service (RDoS) attack [14] [64] is a new trend of DDoS attacks, actively used during 2020, in which the extortionists threaten targeted organizations to pay the ransom in a cryptocurrency, like Bitcoin, through an e-mail message. If the organizations do not meet the requested demands the attacker will start the DDoS attack, that may result in unavailability or disruption of the services, consequently, lead to a high financial loss.

Also, the increase popularity of crime-as-a-service, such as DDoS-as-a-service (DaaS) [126], especially in the Dark Web and using anonymous cryptocurrencies, such as Monero or Bitcoin, but other payment methods are also used, like Paypal or Paysafecards (provide anonymous payments), this may attract and motivate more attacker to engage and participate in these illegal activities.

2.11.1. Revenge

Another motivation for attacker to perform DDoS attacks is *Revenge*, here exists some frustration from the individuals that resort on DDoS attacks to carry out the revenge against organizations, organizations and/or individuals. In most cases, the disgruntled persons have the objective to inflict damage for some previous oppression.

2.11.2. Ideological belief

The malicious actors that fall in this category, also called "hacktivists", become motivated to attack a target because of their ideological belief (e.g., politically motivated). The main attacks of the hacktivists are against governments or politicians' websites to cause outages or disruption. A recent attack, that was politically motivated, was the DDoS attack against Zimbabwean government websites [127] [128] [129], in January 2019, by the hacktivist group Anonymous protesting against internet censorship implemented in the country.

2.11.3. Intellectual challenge

The malicious actors motivated by intellectual challenge have the intention to show off their technical capabilities, skills, and power by attacking organizations and web sites. The high availability of DDoS tools, botnets and services on the Internet motivates these attackers to conduct experiments with the latest technologies.

2.11.4. Personal enjoyment

In this type of motivation attacker intentionally disrupt victims' services with the goal of enjoy with their frustration and losses, can be characterize under the category of cyberbullying. Also, demonstrate to the victim the power of the attacker.

2.11.5. Cyberwarfare

Talking about Cyberwarfare, normally, is associated with nations or terrorist organizations which want to gain political and military advantage. The attacks in this category have the objective to commit damage and significant economic impacts on its targets. People and groups that conduct this type of attacks are, generally, well-trained, organized, experts and belong to government military or terrorist organizations. To execute these attacks governments, need to devote significant resources and time with the main goal to disrupt essential service, successful attacks may result in paralyzation of a country's cyberspace and critical infrastructure.

Besides the six motivations described, exists other reasons why people commit crimes that do not fall in any of those motivations. The scientific study area, criminology, studies and build theories to distinguish the reasons for people to fall to crimes, some theories are *Rational Choice Theory*, *Biosocial Theory*, *Psychological Trait Theory*, *Neutralization Theory*, *Hirschi's Social Bond Theory* and *Latent Trait Theory* [130], the description of the theories are out of the scope of this thesis.

2.12. Chapter Summary

In this chapter, we briefly described the main concepts of cyberattacks. After this, we introduced the type of attacks that this work will focus, which are the DDoS attacks.

We explained all the details about how DDoS attacks work, from the elements of their architecture to the different phases that are carried out in an DDoS attack. To correlate how famous botnets work with the different phases of DDoS attacks, we described the Mirai botnet attack flow.

Additionally, we demonstrated how easy and cheap is to buy a DDoS attack as a service in the clear web, as well as the motivations why malicious actors resort to this type of illegal actions.

Chapter 3
Classification of DDoS Attacks

Nowadays, exists a large variety of distributed denial-of-service attacks that can be executed to make damage to someone. Over the years, in the literature have been presented multiple different classifications [4] [81] [34] [131] [132] [133] [71] [134], this means that, currently, a single standard to classify DDoS attacks was not found in the literature.

In this chapter, the objective is to analyze the different classifications of DDoS attacks presented on the peer reviewed papers [4] [81] [34] [131] [132] [133] [71] [134], articles and white papers [60] [135] [136]), introducing a well-defined and, mainly, easy to understand classification. Thus, we will divide the twenty-seven (27) DoS/DDoS attacks, defined previously in Sections 2.1.4 and 2.1.5, in their respective categories. We will not consider the Ransom DDoS attacks and Blended Attacks in the classification, since they can utilize any of the 27 DDoS attacks, and neither Zero-day DDoS attacks because in these attacks we do not have any information.

With the definition and classification of the DDoS attacks, it is expected to help cybersecurity agents to better understand how the different DDoS attacks work and consequently develop themselves to provide more efficient ways to protect their costumers and services.

3.1. Categories of DDoS attacks

3.1.1. Bandwidth Depletion and Resource Depletion

In the papers of *Mahjabin et al. (2017)* [34], *De Donno et al. (2017)* [131] and *Asosheh & Ramezani (2008)* [132] they classify the attack types as two different categories, *Bandwidth Depletion* or *Resource Depletion*.

In the *Bandwidth Depletion*, the attacker sends a huge volume of packets to a victim or victims, with the intention to overwhelm and consume the victims network bandwidth, resulting in the legitimate packets to be blocked and not reaching the victims services. These attacks can be divided into *Flood* (e.g., UDP Flood Attack and ICMP Flood Attack) and *Amplification* (e.g., DNS Amplification Attack and NTP Amplification Attack).

While in the *Resource Depletion* is used to overflow the victims' major resources, such as memory, sockets and CPU, with the objective to prevent the victim to process legitimate requests, leading to not being able to provide the services. These attacks can be characterized as *Protocol Exploit* (e.g., SYN Flood Attack and HTTP Flood Attack) and *Malformed Packet* (e.g., LAND Attack and Ping of Death Attack).

Thus, in short, the difference between *Bandwidth Depletion* and *Resource Depletion*, is that the *Bandwidth Depletion* attacks aim to flood the victim’s bandwidth, while the *Resource Depletion* aim to exhaust and consume the victim’s resources.

However, DDoS attacks can affect both, the bandwidth and resources, of a target and moreover it depends on the amount of available bandwidth and resources that the victim’s server has. Therefore, a SYN Flood Attack, which is classified as a Resource Depletion, can consume the network bandwidth of a server first than its resources, in this case the victim has a small bandwidth. For this reason, we will not classify the attack types in *Bandwidth Depletion* and *Resource Depletion*.

3.1.2. Volume-based Attacks, Protocol Attacks and Application Attacks

On the other hand, the following authors *Peng, Leckie, & Ramamohanrao (2007)* [133] and *Yusof, Ali, & Darus (2017)* [134]. Also the white paper done by Imperva [60], in 2015, and the articles in the AT&T Cybersecurity [135] and Cloudflare [136] the DDoS attacks are classified as *Volume-based Attacks*, *Protocol Attacks* and *Application Attacks*.

The *Volume-based Attacks* are the attacks that simply generate a large amount of traffic to saturate victims’ available bandwidth, causing that legitimate traffic do not reach the victims services, examples of these attacks are UDP Flood Attack, DNS Amplification Attack and ICMP Flood Attack. This category is measured in bits per second (bps).

Protocol Attacks have the main focus to exhaust and consume the processing capacity, other resources and exploit weaknesses in the protocols of Layer 3 and Layer 4 from OSI Model found on victim's server or intermediate infrastructures, such as firewalls, hinder the server to process valid request and denying the provided service, this includes SYN Flood Attacks and Ping of Death Attack. Thus, the attacks in this category are measured in packet per second (pps).

The last one, *Application Attacks*, in this category of attacks, the application layer (Layer 7 from OSI Model) vulnerabilities are exploited, by opening connections and/or consuming the target resources through requests, making them utilize a large portion of the available processing power, preventing real customers to access their services, attacks like HTTP Flood Attack and SIP Flood Attack are part of this category and in here, attacks are measured in requests per second (rps). This has also drawbacks, in which we do not have as much information or a list represented in the literature, of which attacks belong to each category, compared with the previous categorization, and not all attacks fit perfectly in a single category, there are different opinions.

Summarizing, the *Volume-based Attacks* consists of flooding the victim’s bandwidth, the *Protocol Attacks* has the objective to exhaust and consume the victim’s resources in Layer 3 and Layer 4 and the *Application Attacks*, also exhaust and consume the victim’s resource, but in these attacks the focus in the Layer 7. Thus, we can indicate that *Protocol Attacks* and *Applications Attacks* differ in the attacked layer.

3.2. Classification of DDoS Attacks

None of the above two categorizations is better than the other, different authors have different ways of defining their ideas. However, in this thesis we will classify the attacks as *Volume-based Attacks*, *Protocol Attacks* and *Application Attacks*, since, in our opinion, this categorization is more simple, understandable, and less subjective, even if it has the mentioned downside.

There are attack types not yet classified in the literature, hence, those attacks will be classified and justified, why it belongs to a certain category, in this chapter through our personal interpretation. This will be the first paper with this large number of attack types (27) described and classified in the three categories.

The Table 3.1 and Table 3.2 shows the classification of attack types using the two classification approaches mentioned above. Since some of the attacks described and classified in this work were not previously classified, that is, were not mentioned in which classification category it belongs (*Bandwidth Depletion or Resource Depletion*), we split up the attacks in two different tables, Table 3.1 does only the comparison between the attacks that were already mentioned and classified in the literature. While the Table 3.2 compares the attacks that are not classified in the literature, we will explain for each attack not classified, why we inserted them in *Bandwidth Depletion* or in *Resource Depletion*.

We can verify, considering the definition of each category performed above, that when DDoS attacks are classified in the literature, as *Bandwidth Depletion*, it refers to *Volume-based Attack*. While an attack classified as a *Resource Depletion* will be a *Protocol Attack* or an *Application Attack.*

The CHARGEN Attack, SNMP, SSDP, LDAP, CLDAP and MSSQL Amplification Attacks are not explicitly classified in the literature, but amplification attacks in general are mentioned. Amplification attacks works similarly with the main idea of generating a large response from a small request. Thus, we classified these amplification attacks as a *Bandwidth Depletion*.

The remaining five attacks, DNS Flood Attack, NTP Flood Attack, QUIC Flood Attack, SYN/ACK Flood Attack and UDP Fragmentation Flood Attack, have similar objective which is attempting to consume and exhaust the victim resources by sending a large number of messages, hence we classified then as a *Resource Depletion*. The in-detail definition of how these attacks work as already described previously, in Section 2.1.4 and 2.1.5.

The Table 3.1 and Table 3.2, already shows each of the 27 DoS/DDoS classified in their respective category, in our perspective. So next, we will explain for each attack the reasons why we classified it in *Volume-base Attack*, *Protocol Attack* or *Application Attack* category.

Table 3.1. Comparison between the DoS/DDoS attack classifications, with the attacks classified in the literature

	Volume-based Attacks	Protocol Attacks	Application Attacks
Bandwidth Depletion	Fragle Attack Smurf Attack ICMP Flood Attack UDP Flood Attack DNS Amplification Attack NTP Amplification Attack	-	-
Resource Depletion	-	LAND Attack Ping of Death Attack Teardrop Attack SYN Flood Attack ACK Flood Attack	R.U.D.Y Attack (Slowpost Attack) Slowloris Attack HTTP Flood Attack HTTP Fragmentation Attack SIP Flood Attack

Table 3.2. Comparison between the DoS/DDoS attack classifications, with attacks not classified in the literature

	Volume-based Attacks	Protocol Attacks	Application Attacks
Bandwidth Depletion	CHARGEN Attack SNMP Amplification Attack SSDP Amplification Attack LDAP Amplification Attack CLDAP Amplification Attack MSSQL Amplification Attack	-	-
Resource Depletion	-	QUIC Flood Attack SYN/ACK Flood Attack UDP Fragmentation Flood Attack	DNS Flood Attack NTP Flood Attack

3.2.1. Volume-based Attacks

Smurf Attack

Unlike the classification of this attack type as a protocol attack by *Yusof, Ali, & Darus (2017)* [134], we consider this attack as a volume-based attack, since the reflectors produce a large traffic volume flooding the victim's network bandwidth and not necessarily consume the available resources.

Fraggle Attack

Similarly, with the Smurf Attack this is also considered a volume-based attack, by the fact that the attack process is equal with the only difference being the protocol used.

ICMP Flood Attack

This attack has already been classified by *Yusof, Ali, & Darus (2017)* [134] and the article of AT&T [135] as a volume-based attack. We agreed with this classification, since the ICMP Flood attack will fill the victim’s network with huge number of bogus packets.

UDP Flood Attack

As well as the ICMP Flood attack, the UDP Flood attack has already been classified by the same authors [134] [135] as a volume-based attack. Since the UDP Flood attack is similar to ICMP Flood attack, just differing in the type of packets used, makes sense to classify this attack as volume-based attack.

DNS Amplification Attack

In the article presented by Cloudflare [136], the DNS Amplification attack is classified as a volume-based attack, because this attack generates more and larger responses, with the help of the DNS servers which will be sent to the victim. Thus, based on this article, we classified the DNS Amplification Attack as a volume-based attack.

NTP Amplification Attack

This attack is very similar with DNS Amplification attack, therefore it will produce a large amount of traffic volume with big packets, causing the network bandwidth to flood only with these bogus packets and for this reason we classified it as a volume-based attack.

CHARGEN Attack

The CHARGEN Attack, in our classification is inserted in the volume-based category, since the reflectors will flood the victim with UDP packets saturating the network bandwidth.

SNMP Amplification Attack

In this amplification attack, the reflectors produce bigger packets due to the queries sent by the attacker, that consequently will be sent to the victim. Those big packets will overwhelm and eventually hinder legitimate packets from clients, hence we classified the attack as a volume-based attack.

MSSQL Amplification Attack

In the MSSQL Amplification Attack, it is utilized the Microsoft (MS) SQL Servers as reflectors to flood the victim's network with response packets that have information about the instances in the abused MS SQL servers, that is, the more instances in the abused MS SQL servers, the greater will be the traffic volume, hence we classified this attack as a volume-based attack.

SSDP Amplification Attack

We classified this attack type as a volume-based attack because the attacker sends queries to the reflectors, to make them produce larger packets, that will be further used to flood the victim bandwidth.

LDAP Amplification Attack

This attack was classified as a volume-based attack because it will use the reflector to produce big messages with the information they retrieved, which will be sent to overwhelm the victim.

CLDAP Amplification Attack

The CLDAP Amplification attack is very similar with the LDAP Amplification attack, having only one difference, the transport protocol used, hence we classified this attack also as a volume-based attack.

3.2.2. Protocol Attacks

Local Area Network Denial (LAND) Attack

The LAND Attack, in our interpretation, is a protocol attack by exploiting a vulnerability (i.e., accepting a packet with the same source and destination IP address) to crash the victim's device using the network layer protocol, TCP.

Ping of Death Attack

We classified this attack as a protocol attack, as also *Yusof, Ali, & Darus (2017)* [134] and AT&T Cybersecurity [135], in which it exploits the vulnerability of sending a data packet larger than the max size expected, resulting in the crash of the victim's device.

Teardrop Attack

The Teardrop Attack, we considered as a protocol attack and the reason is because it exploits a vulnerability by manipulating the fragmented packets in TCP, making the victim's device to crash.

SYN Flood Attack

The SYN Flood Attack was already been classified in the literature [134] [135] [136] like a protocol attack. This is not a volume-based attack because it exhausts, primarily, the resources of the victim's server, more specifically, the memory instead of the network bandwidth, because the victim's server needs to store the information about the SYN packets in TCP three-way handshake.

SYN/ACK Flood Attack

This attack was classified as a protocol attack, since it exploits, mainly, the vulnerability of sending packet out-of-order to consume the available resources, through the necessity of process each received packet.

ACK Flood Attack

Similar to SYN/ACK Flood attack, this attack will send packet out-of-order to make the victim's server consume resource to verify each packet, hence we classified this as a protocol attack.

UDP Fragmentation Flood Attack

The UDP Fragmentation Flood Attack was classified as a protocol attack, because of the high resource consumption by the victim's server since it needs to store the fragmented information and try to re-build the fragmented packet.

QUIC Flood Attack

In this attack type, we classified it as a protocol attack, since QUIC is a transport protocol and floods the victim's server with packets, but with QUIC the server will need to process each encrypted packet. Eventually, the server will cannot handle to process every packet and deny legitimate packets.

3.2.3. Application Attacks

R U Dead Yet? (R.U.D.Y) Attack

This attack, focus on sending slow requests to websites (i.e., application layer) making it keep the connection open and exhausting the victim's resources, therefore, undoubtedly, in our perspective, belongs to the application attacks category.

Slowloris Attack

Similarly, to the R.U.D.Y attack, this attack affects the application layer by opening connection and maintaining it open longer as possible, disrupting the victim’s services. Hence, we and the authors *Yusof, Ali, & Darus (2017)* [134] classified it as an application attack.

DNS Flood Attack

The article by G-Core Labs [137] classified the DNS Flood attack as a volume-based attack, however, in our opinion this attack is inserted in application attack category, since the attack it is used at application layer to flood domain name servers, which have a crucial role in accessing websites, resulting in the impossibility of the customers to reach the DNS server and consequently could not resolve the domain name of a website.

NTP Flood Attack

The NTP is an application, in which the attacker floods the NTP Servers with NTP packets with the goal to prevent clients to communicate with the NTP servers by exhausting the systems and network resources.

HTTP Flood Attack

The HTTP Flood Attack has already been classified as an application attack by AT&T [135] and Cloudflare [136], the explanation is that the attack sends requests to the victim's website with the objective to consume all available resources.

HTTP Fragmentation Attack

The HTTP Fragmentation attack consume the resources of the web application by opening and maintaining as many connections as possible, for this reason we classified this attack as an application attack.

SIP Flood Attack

This attack was classified as an application layer attack since the SIP is used in application layer services. Hence, those services will be affected when SIP servers are attacked, this means that the attacker will flood the SIP registration servers to disrupt the victim's services.

3.3. Chapter Summary

In this chapter, we presented two different categorizations of DDoS attacks mentioned in the literature (peer revied papers, articles, and white papers) and from those two categorizations we chose the one that would be more intuitive and classifying DDoS attacks. This led us to classifying each of the 27 DDoS attacks defined in Sections 2.1.4 and 2.1.5.

Having already the understanding of how DDoS attacks work and how DDoS attacks are classified, we now need to understand how real-world companies fight against DDoS attacks so we can develop a framework for companies to protect themselves against DDoS attacks, which is the principal objective of our work.

Therefore, in the next chapter we will describe each of the tools, method and techniques that will help the companies to fight against DDoS and they will be used in our framework.

Chapter 4
DDoS Solutions

The purpose of this section is to present and demonstrate different DDoS solutions utilized to prevent, detect, and mitigate DDoS attacks and group them in their respective categories, as well as referring the strong points and drawbacks of the solution in each category.

Over the years, DDoS solutions evolved with the support and research of cybersecurity agents, academic researchers, and other researchers. The efforts to upgrade and evolve DDoS solutions by different entities have the objective to respond to the needs of the real-world problems and to face the new adversities.

These problems and adversities can be originated by the usage of new technologies that bring with them new vulnerabilities or because of the persistence of malicious actors to find new ways to exploit unknown vulnerabilities leading to an increase of their attack power through the increase of new bots and/or reflectors, but also it can be through finding novel DDoS attack types that have not been seen before, these attacks are called Zero-days DDoS attacks.

Zero-days DDoS attacks can cause a greater impact than known attacks to the companies, since most of the companies' DDoS protection mechanisms are trained and tested using the attacks that already exist and known by the community, while novel attacks that are unknown to the cybersecurity agents cannot be used in the training and testing of the protection mechanisms, therefore is not possible to determine if the implemented defense will be efficient to protect against the new DDoS attack type.

Currently, we have at our disposal to use, a huge number of different DDoS mechanisms/solutions to protect companies from DDoS attacks. Nonetheless, each specific DDoS solutions do not protect the company entirely, that is, a solution do not cover all types of DDoS protection, the DDoS protection types are the following: prevention, detection, mitigation, and tolerance. Thus, companies utilize multiple solutions to cover the gaps of different solutions.

With the analyze of the questionnaire we verified that every participant selected that their companies utilize DDoS commercial solutions, therefore it is important to provide them as an option in our framework, since most of the companies will resort to these solutions. However, for companies that do not want to pay for commercial solutions or for other reasons, we will also utilize open-source methods and tools in our framework.

We can say that DDoS protection mechanisms that companies can rely on can be inserted/divided in three (3) categories: DDoS commercial solutions (for example: Akamai, NetScout and Cloudflare), Open-Source and Freeware DDoS solutions (for example, Snort, Suricata and HAProxy) and solutions which we do not have access or do not exist an usable implementation/application, but are described in detail on papers and presented in Conventions and Organizations, such as, Springer or IEEE. These papers can also be found in other locations, like Google Scholar, ACM Digital Library or Wiley Online Library. We will call this solution category – Other Solutions described in the Literature.

In this chapter, we will describe the benefits and present examples of the three categories mentioned previously. From the DDoS solution presented in each category, we will designate the type of DDoS solution that it was design for, that is, if the solution is for prevention, detection, mitigation or tolerance. Finally, we will complete the chapter by defining our proposed DDoS framework, which describe different paths that cybersecurity agents need to take in consideration before choosing the DDoS solutions.

4.1. DDoS Commercial Solutions

The usage of commercial solutions has some benefit that the other two categories does not provide. The benefits of DDoS commercial solutions are:

- Companies that purchased a DDoS commercial solution does not need to provide any type of specialized training to their personnel, which leads to financial costs and time consumption, so that they can utilize correctly and effectively DDoS tools. Since the company purchase a service and therefore the DDoS commercial solution company supports their clients with specialized agents dealing with DDoS attacks, with this companies do not need to worry about another burden.
- DDoS commercial solutions companies can utilize their client network to enhance their protection mechanisms, in which observing a novel DDoS attack in a client, it is possible to communicate the new attack to other clients and update the solutions, so the next client attacked by the DDoS attack is protected.
- Behind commercial solutions exists groups of specialized cybersecurity agents that are attentive to new threats (i.e., Threat Intelligence) and continuously update their solutions, so that they can defend companies from novel DDoS attacks.

The companies can offer their DDoS commercial solutions to clients in three different ways: on-premises, cloud or hybrid. The hybrid are the solutions that can provide a combination of protection mechanisms on-premises and cloud. It is important to note that on-premises the solution hardware is located in the company site, while cloud solution it is the usage of scrubbing servers to clean malicious traffic.

Companies that want to protect their services from DDoS attacks need to analyze and understand which type of solution, on-premises, cloud, or hybrid, will suit better to their needs considering their budget, since on-premises and cloud solutions have drawbacks and benefits. While hybrid solutions, that utilize both, on-premises, and cloud solutions, to compensate their weaknesses leading to an increase of the price.

The principal benefit of using cloud solutions is protect companies from massive flood attacks that reach many Gbps and some Tbps, since these days the size of DDoS attacks are growing. Nevertheless, it has other benefits, such as the fast deployment of the solution and the possibility of only using the solution on-demand, hence only when the companies are facing a DDoS attack is that the solution is used, with this the company can spend less money when they are not attacked, but when attacked the value can increase tremendously, being a crucial point to discuss with the vendors when buying a DDoS cloud solution.

While the drawbacks of cloud solution, which utilize scrubbing centers, are the speed of the network is affected (increase of latency), since the scrubbing servers may be located at a considerable distance from the company’s site, slow post attack (application layer attacks), for example a HTTP Fragmentation attack, that sent packets slowly by disguising themselves as legitimate traffic can go undetected by not triggering the defined thresholds and for the companies that their services work with confidential, private information cloud solutions is not an option, since that information need to travel to those scrubbing servers and be decrypted for it to be cleaned and the increase of the price charged by attack size [138].

On the other hand, the benefits of on-premises solution are that the solution is located on the companies site performing immediate and automatic attack detection and mitigation, including the slow post attacks and minimal latency during peacetime or with an attack. However, the drawback is that the hardware cannot handle large-sized volumetric attacks.

The hybrid solution came to solve the problems/drawbacks of on-premises and cloud solutions, by combining them and using the best of both solutions. In the hybrid solution, the on-premises hardware performs the first layer of detection and mitigation of DDoS attacks, whenever the on-premise hardware became saturated, by an volumetric attack or by multiple attacks, it will redirect the traffic to the cloud, where it is scrubbed and sent back to the company.

As we mentioned before, currently, companies have a wide range of DDoS commercial solution from different companies to choose from. Thus, from those companies we selected seven, in which we categorized them in the following groups:

- **Main DDoS Companies:** companies that their core business are DDoS solutions, and they are known because of those solutions.
- **Competitive DDoS Companies**: companies that when appeared their core business are not DDoS solutions. Nonetheless, they are companies that focused in offering solutions in the cybersecurity field and entered the DDoS solutions market by evolving their solutions, making them offer competitive functionalities.
- **Cybersecurity Companies:** companies that their business is focused on security aspect, therefore even if they provide DDoS solutions, it is not their strong point.

The companies that we selected are: NetScout (former Arbor Networks), Akamai, Radware, Imperva, Cloudflare, F5 and Check Point. They are categorized as the following:

- Main DDoS Companies – NetScout (former Arbor Networks) and Akamai.
- Competitive DDoS Companies – Radware, Cloudflare and Imperva.
- Cybersecurity Companies – F5 and Check Point.

The information that we will present about the company's DDoS solutions, are the information that it is available and can be found on the internet. Since we could not test the solutions, consequently, we could not perform a deeper analysis about how the solutions works and their functionalities, as well as, describing them.

We contacted Imperva to verify if we could get free access to a DDoS solution demonstration and a Imperva agent responded to our request, but the response was not what we expected. We receive a couple of questions, asking about our infrastructure and network, two of the questions sent by Imperva are the number of sites/domains we want to protect and the amount of clean bandwidth in MB per second. The complete Imperva's response email to our request for the DDoS solution demonstration can be verified in the Appendix B, Figure B.10.

Thus, for we to receive and test the Imperva DDoS solution demonstration, we need to answer to those questions and provide that information, so the Imperva could supply their solution correctly, that is, matching the client's company needs. Nonetheless, we did not have the information to respond to the questions and consequently we could not get the access to the DDoS solution.

With this experience, we understood that for we to test any DDoS commercial solution we need to setup an infrastructure with the information about the amount of clean bandwidth traffic, location of the protected assets, number of assets and expectation budget, at least. Since, we were not able to respond

Imperva's initial questions, therefore we do not know if we would receive more question about our infrastructure and what type of questions it would be.

The reasons we mention above described why we could not test a DDoS commercial solution and characterize their functionalities, this led to this work only defining the solutions through the information we could find on the internet.

It is important to note, that the prices for the DDoS solution will vary depending on the infrastructure, hence we also do not have information about the specific prices that vendors charge for DDoS solutions neither indicating what are the cheapest and most expensive.

The work of the authors *Bhardwaj et al. (2021)* [78] mentioned that NetScout, Check Point and Imperva as very expensive solutions, whereas the Cloudflare solution have competitive pricing. However, we do not have information about the parameters utilized by the author to classify a solution as expensive or not.

We have very little available information about DDoS commercial solutions, without being the information made available by the organization itself explaining the characteristics and functionalities of their services. The only report we could get free access, from a trustful, known and impartial source was the report "DDoS Mitigation Solutions", in first quarter of 2021, by Forrester Wave [139].

The Forrester Wave report present a table that classify solution functionalities/services provided currently by the vendors, on a scale of 0.00 to 5.00. Where 0.00 means that the vendor does not provide that service, while 5.00 represent that the service performs what is intended to do and being one of the best in the market.

Next, we will describe for each DDoS commercial solutions the functionalities that are provided, according to the vendors' websites.

4.1.1. Main DDoS Companies

NetScout (former Arbor Networks):

The NetScout, which acquired Arbor Networks, offers DDoS solutions on-premises, on cloud or both, that is, hybrid by combining both solutions.

The NetScout on-premises solution is the *Arbor Edge Defense* (AED) [140], which is deployed between the companies' internet router and network firewall. The AED appliance due to the location where it is deployed and for being stateless will process every packet every packet that enters and leaves the company as an isolate packet, hence it will detect and stop DDoS attacks and communications between an internal compromised device and the C&C server.

With the on-premises appliance Arbor perform the decryption of packets, consequently blocking malicious packets that could bypass the security measures if were not decrypted.

On the other hand, the cloud solution from NetScout, called *Arbor Cloud* [141], utilize cloud scrubbing centers from 14 locations worldwide to clean the malicious traffic, providing over 11 Tbps of DDoS attack mitigation capacity. Whenever companies are under attack, the malicious traffic is redirected to the cloud scrubbing centers to be clean and then forward to the victim/client.

The hybrid solution is created by using both solutions, thus the monetary value of this solution will be higher the using only one. In the NetScout hybrid solution, the AED will be used to protect from protocol DDoS attacks and application DDoS attacks, while the Arbor Cloud will mitigate volumetric-based attacks.

The in-depth description of the flow of the hybrid solution can be seen in [142], but in short, when the AED detects a volumetric-based attack it performs a *Cloud Signaling* (developed by NetScout in 2011) that allows communication between the on-premises DDoS solutions and cloud solutions, with the *Cloud Signaling* the volumetric-based attack will be redirected to the cloud scrubbing server, while the remaining attacks will be mitigated by the on-premise appliance.

The NetScout have a Threat Intelligence team (ATLAS [143]), which updates millions of IP reputation indicators of source/port combinations that are actively propagating specific DDoS attack vectors anywhere in the world. This DDoS IP reputation data can be used to block specific attack vectors automatically and surgically.

In the report of the Forrester Wave [139], NetScout chose not to participate in the assessment, therefore we do not have a concrete estimation about their DDoS solutions capabilities. However, due to its very known presence in the field of DDoS solutions and the from the older SPARK (Strategic Performance Assessment and Ranking) matrix from 2019 by Quadrant Knowledge Solutions [144] we can refer that NetScout (former Arbor Networks) have a great market presence and be considered a Leader among the other Leaders classified by Forrester Wave.

Akamai:

The Akamai only offers a on cloud DDoS solution, called *Prolexic* [145], which utilize 19 cloud scrubbing centers distributed globally, having 8 Tbps of dedicated mitigation capacity. Each cloud scrubbing center will proactively perform mitigation controls to drop all malicious traffic, the remaining traffic will be analyzed by Akamai staff, which will drop detected attacks. After the traffic was cleaned, it will be forward to the origin application.

The flow of *Prolexic* can be described as follows: the inbound traffic will be routed to the closest scrubbing center where malicious IP addresses are identified and blocked, when the traffic from the multiple scrubbing centers are cleaned it will be forwarded to the client through virtual Generic Routing Encapsulation (GRE) tunnels or Virtual Leased Lines, the explanation about these communication methods are out of the scope of this work, but more information about these point-to-point communication can be found in [146] and [147], respectively.

The Akamai gather Threat Intelligence information through 233,000 servers across more than 130 countries that are observing the network traffic around the world, this led to Akamai being one of the few organizations with a better global view of the Internet traffic [148]. The Akamai also gather Threat Intelligence at third parties, network traffic, monitoring underground forums for information related to upcoming attacks (look for attackers targeting specific organizations, learn the attacker's timeline, monitor for the attacks).

The Forrester Wave report [139] performed the assessment to the Akamai DDoS solutions, in which we can verify in the report that Akamai is one of the Leaders compared with other DDoS solutions vendors and with a great market presence. Akamai received 5.00 score points in "*volumetric scrubbing*" and "*threat intelligence*" by Forrester Wave analysts, this means that Akamai DDoS solution is very effective in mitigating volumetric DDoS attacks, as well as, finding new threats on the wild. However, it only received a score of 3.28 in "*detection and attack mitigation*".

4.1.2. Competitive DDoS Companies

Radware

The Radware offers on-premises, on cloud and hybrid solutions.

The Radware on-premises DDoS solution hardware is called *DefensePro* [149]. The solution utilizes a behavior-based detection technology, instead of signature-based detection, which allows the companies to detect attacks more accurately and minimizing the false positive rate.

The Radware cloud solution [150] utilizes 16 scrubbing centers distributed globally with 10 Tbps DDoS mitigation capacity. The scrubbing centers are globally connected in full mesh mode, using Anycast-based routing with this will ensure that attacks will be mitigated close to the attack origin.

The Radware cloud solution can be flexibly deployed, that is, can be deployed on-demand or be always-on. In the on-demand, the solution will only be activated during an attack (i.e., during the attack the traffic will be routed to the scrubbing centers), and it is for companies that are looking for low-cost solutions, while the always-on, as the name implies, the solution is always-on and the traffic is always routed to the cloud scrubbing centers.

The Radware hybrid solution utilizes the on-premises and cloud solutions, with this the companies will have minimal induced latency in peacetime, since the redirection of the traffic to the scrubbing centers only occurs when a volumetric DDoS attack aims to saturate the client bandwidth, and the detection and mitigation of DDoS attacks will be performed faster, in real-time, with the on-premises appliance.

The Radware solutions provides a capability that differentiates from other solutions, which is the capability of detecting, characterizing and mitigating SSL attacks without the need of SSL decryption, called Keyless SSL Protection [151], this works because the algorithm learns and automatically creates a baseline during peacetime based on applicative traffic. This will be a huge differentiator factor for companies that the privacy and confidentiality of the traffic information is crucial of their business.

However, Radware provides other 3 modes for SSL protection, which are:

- First Request SSL Protection – Decryption of the request only under attack and only on the first request of each session to authenticate legitimate users.
- Full SSL Protection – Fully decrypts all suspicious sessions when under attack.
- Selective Full SSL Protection – Decrypt all SSL sessions towards a protected object and applies all protections on the cleartext traffic. This can be done always, under attack or on-demand.

Radware was classified as a Leader in the DDoS solution market by Forrester Wave [139]. It received a 5.00 score point at "*detection and attack mitigation*", therefore Radware solution it is one of the best DDoS solutions, currently, at detecting and mitigating DDoS attacks more effectively. But it falls behind at "*volumetric scrubbing*" and "*threat intelligence*" with 3.60 and 3.00, respectively.

Cloudflare

Cloudflare offers three cloud solutions to protect companies against DDoS attacks [152], which are the following:

- *Cloudflare DDoS Protection for Web Applications*: This solution it is used to protect websites, APIS and web applications (Layer 7) from DDoS attacks. The advantage of utilizing this solution by clients will not increase the charged price when there is a period with attack traffic.
- *Cloudflare Spectrum*: This solution works in the transport layer (Layer 4), and it is a reverse proxy, hence it provides DDoS protection for any application that runs over a TCP/UDP protocol. To make the traffic arrive faster to the destination, the solution is integrated with the Argo Smart Routing, which provides congestion avoidance through routing decision informed by real-time network conditions [153].
- *Cloudflare Magic Transit*: This solution is used in the network layer (Layer 3) to protect on-premises, cloud, and hybrid networks from DDoS attacks. *Magic Transit* introduces a solution where it is not utilized dedicated scrubbing centers, the Cloudflare let every single server participate in mitigation, load balance DDoS attacks across the centers and servers within them and then apply smarts to the handling of packets. Additionally, every Cloudflare servers runs the full stack of Cloudflare services, meaning that the traffic only needs to go to the nearest Cloudflare server and consequently not creating the trombone effect.

The Cloudflare’s network has a capacity of over 155 Tbps distributed by 100 countries and this network it is used to provide DDoS mitigation.

The Forrester Wave assessed the Cloudflare DDoS solution, in their report [139], they classified the Cloudflare as a Leader in the DDoS solution market. Cloudflare solution “*volumetric scrubbing*” and “*detection and attack mitigation*” are not considered the bests by Forrester Wave, but still received high scores, 4.20 and 4.16, respectively. Nevertheless, Cloudflare “*threat intelligence*” still lack improvements compared to Akamai and Imperva, only scoring 3.00. Thus, Cloudflare DDoS solution is still a viable and reliable option for DDoS protection, but companies that opt to utilize this solution should also acquire a threat intelligence solution from another vendor.

Imperva

Currently, Imperva do not offers on-premises solution, but it offers four different cloud solutions for DDoS attacks [154], in which three of them are *Website Protection*, *Individual IP Protection* and *DNS Protection*. These solutions protect specific websites, a single IP and DNS, respectively, therefore they are more granular solutions.

The last one is the *Network Protection*, where it is used cloud scrubbing centers with over 9 Tbps of mitigation capacity. The client’s traffic will go through the scrubbing centers of Imperva to be clean and then forward to the client’s network with the direct connection between the client’s router and the scrubbing center (for example, using GRE tunnels).

Imperva explicitly presents that its scrubbing centers can block any attack in less than 3 seconds and with typical time to mitigation of 1 second. Thus, presenting this means that Imperva have a high level of trust in their services.

The Imperva’s DDoS solution has been classified as a Leader by the Forrester Wave in their report [139]. Imperva solution received high scores at “*detection and attack mitigation*” and “threat intelligence”, with 4.44 and 5.00, respectively, indicating that the Imperva can those functionalities very efficiently. However, their weak point is the “*volumetric scrubbing*”, this mean that Imperva solution is not very good against high volume DDoS attacks.

4.1.3. Cybersecurity Companies

F5

The F5 offers a cloud solution for DDoS attacks, called Silverline DDoS Protection [155], that utilizes scrubbing centers to sanitize the client’s traffic, that is, the malicious traffic will be blocked while the legitimate traffic will be forward to the client. The F5 scrubbing centers have 12 Tbps of scrubbing capacity [156].

The Silverline DDoS Protection solution can be delivered *Always On*, in which the traffic will be continuously routed and processed through the solution, and *Always Available* where the connections between the scrubbing centers and the client’s routers are pre-configured, being initiated only under attack.

F5 does not have specific on-premises hardware for DDoS protection, however the on-premises appliance F5 Big-IP have provides DDoS mitigation mechanisms and the cloud solution can be used together with it, creating a hybrid solution, where the F5 Big-IP use the Hybrid Signaling to provide real-time communication to Silverline DDoS Protection when volumetric attacks are detected, for more in depth details about the F5 cloud and hybrid solution can be seen in the *F5 Silverline DDoS Protection | F5 Product Datasheet* [157].

The F5 was asked by Forrester Wave to participate in the assessment, but they chose to not participate, therefore the Forrester Wave report [139] do not have any information about the F5 DDoS solution.

F5 is a company that focused on the cybersecurity field and their solutions in this field are very known by the companies, however their core and strength is not DDoS attacks, even if they continue to improve their DDoS solutions, currently, F5 cannot be considered a Leader (in the Forrester Wave classification) since the Leaders by Forrester Wave (i.e., main DDoS companies and competitive DDoS companies) already have many years in the DDoS field, where they continuously improved their solutions and, as we can see in the SPARK matrix of Quadrant Knowledge Solutions [144], in 2019, they classified/ranked F5 as a Challenger company regarding to DDoS solutions.

Nevertheless, F5 DDoS solution is an option for companies to protect against DDoS attacks, companies that already utilize F5 products and solutions can have a discount when acquiring their DDoS solution, therefore there are many other pros and cons that can led companies to choose this solution instead the solutions of main DDoS companies and competitive DDoS companies.

Check Point

The Check Point offers on-premises, cloud and hybrid solutions [158].

The Check Point on-premises hardware is called DDoS Protector, there are different models of the DDoS Protector that have different mitigation capacities ranging from 6 to 400 Gbps. With these different models, companies can purchase the appliance that best fit their needs.

The DDoS Protector mitigates DDoS attacks through behavioral-based real-time signature technology.

The cloud solution of Check Point is backed by a worldwide network of 16 scrubbing centers, with 8 Tbps of mitigation capacity. These scrubbing centers are connected in a full mesh mode, using Anycast-based routing, thus with this, DDoS attacks can be mitigated closest to their point of origin. This solution can be used *On-demand* or be *Always-on.*

The on-premises solution can be integrated with the cloud solution, where the on-premises devices will perform a signaling and redirect the traffic to the cloud scrubbing centers whenever a volumetric attack is detected, hence if a DDoS attack do not appear the traffic will be routed only through the on-premises device.

Check Point was the only company that was not mentioned in the Forrester Wave report [139], but Check Point, similar to F5, it is a company focused on cybersecurity solutions and entered in the DDoS market with their solution. Such as F5, Check Point cannot be considered a Leader in the DDoS market, due to the many years of experience that the other companies (i.e., main DDoS companies and competitive DDoS companies) already have.

4.1.4. Section Summary

In this section we described the DDoS solutions from 7 different vendors, indicating which services they provide between on-premises, cloud, or hybrid solutions.

We can say that all vendors presented here, with their cloud scrubbing centers, can mitigate the DDoS attacks with the highest volume, mentioned in the **Introduction**.

With the analyze of these 7 vendors, we can conclude that their DDoS solutions are very similar, excluding Cloudflare, in terms of high-level operation, where the client's traffic is redirected to scrubbing centers to be clean and then forwarded to the clients. In hybrid solutions, the traffic goes through the on-premises appliance and whenever is detected a volumetric attack it is redirected to the cloud scrubbing centers.

In the Table 4.1, it is represented an overview of the 7 DDoS commercial solutions described above, with the objective of seeing which solutions have on-premises, cloud and/or hybrid solutions, as well as their scrubbing capacity.

Additionally, when a company purchase a DDoS commercial solution, in the communication with the sales area is necessary to understand which services will be provided, in order to understand if the vendor will the prevent, detect, mitigate, and/or tolerance DDoS attacks.

Table 4.1. Overview of all DDoS commercial vendor presented in this work

	DDoS Commercial Solutions Vendors						
	NetScout	Akamai	Radware	Cloudflare	Imperva	F5	Check Point
On-premises	✓	✗	✓	✗	✗	✓	✓
Cloud	✓	✓	✓	✓	✓	✗	✓
Hybrid	✓	✗	✓	✗	✗	✓	✓
Scrubbing Capacity (in Tbps)	11	8	10	155*	9	12	8

*Cloudflare do not have scrubbing centers, thus the number presented is the network capacity

4.2. Open-Source and Freeware DDoS Solutions

Freeware and Open-Source are both software, that means, we have an application where we can use the functionalities of the software. However, it has a crucial difference between them, which is that in the Freeware is we have the software available free of cost, but we do not have permission to modifying, analyze, upgrade, and update the program as we wish. While, in the Open-Source the source code of the software is available to everyone, therefore, users have access to modify, analyze, upgrade, and update the code to best meet the user’s needs. Nevertheless, the solutions presented in this section are both, Open-Source and Freeware.

In this section, we will describe the Open-Source and Freeware solutions that companies can utilize to protected themselves against DDoS attacks. These solutions can be used as a complement to the DDoS commercial solutions, providing a new layer of protection, or be used as an alternative in case that the company do not want purchase DDoS commercial solution or not have the monetary power to purchase it.

Snort

Snort is an open-source network-based intrusion detection system (IDS) [159] which has the capacity of performing real-time traffic monitoring and packet logging on Internet Protocol (IP) networks. With Snort, we can observe and analyze all incoming packets, detecting malicious packets through the implementation of rules and performing alerts to cybersecurity agents. Thus, this means, that Snort is a signature-based tool, where it is implemented the rules that matches the DDoS attacks signatures.

This solution can prevent a DDoS attack, in case of the signatures are already implemented before the attack. On the other hand, if we are targeted by a DDoS attack that we still do not have the signature implemented and its implementation is only performed when we were already affected by the attack, then we consider it as attack mitigation.

The paper of the authors *Hassan et al. (2018)* [160] utilize Snort tool to detect and drop packets that matches the rules implemented in cloud computing environment. While the paper of *Karan et al (2018)* [161] utilize the Snort tool to capture the traffic and further classify the traffic with machine learning method in Software Defined Networking (SDN).

Suricata

Suricata is a signature-based open-source tool that provides the functionalities of IDS and intrusion prevention systems (IPS) [162]. Thus, this tool can detect, alert and block traffic that matches the implemented rules.

Many of the features and functionalities in Suricata are very similar to Snort, however, the main difference of Suricata compared to Snort, it is multi-threaded, therefore whenever the traffic volume increases, it is possible to add more threads to perform packet processing.

The authors *Hyun et al. (2017)* [163] in their paper describes a framework where it is utilized the Suricata to block the traffic according to the packet threshold set by the administrator, with this it is possible to mitigate DDoS attacks in the SDN controller.

FastNetMon

The FastNetMon is a load analyzer, used to detect DDoS attacks and built on top of multiple packet capture engines, such as NetFlow, PCAP, sFlow and others.

Currently, FastNetMon have a community edition, which have their source code available in GitHub [164] for anyone that want to use the solution. On the other hand, it also has a paid version [165], but this version is not in the scope of this work.

The solution in the client's network with the objective to detect hosts within the network that are sending or receiving large volumes of packets/bytes/flows per second and perform configurable action, which can be a notification, switching off the server or blackholing the client.

The authors *Mirkovic, Feng & Li (2022)* in their paper [166] utilized the FastNetMon in their approach to detect DDoS attacks in regional network, since the COVID-19 stay-at-home measures the increase of traffic in local network increased drastically and consequently the number of attacks. The paper concluded with their study that during stay-at-home that the traffic shifted from education and government institutions to local ISPs, large traffic change in online meeting software and VPN usage, increase in network anomalies. With this study, the paper wants to help us to prepare for future emergencies.

Gatekeeper

The Gatekeeper is an open-source DDoS protection system [167]. It has two main components, Gatekeeper servers and Grantor servers. The Gatekeeper servers are deployed at locations called vantage points (VPs), in which they are Internet exchange points (IXPs), border and peering-link routers, and (potentially) cloud providers. While the Grantor servers are located near the protected destination and are responsible for making a policy decision on each flow in the request channel. The policy decisions are sent to the corresponding Gatekeeper servers to enforce them. The more in-depth explanation about how each component work within the solution can be observed in solution's GitHub [171].

It is important to hightlight that Gatekeeper solution can prevent volumetric attack, which target to consume the bandwidth, through the following key points:

- Ensuring that 5% of the path bandwidth is reserved only for requests;
- Assigning priorities to those requests based on the time between requests in the same flow;
- Drop packets of lower priority when the bandwidth of the request channel is overflowing.

HAProxy

The HAProxy (stands for High Availability Proxy) is considered a TCP and HTTP load balancer, as well as a proxy server that allows a web server to forward incoming requests to multiple endpoints. Thus, the objective of the HAProxy is to receive the connection of the clients, in which it will use a reserve proxy to forward the requests to one of the available endpoints through a load-balancing algorithm. The source code and more information about this solution can be found in GitHub [168] or in their website [169].

In the paper of *Ezenwe, Furey & Curran (2020)* [170], the HAProxy as used as a load balancer and first line of defense against DDoS attacks in order that attacks using HTTP will not overload the backend servers (i.e., endpoints). The paper described that HAProxy enables the servers to be used as an active-backup (failover) in case of one or more active servers' crashes.

The paper of *Zebari et al. (2020*) [171], it is compared the performance of the HAProxy load balancer in the mitigation of SYN flood attacks with a Network Load Balancing solution (NLB). The paper concluded that the NLB in the windows platform had better performance than the HAProxy in the Linux platform. However, the paper presented many other papers [170] [172] [173] that resorted to HAProxy to mitigate DDoS attacks, such as HTTP Flood.

Thus, this free solution is a good option for companies that have websites and web applications to defend against DDoS attacks, since many researchers already tested this solution, it provides a high level of confidence that it will work as expected.

4.2.1. Section Summary

In this section, we described 5 Open-source and Freeware solutions that companies can utilize, as a complement of the DDoS commercial solutions or as an alternative to them, to protect their business against DDoS attacks. However, since these solutions are free and not provided by anyone, this means that companies that decide to utilize these solutions will need to train personnel, in order to them to setup the solution and configure it when necessary.

In the Table 4.2, we presented for each solution what types of DDoS protection they provide, between prevention, detection, mitigation, and tolerance, based on our understanding from reading the solutions description and how they work. The Snort and Suricata can prevent and mitigate DDoS attacks because they are signature-based solutions, therefore implementing rules with the signatures of specific DDoS attacks, those attacks will be blocked (i.e., prevented), while in the case of mitigation, the implementation of the rule with the attack signature is only done when an attack is detected (i.e., the attack is already ongoing, but implementing the rule will mitigate the attack).

For the other 3 solutions their description above is enough to understand why they can only detect and mitigate DDoS attacks.

Table 4.2. Overview of what types of DDoS protection the Open-source and Freeware solutions provide

	Open-source and Freeware Solutions				
	Snort	Suricata	FastNetMon	GateKeeper	HAProxy
Prevention	✓	✓	✗	✗	✗
Detection	✓	✓	✓	✓	✓
Mitigation	✓	✓	✓	✓	✓
Tolerance	✗	✗	✗	✗	✗

4.3. Other Solutions described in the Literature

The Other Solutions described in the Literature are different from the Open-source and Freeware solutions, due to the fact that these solutions do not have a software developed that we can utilize the solution, but in their papers are explained how the authors implemented them. Thus, companies can utilize methods and line of thinking of the papers to implement the solutions that best suit their needs.

We read (22) twenty-two papers [174] [175] [176] [177] [178] [179] [180] [181] [182] [183] [184] [185] [186] [187] [188] [189] [190] [191] [192] [193] [194] [195], which presented different solutions to protect against DDoS attacks.

Nevertheless, in this section, we will only describe 4 papers that we considerate, in our interpretation and perspective present interesting strategies, methods and techniques to combat DDoS attacks, since the objective this work is not to perform a review of DDoS solutions in the literature. However, it is important to highlight, that each mentioned paper present a different solution, therefore companies should read these solutions and verify which ones are the most relevant for their needs.

The solutions that we considerate relevant to describe in this section are from the following authors: *Zhou et al. (2022)* [177], *Khooi et al. (2020)* [184], *Lima Filho et al. (2019)* [190] and *Liu et al. (2018)* [193].

It is important to highlight that we do not find any paper that described and defined a solution to tolerate DDoS attacks (i.e., be able to withstand a DDoS attack), we though that this was due to the fact that for a system be tolerant to DDoS attacks, it needs to be tolerant against any other attack, therefore solutions to make a system fault tolerant and which have some essential properties, such as Redundancy, Diversity and Independence can be used to tolerant DDoS attacks [195].

Redundancy means that there are other systems that can take over if the active one fails. Diversity refers that different components can be used on different designs (i.e., from different vendors). And Independence is when there is electrical isolation, physical separation and independence of communication between systems.

A novel feature-based framework enabling multi-type DDoS attacks detection [177]

In this paper, the authors presented five new features, which are entropy of packet size, entropy rate of packet size, entropy rate of IP source flow, entropy rate of flow, and number of ICMP destination unreachable packet, to be used with classification models (for example, Decision Tree, Deep Learning, K Nearest Neighbor, Random Forest and others) in order to detect DDoS attacks. In the paper, were tested the performance of these basic models with the five features.

It was demonstrated that the features had high performance detecting SYN Flood, DNS Amplification, Low Rate, Pulsing and Spoofing attacks and the solution proposed, utilizing the classification model Random Forest, was compared with eight (8) state-of-the-art solutions presented in the literature (Umbrella [193], RADAR [196], GE [197], Entropy [198], SAFETY [199], MLP [200], SKM-HFS [201] and Fuzzy [202]), in which was observed that this solution had high F1-scores in the five DDoS attacks, while the others do not had high F1-scores in all five attacks.

Thus, since this solution had a good performance detecting SYN Flood, DNS Amplification and Low Rate attacks, which are the DDoS attack that the participants of the questionnaire indicated that are the most detected by their tools (SYN Flood and DNS Amplification), as well as the DDoS attack most undetected (Low rate attack), in question 9 and 10 of section 5.5, this means that this solution can be used by companies to detect DDoS, as an alternative of DDoS commercial tools or to complement them to mitigate their weaknesses.

DIDA: Distributed In-Network Defense Architecture Against Amplified Reflection DDoS Attacks [184]

The paper proposes DIDA (Distributed in-network defense architecture), which have the objective of detect and mitigate amplified DDoS attacks (for example, DNS Amplification Attack).

The DIDA solution was implemented in an ISP network, but the idea that the authors described in the paper to detect and mitigate amplified DDoS attack can be used in companies' network. The main idea is the utilization of border and access routers, where access routers store the information about the incoming requests, and it is managed an Access Control List in each border router.

A simple flow using DIDA is: a client sends requests, for example, 10, to a public DNS resolver through an access router, in which this router will store the information that this specific client sent 10 requests to the DNS resolver, expecting to receive 10 responses from the DNS resolver through the border router, if the access router receive the 10 responses from a border router from the DNS resolver, this means, those request are no unsolicited and the client is not under attack.

Thus, if a compromised/abused server is used by an attacker to send an amplified DDoS attack to a victim, it will need to pass through a border router, which will forward the requests to the victim's access router, however in the table of the access router it is not stored information, this means, that the victim is not expecting responses from the abused server and consequently the access router will block that traffic and considering that the victim's is under attack.

DIDA can be a great option for companies to implement, since the architecture and strategy of DIDA can detect and mitigate amplification DDoS attacks, which are the attacks that the participant of the questionnaire indicated be the most targeted their companies.

Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning [190]

The authors of this papers presented the Smart Detection, which is a detection system focused on detection DDoS attacks, such as SYN Flood, UDP Flood, HTTP Flood attacks, as well as slow post/read attacks.

Additionally, it is mentioned that the Smart Detection is compatible with the current Internet Infrastructure and does not require any software and hardware upgrades on Internet Service Providers (ISP). As well as ensures that data remains private at all stages, since the Smart Detection does not need the traffic redirection, connection intermediation, processes only a small part of the traffic and does not perform packet deep inspection.

The Smart Detection core components are a Signature Dataset and a machine learning algorithm (MLA).

The first step to implement the solution is to extract, label and store the normal traffic and DDoS signatures, so it can be created the Signature Dataset using feature selection techniques. And then it is necessary to select, train and load an MLA.

In short, the Smart Detection flow works as follows: receive network traffic samples (collected from network devices), with this samples will be created a new flow based on the 5-tuple (src_IP, dst_IP, src_port, dst_port, and transport_protocol). If this is a new flow (i.e., there is no other flow table stored with the same 5-tuples), then it is created a flow table and registered in shared memory buffer. Otherwise, if there is a flow table, the data of the new flow will be merged with the data in the existing flow table.

Upon merging the data, it is verified if the table length is greater than or equal to a specified reference value, in affirmative case, the table is classified. If it is classified as an attack, then a notification is sent to the administrator, otherwise, if the classification was not attack, the table is inserted back into the shared memory buffer.

The participants of the questionnaire referred that low volume attacks (i.e., slow rate attacks) are the attacks that were not detected by their implemented tools, therefore this solution can be option for companies to detect those attacks. Moreover, the solution can detect other DDoS attacks, such as SYN Flood, which is the attack most detected by the participant tools, this means, that this attack type target the company, thus a solution that can detect this attack is crucial, and UDP Flood which is attack type that most occurred between July 2020 to June 2021, according to *Microsoft Digital Defense Report* [16].

Umbrella: Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services [193]

In this paper, it is presented the Umbrella, which is a new DDoS defense mechanism enabling Internet service providers (ISPs) to offer readily deployable and privacy-preserving DDoS prevention services to their customers. In its core, Umbrella performs a multi-layered defense architecture to defend against a wide spectrum of DDoS attacks against amplification attacks.

The Umbrella is a three-layered defense architecture, in which the layers are: Layer one – Flood Throttling; Layer Two – Congestion Resolving; Layer Three – User-specific Policies.

The user-specific policies layer is where it is enforced the policies defined by the victim and it has priority over the other layers, which operate in parallel.

The Flood Throttling layer is implemented by installing a set of static filters based on already known attacks, with the objective to throttle large DDoS attacks (i.e., volumetric attacks).

The layer two is designed to stop subtle and sophisticated DDoS attacks that rely on seemly legitimated TCP traffic. In volumetric DDoS attacks, the attacker objective is to exhaust the network, therefore they will consistently generate traffic to maintain the victim's network congested. To resolve the congestion, Umbrella utilizes a *rate limiting window*, which will prevent any user from sending a huge number of packets in a short time and consequently preventing volumetric attacks to occur. The *rate limiting window* is calculated based on the users' sending rate and packet losses.

This paper presents a solution to prevent volumetric DDoS attacks, thus this solution could be a good option to the participants that could not detect CLDAP/LDAP amplification attacks with their tools. The Umbrella, resorts to methods and techniques to prevent known volumetric attacks, with the layer one, as well as unknown attacks through the layer two. While the layer three is to provide flexibility, in which companies can setup and enforce traffic control policies that are most suitable to their business.

4.3.1. Section Summary

In this section, we described 4 of the 22 papers mentioned, presenting the ideas of the authors of those papers and their solutions, with the goal of demonstrating that in the literature there are interesting strategies, methods and techniques to combat DDoS attacks, which are not used nor implement in real-world environments.

However, due to lack of tests and maturity of these solutions in real-world environments is not the best idea to use solely these solutions to protect a company but complementing the DDoS commercial solutions with these to mitigate the weaknesses of the commercial solutions is a good starting point.

Reenforcing, that the papers that are not described are still present interesting, important. and different strategies, methods, and techniques to combat DDoS attacks. Thus, we highly recommend their reading with the objective of improving the current DDoS defense mechanisms.

To help cybersecurity agents and companies, we built the Table C.1 in Appendix C, which have the information about DDoS protection type of the solutions, that is, if the solution is focused in prevention, detection, mitigation and/or tolerance of DDoS attacks.

4.4. Chapter Summary

In this chapter, we presented and described three different DDoS solutions categories, DDoS Commercial solutions, Open-source and Freeware DDoS solutions and Other solutions describe d in the Literature, that differ between them due to their implementation and monetary value.

Within the DDoS Commercial solutions category, the solution vendors can be divided in other three categories, which are Main DDoS companies, Competitive DDoS companies and Cybersecurity companies.

In the next chapter, we described in detail the motivation and creation of the questionnaire, which will be sent to the personnel specialized in DDoS attacks within different companies, with the objective to gather the specialized knowledge about the techniques and tools used by them to protect against DDoS attacks.

Chapter 5
Questionnaire

Our motivation, in this section, is to have a practical view and gather information of how cybersecurity agents deal with real-word DDoS attacks and which tools, practices and techniques are used, since the tools, practices and techniques used in real-world differ from those described in the literature.

Therefore, to reach our objective, we decided to build a questionnaire, since with it we can get the information, we need for our work, and the questioned personnel can answer it whenever they can, providing flexibility. Different from interviews, where we need to perform a meeting with the questioned cybersecurity agents and consequently arranging the meetings cannot be easy, because they can be busy and do not know when they will be available to do the interview, this includes that the availabilities between our team (i.e., EY members who are involved in helping this work) and the agents may not match. For these reasons, we opted for to build questionnaire.

The purpose of the questionnaire is to analyze the gathered information and understand that the tools, practices, and techniques used by cybersecurity agents are effective in protecting their organizations from DDoS attacks. Additionally, we will also understand which the tools, practices and techniques are the most relevant and we should perform further research for the preparation of our DDoS framework.

In this chapter, we will make a walkthrough of the built questionnaire, presenting the line of thought behind the construction of the questionnaire, as well as explaining the reasons why and the importance of each question used in the questionnaire to gather information.

5.1. Questionnaire Structure

The questionnaire structure follows the National Institute of Standards and Technology cybersecurity framework (NIST CSF) [203]. Thus, the questions within the questionnaire are grouped in the following five (5) categories/topics *Identify*, *Protect*, *Detect*, *Respond* and *Recover*. By using the NIST cybersecurity framework we are using a common language to understand, manage and express cybersecurity risks.

The framework helped us in the construction of the questions and facilitate participants' understanding the questions in the questionnaire and with their answers.

Although we followed the NIST CSF to structure the questionnaire, the definition of each of the five topics is different, by the fact that the definition in the NIST document focuses on cybersecurity risks [203], while the definition of the five topics in the context of the questionnaire are the following:

- *Identify*: This topic was used in the questionnaire with the objective of getting information about the measures, tools and functionalities utilized by companies to detect and protect/prevent DDoS attacks.

- *Protect*: To identify the functionalities used by companies to protect themselves from DDoS attacks.
- *Detect*: Understand how DDoS attacks are detected, which measures, and tools are utilized, and the DDoS attacks most viewed by cybersecurity agents in the real-world.
- *Respond*: In this topic the objective was to identify the procedures and/or measures utilized by companies to tolerate DDoS attacks and prevent the disruption of their services, that is, what it is performed when companies are under attack.
- *Recover*: In this topic we expect to gather information relative of the consequences and damages caused by the DDoS attacks, that resulting when companies defense measures were not effective in stopping the attacks. Furthermore, the measures put into action to prevent the total disruption of their services.

5.2. Questionnaire Questions

In the questionnaire most of the questions are multiple choice, allowing the participants to choose more than one. Furthermore, in each of the multiple choice we added a text box where participants could write others measures and tools used by them, with the objective of gathering all the essential information.

The other questions that are not multiple choice, are text boxes where participants are open to write the most adequate response.

In the rest of the section, we will present all the questions in the questionnaire, grouped by the categories described in the previous section and the reasons why we put them in the questionnaire.

5.2.1. Identify

The questions that belong to the Identify topic are the following:

1) What measures haven been applied to prevent DDoS attacks?
2) What tools are being used to detect DDoS attacks?
3) What tools are being used to protect/prevent DDoS attacks?
4) Which provided functionality from the identified tools above are the most relevant and should be implemented in all anti DDoS tools?
5) If you have ever changed tools, which were the main reasons (i.e., which benefits the new tools provide that the old ones do not)?
6) What are the most important functionalities which should exist and do not exist in the currently available tools?

As mentioned previously the objective of this topic is to identify the measures and tools utilized to combat DDoS attacks. Thus, in the first question have the goal to verify if every participant's company use DDoS commercial solution and besides that which other measures are used to prevent DDoS attacks.

The second and third questions are used to identify the commercial solutions chosen and utilized by the participants to protect their companies' services.

In the question four, which is an open question, was the objective to understand what the best functionalities in the cybersecurity are in the agents' perspective since they the knowledge of the important functionalities to combat DDoS attacks.

The fifth question is to determine, for the participants which have ever changed from different commercial solution, what are the principal characteristics they took in consideration that led them to change to a new DDoS commercial solution.

The last question in this topic is to identify the most important functionalities that will help or help them currently to defend their companies from DDoS attacks, since with their experience they know the specific functionalities they most need.

5.2.2. Protect

The question that belongs to the Protect topic is the following:

7) What are the functionalities that the tools provide to protect from DDoS attacks?

In this topic it is present only one question, which has the objective of determining the set of functionalities/measures already implemented by the organizations to prevent being hit by DDoS attacks.

5.2.3. Detect

The questions that belong to the Detect topic are the following:

8) How are the DDoS attacks detected by the used tools?
9) What are the most common attack types detected?
10) From your experience, were any of the DDoS attacks you watched not identified by the tools in place? If yes, why it was not detected (i.e., incorrect implementation of rules) and what type of attack was used?
11) What was the destination of the DDoS attacks?

The eighth question of the questionnaire aims to understand from the tools identified in the topic Identify, which are the most used functionalities to detect DDoS attacks. Thus, the functionalities that companies must have implemented to detect DDoS attacks.

The ninth and tenth questions are to verify the most observed DDoS attack with the existing security measures and the attacks that bypassed those measures, with this we can understand the attacks that already have good security measures to protect companies and the attacks that still need to be carefully analyzed.

The eleventh and last question in this topic, aims to realize which are the main targets of DDoS attacks and, therefore where we need to pay more attention when defending the organization resources.

5.2.4. Respond

The questions that belong to the Respond topic are the following:

12) What procedures are used when facing a DDoS attack?
13) What tools are used to mitigate the DDoS attacks?
14) Was it possible to find the source of the DDoS attacks?
15) The team gather any information from OSINT to identify and mitigate DDoS attacks?
    15.1) If yes, where and which information did you gather?

The twelfth question is to understand the principal procedures that companies utilize to mitigate DDoS attacks and verify if different companies in different countries have different procedures.

The thirteenth question is to identify the commercial tool used specifically to mitigate DDoS attacks.

The fourteenth question have the goal to verify if cybersecurity agents can find the source of the attack and if the source machines are part of a known botnet, for example: Mirai botnet or Meris botnet.

Threat Intelligence is crucial in cybersecurity world, in which gather information through different sources, one of them is through OSINT. Thus, we used the fifteenth questions to verify if companies really perform this kind of information gathering and from which open sources the information is gathered.

5.2.5. Recover

The questions that belong to the Recover topic are the following:

16) What was the damage caused by the DDoS attack?
    16.1) How long did it take you to fully recover?
17) What is the procedure executed when a DDoS attack cannot be mitigated within a reasonable time (i.e., current mechanisms cannot defend from the attack effectively)?
18) After the attack mitigation, which were the new measures implemented to tolerate more efficiently future attacks (i.e., lessons learned)?

The sixteenth questions are to determine what consequences did happen to the participants when attacked by DDoS attacks and from those damages how long it took to recover. With this we can verify if the different companies have different or similar consequences and the interval of time needed to return everything to normal.

The seventeenth question is to understand which the best options/procedures are to execute when we are facing a DDoS attack that cannot be mitigated and will disrupt our services.

The last question of the questionnaire has the objective to gather the knowledge that the cybersecurity agents acquire when faced a DDoS attack, leading them to implement new and reinforced security measures.

5.3. Questionnaire Target Audience

The target audience of the questionnaire, ideally, would be a significant high number of cybersecurity agent, that work to protect their companies from DDoS attacks, so we have a great statistical weight to generalize the answers. To do that we would need a way to reach to those cybersecurity agents and encourage/motivate them to answer the questionnaire, which consequently they would need to expose their tools, techniques, and practices, as well their knowledge about DDoS, for the sake of this work.

However, no one will give sensitive information to unknown personnel, therefore I will not receive the expected results, if we send the questionnaire to a significant number of cybersecurity agents. Additionally, the effort that it will take to find (i.e., these agents are a niche in the cybersecurity field and finding all of them would be impossible) and motivate the agents will be too high.

For these reasons, we decided considered only the cybersecurity agents within EY and those from outside but had relations with EY (i.e., EY clients), that EY knows that they work in the DDoS field.

Furthermore, the distribution of the questionnaire by someone within EY will have more impact, than being sent by a student. Furthermore, the information that will be answered by the cybersecurity agents are high-level confidential, since malicious actors that know what kind of tools a specific company use, will be easy for the malicious actors to prepare methods to exploit them, hence seeing that it is EY asking for the responses will increase the level of trust.

EY helped to identify eighteen (18) cybersecurity agents with many years of dealing with DDoS attacks, thus they are experienced agents in the field, and sent the questionnaire to them. Those 18 cybersecurity agents are from different industries (telecommunications, energy, insurance, online services, and financial sector) and are part of Security Operation Center (SOC) teams, who have already witnessed and defended their companies against DDoS attacks. From these 18 cybersecurity agents, which we sent the questionnaire, 4 of the cybersecurity agents are from outside Portugal, being from different countries, which are United States, Poland, Belgium, and India.

We gave 3 to 4 weeks for the cybersecurity agents to answers the questionnaire, from 17/02/2022 to 12/03/2022.

In the period we indicated above, from those 18 questionnaires sent, we only received seven (7) responses, in which from those 7 responses, 3 are from cybersecurity agents located in Portugal, while the rest of the answers (i.e., the 4 answers) are from agents outside Portugal, this means that, every cybersecurity agent that is not located in Portugal answered the questionnaire.

We can speculate that the low rate of response from cybersecurity agents in Portugal was because at the time the questionnaire was sent Portugal has been affected by multiple cyberattacks, that lead companies and their cybersecurity agents reluctant in giving sensitive information, for example the cyberattack to Vodafone [204].

5.4. Questionnaire development

Currently, there are many websites for building questionnaires and are free, such as the Google Forms [205], LimeSurvey [206], SurveyPlanet [207] and EUSurvey [208]. Thus, we could choose where to build our questionnaire from a wide range of option. However, due to the content of the responses, we needed to take into consideration the privacy of the answers when choosing the website for the construction of the questionnaire.

It is important to highlight, that most of those questionnaire websites are free until a certain limit of question or answers, to bypass that limit it is necessary to upgrade the service.

The questionnaire was built in the EUSurvey website, which is supported by the *European Commission's ISA programme, which promotes interoperability solutions for European public administrations* [209].

We choose to build the questionnaire in the EUSurvey website because the questions we made were sensitive to the organizations, therefore the questionnaire and the responses stored in a database supported by European Commission will provide a high confidence that the sensitive information will not be leaked or analyzed by third parties without our knowledge, allowing the cybersecurity agents to answer he questionnaire without fear.

The described questionnaire above is available to be accessed through the following link https://ec.europa.eu/eusurvey/runner/FCULResilienceToDDoSAttacks2022, in which it is necessary to enter the password "*FCULDDoS2022*". It is available in English or Portuguese.

5.5. Results and Analysis

In this section, we will present and analyze the 7 responses received from the questionnaire.

The Table 5.1 present in an aggregated way, all the responses of the participants to the questions and the number of participants that selected/responded that exact answer. The answers in each question are in descending order, this means that the answers that are selected/responded by more participants appear first.

It is possible to have a global view of the result of the questionnaire.

5.5.1. Identify

Regarding the first question, the result we received after going through all responses is that, currently, every participant's company utilize a commercial DDoS protection tool to prevent attacks. Thus, we can consider that commercial DDoS protection tools, such as those provided by Cloudflare and Radware, are essential for companies in a real-world environment. Furthermore, six (6) of the participants also apply Firewalls in their defenses against DDoS attacks.

In the second question, we verified a huge number of different answers, in which participants utilize from in-house scripts to detect DDoS attacks, monitoring NetFlow from routers, web application firewalls and commercial DDoS tools. The commercial tool to detect DDoS attacks most used by our participants is Active Bot Protection [210], which is used by three participants, and two participants utilize the NetScout (former Arbor Networks) [211] services. Nevertheless, the Active Bot Protection is provided by a Russian organization and because of the war we have very little information available on the internet about the tool. In Table 5.1, we only presented the answers that indicated the utilization of DDoS commercial solution, since the remaining answers are only utilized by one participant and will not provide statistical relevance.

Currently, exists a huge number of commercial tools dedicated in protecting organizations from DDoS attacks. From a wide range of solutions, those that gained the trust to protect our participants organizations and are being used by them are: Radware, Akamai and Cloudflare. The three solutions are the ones that got more answer in the third question.

Since the fourth question was open for the participant to write their most relevant functionality, therefore we received different responses being them the possibility of doing BGP FlowSpec, the improvement of rule-based traffic which led to easily drop certain traffic (for example: SYN Flood packets), bot protection and the detection of when servers are stressed and the increase of Tbps. In few words, BGP Flow Spec can be used to drop traffic that match the flow specification.

With the responses we received in the fifth question we verified that the participants companies gave more relevance to commercial tools that provide the following functionalities: protection against high volume attacks, where six participants chose this option, and automatically detect and filter suspicious packets, with 5 participants choosing it. While, having a best monitoring characteristic and providing detection against Zero-days DDoS attacks are not that appellative for companies compared to the other functionalities.

The sixth question just got one response from a participant. We can say that this was due to the fact it is not a multiple-choice question and it ask for a functionality that does not exist, hence the participants did not remember any functionality that currently not exist but would help combat DDoS attack. The participant that answered, indicated that the most important functionalities which should exists in the commercial tools are performance automatically external attack surface scanning and management for the hosted assets.

5.5.2. Protect

Of the available options in the seventh question all of them are chosen by more than half of the participants, this means that current commercial solutions already provide more than one of the following functionalities: packet filtering, UDP rate control, whitelisting and blacklisting.

One participant highlighted that the functionality of Geo-blocking based on location is provided by their commercial solutions, which allows companies to block the access o specific content based on the costumer's location. Thus, this functionally is useful for companies to block the access from the major threat countries.

5.5.3. Detect

With eighth question we realized that all participants utilize a threshold to detect the existence of a DDoS attack. Furthermore, five participants also use detection through suspicious source and four also through suspicious payload. This means that it is analyzed previous DDoS attacks or performed information gathering through OSINT or other tools, so they can determine which are the suspicious source and what kind of payload is malicious. Currently, just one participant employs the detection through attack signature, this means that cybersecurity agents do not trust this functionality, probably because it can be easily bypassed by attackers.

In the answers of the ninth question, we verified that all cybersecurity agents' organizations detected DNS Amplification Attacks and six of them also detected SYN Flood Attacks. The UDP Flood Attack and HTTP Flood Attack least seen by the participants, with 4 and 3 participants detecting them, respectively. Unlike of what was presented in the Microsoft report of 2021 [16], where the attack that most occurred was UDP Flood, in our participant perspective it was not the case.

The tenth question demonstrated that CLDAP Reflection/Amplification Attack, which can be considered a recent attack type exploiting a new protocol vulnerability compared to SYN Flood, UDP Flood and HTTP Flood attacks, and the low volume DDoS attacks that do not trigger the organizations thresholds and are harder to distinguish from legitimate traffic, these were the attacks that at least two participants companies could not detect with their tools. One participant indicated that a SYN Flood attack was not identified by the implemented tools, this means that even a well-known attack can bypass the security measures of commercial tools. It can happen because attacker found new ways to perform the attack that the tools do not expect, incorrect implementation of rules or configurations are not well defined.

Relatively to last question in this topic, the responses received presented that the main target of the attackers are the victims' websites, the option was selected by all participants. The reason why the websites are the main target of the attacker is because the company provides their services to the clients through their websites and therefore it is exposed to everyone on the internet, being an easy target. Furthermore, the second most attacked target is the company servers, among the participants five of them have their servers targeted by a DDoS attack. Since the servers are the ones who allow the correct availability of the services, taking them down will hinder the clients to access the company services. Thus, to cause serious damages to the company, malicious actors focus on targeting websites and servers.

However, participant also indicated other targets of DDoS attacks, two participants pointed that a company device was the target of an attack and other participant mentioned DNS servers. This means that, besides websites and servers, the other targets of the attacker will depend on multiple factors, such as their objective, knowledge (i.e., the information they have about the target) and impact. Additionally, one participant indicated that honeypots are targeted by attacker, this means that some attackers also fall into the traps set by the cybersecurity agents.

5.5.4. Respond

The twelfth question allowed us to understand how the companies behave when are under a DDoS attack. In this phase of the attack, six participants perform the filtering of malicious packets and five contact their ISP, so the ISP can put into action their DDoS mitigation mechanisms. Less than a half of the participants, three of them, execute other procedures, such as the implementation of the backup server and/or informing the clients about the attack. We can understand that some organizations do not consider this phase of the attack to be necessary to inform the clients or utilize their backup server, because the attack impact may not be that significant to waste resource to perform those two procedures.

The thirteenth question show us that, currently, the commercial DDoS solutions for mitigation used by our participants are Radware, Cloudflare, Akamai and Imperva. We verified that the commercial solutions chosen by our participants for preventing and mitigating DDoS attacks are the same, this means that those tools provide functionalities to prevent and if the DDoS attacks cannot be prevented the attack they had as well mitigation mechanisms.

In the fourteenth question, just three participants found out the source of the DDoS attack and from these three all of them were attacked by a Mirai botnet or a Mirai variant, thus Mirai botnet and their variants are really very famous in the real-world environment.

In the fifteenth questions, five participants indicated that they performed information gathering through OSINT, therefore already some organizations understand the importance of gather and analyze the information for later using to better prepare themselves with adequate tools and procedures to prevent and detect new and active threats. From those five participants, three of them utilize FireEye [212], but all the others OSINT website mentioned/chosen are important, which are: NetScout Omnis Threat Horizon [123], Cloudflare Radar [124], Kaspersky Cyberthreat Real-Time Map [213], Shadow Server [214] and Shodan [215]. Due to the Ukraine-Russia war, most of the organizations are discontinuing Kaspersky product [216] [217], very likely that the Kaspersky Cyberthreat Real-Time Map will be affected by it.

5.5.5. Recover

The responses to the question sixteen did not had a great discrepancy, thus the damage caused by the DDoS attacks was similar between all participants. The main consequence that affected six participants was the disruption of the services that prevented their access by clients, damaging the reputation of the organization. Additionally, three participants were affected by a different damage, which was the prevention of the company employees from performing their tasks correctly. We can say that when the security measures and tools do not effectively defend a DDoS attack, it will cause reputational damage to organizations.

On the other hand, the question 16.1) receive a large discrepancy of responses, we understood that the time organizations take to fully recover when attacked by a DDoS can vary from organization to organization and due to other variables, therefore in some cases it can take few hours and in other cases days. Three participants did not answer to this question, probably because they do not remember the duration it took to recover or because the damage caused by DDoS attacks did not need to be recover.

In the seventeenth question, six participants indicated that they implement the Business Continuity Plan (BCP) and five participants, which is more than the half of the participants, communicates to the public what is happening. Thus, we can determine that in this stage most of the participants conclude that it is necessary to inform the clients of the situation. Comparing with the phase where the company is under attack, but the impact is not significant, only three participants decide to inform the clients about the situation. In addition to these procedures, three participants also specified that they put in production the backup servers, two participants monitor for a different attack type because organizations under a DDoS attack are more vulnerable, hence the attacker will utilize this opportunity to bypass the security measure with another type of attack, such as trojans or other type of malware. One participant indicated that when is necessary implements geo blocking rules.

The last question of the questionnaire, which is an open question, allowed the participants to write the new measures that they verified to be extremely important to implement, since with them in execution mitigating and tolerating the attack it would have been easier. The new measures identified by the participants are the following: better link with the ISP, implementation of better tools, change the order of the implemented filtering rules, configuring properly the DDoS protection tools thresholds, existence of redundant servers, commercial DDoS solutions that provides a higher bandwidth and a greater number of scrubbing centers across the globe, utilization of Multicloud DDoS solutions (i.e., use cloud DDoS solution services from more than one cloud vendor), contact the entities that manages the source network of the attack in order to remediate the infected bots used to attack the organization and streamlining of DDoS response plans and BC/DR plans.

We can observe that different organizations had different problems and when the information about the attack was carefully analyzed, organizations lessons learnt from it and improved their weaknesses. Thus, every response we receive in the eighteenth question is very important to take in consideration when defending from DDoS attacks, so we do not make the same mistakes.

Table 5.1. Answers received from participant to each question of the questionnaire

Question Number	Participant Responses	Number of Participants
Identify		
1	DDoS protection tools (ex: Cloudflare, Radware, ...)	7
	Firewalls	6
2	Active Bot Protection	3
	NetScout (former Arbor Networks)	2
	Radware	1
3	Radware	4
	Akamai	3
	Cloudflare	3
	Imperva	2
4	BGP FlowSpec	1
	Improvement of rule-based traffic which led to easily drop certain traffic	1
	Bot Protection	1
	Detection of when servers are stressed and the increase of Tbps	1
5	Protection against high volume attacks	6
	Automatically detect and filter suspicious packets	5
	Best monitoring	2
	Detection against Zero-days DDoS attacks	1
6	Automatic external attack surface scanning & management for hosted assets	1
Protect		
7	Packet Filtering	6
	UDP rate control	6
	Whitelisting	5
	Blacklisting	5

	Geo-blocking based on location	1
Detect		
8	Exceeded a threshold	7
	Suspicious source	5
	Suspicious payload	4
	Attack signature	1
9	DNS Amplification Attack	7
	SYN Flood Attack	6
	UDP Flood Attack	4
	HTTP Flood Attack	3
10	CLDAP Reflection/Amplification Attack	2
	Low volume attacks	2
	SYN Flood Attack	1
11	Website (e-Commerce, digital services, etc.)	7
	Server	5
	Company devices	2
	Honeypot	1
	DNS servers	1
Respond		
12	Filter the malicious packets	6
	Contact ISP	5
	Implementing the backup server	3
	Inform the clients about the attack	3
13	Radware	4
	Cloudflare	4
	Akamai	3
	Imperva	2
14	Mirai Botnet	3
15	Yes	5
	No	2
15.1	FireEye	3
	Cloudflare Radar	1
	Shadow Server	1
	Shodan	1
	Kaspersky	1
	NetScout (former Arbor Networks)	1
Recover		
16	Service cannot be accessed by client (i.e., Reputational damage)	6
	Employees prevented from performing the tasks correctly	3
16.1	1-2 hours	1

	1-3 days	1
	Several days	1
	Minutes to hours	1
17	Implement the Business Continuity Plan (BCP)	6
	Public message to clients	5
	Implement the backup servers	3
	Monitoring for a different attack type (ex: ransomware, trojans, malware and others)	2
	Implement geo blocking rules	1
18	Better link with the ISP	1
	Implementation of better tools	1
	Change the order of the implemented filtering rules	1
	Configuring properly the DDoS protection tools thresholds	1
	Existence of redundant servers	1
	Commercial DDoS solutions that provide a higher bandwidth and a greater number of scrubbing centers	1
	Utilization of Multicloud DDoS solutions	1
	Streamlining of DDoS response plans and BC/DR plan	1
	Contact the entities that manages the source network of the attack	1

5.6. Chapter Summary

In this chapter, we described how we built the questionnaire, since its structure to each question, that was sent to multiple cybersecurity agents that work daily, in their companies, with DDoS attacks.

Furthermore, we presented and analyzed the received responses with the objective to understand the real-world practices of various companies to protect themselves against DDoS attacks. Performing the analyze of the questions will help us in the development of the DDoS framework, since we will notice the trends of the companies and consequently utilize in our framework tool, methods and techniques that matches the companies needs and tendencies.

We also mentioned the difficulties we had of finding the cybersecurity agents that work with DDoS attacks and for them to respond to our questionnaire, due to the confidential information they need to provide and the cyberattacks affecting Portugal.

Therefore, with the development of this chapter, we can address the information to answer the first question in section 1.1, in which we can determine that organizations that are targeted by DDoS attacks can be helped in strengthen their robustness and resilience against future DDoS attacks through the usage of the DDoS solutions. As we can see in the question 9, where companies can detect and consequently mitigate different types of DDoS attacks, however some DDoS attacks can bypass the implement defense mechanisms, existing the necessity of complementary/additional of different DDoS solutions for them to be detected and mitigated in the future.

With this we already have the necessary information to describe our framework, which will be done in the next chapter.

Chapter 6
Proposed DDoS Framework

This section presents our proposed framework which provides the necessary steps to be follow by cybersecurity agents, when choosing DDoS solutions to be implemented in their companies, however different companies have different perspectives, needs and financial power regarding to the DDoS solutions, hence these problems need to be addressed, our framework address them through the implementation of decision paths.

The Figure 6.1 presents the framework process flow, in which it is necessary in a first phase to understand what kind of company we want to protect, second phase, what are the assets needed to be protected against DDoS attacks and then, after this, we can decide which are the best solutions that should be implemented.

In our proposed framework, it is utilized the DDoS solutions, previously presented in the section 4.1, 4.2 and 4.3, but new iterations of the framework can increase the number of the solution used or change solutions that became irrelevant in real-world scenarios.

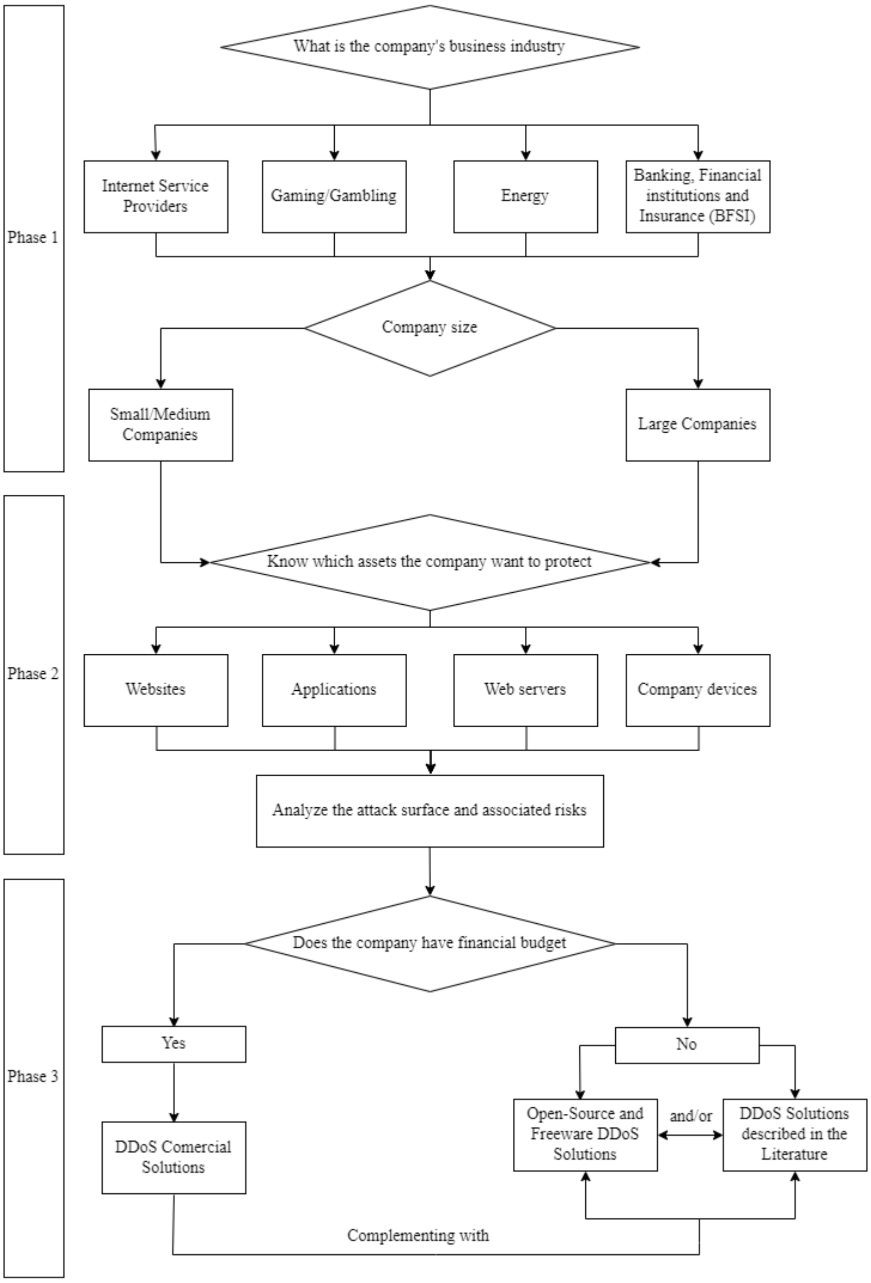

Phase 1
What is the company's business industry
Internet Service Providers
Gaming/Gambling
Energy
Banking, Financial institutions and Insurance (BFSI)
Company size
Small/Medium Companies
Large Companies
Phase 2
Know which assets the company want to protect
Websites
Applications
Web servers
Company devices
Analyze the attack surface and associated risks
Phase 3
Does the company have financial budget
Yes
No
DDoS Comercial Solutions
Open-Source and Freeware DDoS Solutions
and/or
DDoS Solutions described in the Literature
Complementing with

Figure 6.1. Proposed framework flow

6.1. Phase 1 – Company's business

Since there are a great number of different industries and for some of the industries DDoS solutions are more crucial for their core business than for the others, therefore it is important to perform this first analysis.

For the companies in industries, which their main business will be greatly affect if targeted by a DDoS attack, such as telecommunications, energy, gaming/gambling, banking, financial institutions and insurance (also designated as BFSI [218]), and cloud services industries, it makes sense for these industries to spend more resources in the implementation of DDoS solutions than companies from industries like education, agriculture or construction, in which their impact from a DDoS attack will not be so destructive compared with the others. However, is always important to have a DDoS solution because the DDoS attack can disrupt the work of the company's employees, preventing them to continue their work.

The most recent article from Cloudflare, which it is mentioned the trends of the DDoS attacks in the second quarter of 2022 [218], is presented which are the industries most targeted by DDoS attacks. In this article, we can verify that currently aviation & aerospace, telecommunication, BFSI and gaming are the most targeted industries. However, the previous article from Cloudflare of the first quarter of 2022 [219], the aviation & aerospace and BFSI industries were not the most attacked industries, this means, that attacker change their targeted industries, hence companies should perform threat intelligence because the threatened industries are always shifting and having this intelligence about the current threats, companies can better prepare for DDoS attacks. It is important to highlight, that telecommunications and gaming industries, form the first quarter to second quarter of 2022, remained the most targeted industries.

There are companies that still do not perform threat intelligence as we can see in the responses gathered from the responses of the questionnaire, section 5.5, where the companies of two participants do not utilize any threat intelligence tool, it will make these companies more vulnerable and preventing them to perform proactive measurements to prevent and mitigate DDoS attacks.

After determining which industry, the company is in, it is also necessary to determine the companies' size, small/medium or large, because depending on the company's size their needs for DDoS solutions will differ.

We consider a small/medium company/enterprise, those who have less than 250 persons employed and should have an annual turnover (i.e., refers to the total income made by a business over a year) of up to 50 million euros or a balance sheet total of no more than 43 million euros, according to the Eurostat [220]. While, for a large company/enterprise, we consider those who have more than 250 employees [221].

The small/medium companies, which have less employees and revenue compared with large companies, this means, that they will have less financial and human resources and consequently some of the DDoS solutions will not be viable.

On the other hand, large companies have financial and human resources to implement more expensive and complementary solutions and since they have more presence in the market than the small/medium companies, being attacked by a DDoS attack will have a greater impact, such as reputational damage, which is the principal consequence from a DDoS, as we can see from the questionnaire answers in section 5.5, therefore implementing DDoS commercial solution with Open-Source and Freeware solution and/or DDoS solutions described in the literature, will help that consequence to not happen.

In our framework, we highlighted and created a separated category for Internet Service Providers (ISPs), because these are the most targeted companies by the attackers, as we verified in the Cloudflare articles, and they are the first line of defense to the companies and individuals (i.e., home users), therefore it is critical for these companies to implement and maintain their DDoS solutions as up-to-date as possible.

ISPs in addition of using a DDoS commercial solution, they should implement methods, techniques and strategies presented in the literature (i.e., reviewed peer papers and white papers), since most of the papers described novel ideas and solutions.

Trusting entirely in DDoS commercial solutions is an error, since these solutions most of the time can only mitigate "*large-but-obvious-to-catch*" DDoS attacks [17], that is, although the great traffic volume with the objective to flood the victims bandwidth or to consume their network resources (i.e., volume-based attacks and protocol attacks), it is easy to identify the attack traffic and most of them attack types are already known, such as DNS, NTP, SNMP amplification attacks and SYN Flood attack. Fortunately, currently, most of the attacks that occurred between July 2020 to June 2021, from the

Microsoft report [16], belong to the categories of volume-based attacks and protocol attacks. However, the fast pace that attackers change their targets, it is not surprising that the attack types will also change, therefore it is essential to upgrade the existent defense mechanisms and implement novel methods, techniques and strategies and not just be at the mercy of defense mechanisms provided by the DDoS commercial solutions.

6.2. Phase 2 – How and where the company can be attacked

After completing the first phase of the framework, where we understood the context in which the company is inserted, it is necessary to determine which assets the company want to protect because depending on the types of the indicated assets by the company, we can verify which solutions are the most adequate to implement and those who do not make sense, as it will not protect the asset effectively.

A company's information technology assets are websites, applications, web servers, databases, company devices (laptops, computers, smartphones and IoT devices), network infrastructure (includes DNS servers, routers, switches, firewalls) and cloud services.

In the case a company wants to protect a website or an application, it is necessary to gather additional information with the objective to understand where the asset is deployed, since websites and applications can be deployed on-site servers or on a cloud provider, for example, in Amazon Web Services [222] or Google Cloud [223]. Therefore, the attack surface from where a DDoS attack can disrupt the company's website or application will be different if it is deployed on-site servers or in a cloud provider. This means that, we need to verify and anlyze the risks associated to the attack surface.

Websites and applications can be targeted directly with layer 7 DDoS attacks, but also can be indirectly affected with layer 3/4 DDoS attacks targeting on-site servers or the cloud provider where the websites and applications are deployed, hindering them to handle the requests from the clients.

Therefore, when protecting websites and applications we need to consider that these have attack surface larger than web servers or a network infrastructure device, since web servers and network infrastructure devices can only be targeted with layer 3/4 DDoS attacks, while the websites and applications have an additional layer, in this case the application layer (layer 7), leading to the attack surface to be larger.

Noting that, when it is mentioned attack surface, we are only considering DDoS attacks, discarding the other cyberattacks, which are out of the scope of this work, hence in this work the attack surface is from where a DDoS attack can disrupt the company's asset. However, in general, companies when determining the attack surface should consider all attacks and not restricting their scope, as we are doing in this work.

6.3. Phase 3 – List of DDoS solutions

After the phases 1 and 2 we have the global overview of the company, as well as the asset we need to protect. However, before we start analyzing which solutions are the most adequate for a company we need to know if the company have a financial budget for a DDoS commercial solution, since some companies have financial budget to spent on DDoS commercial solutions, while others do not have the financial health and consequently, they cannot purchase a DDoS commercial solution or because they do not want spent that monetary value in DDoS commercial solutions, which is not the most indicated approach due to the recent increase of these attacks in number and in size, as we can see in the reports of ENISA [14], Microsoft [16] and mentioned in the **Introduction**.

For the companies that have a financial budget they should it spend on a DDoS commercial solution, as it will provide the benefits mentioned in the section 4.1.

Regarding to small/medium companies, which we already described above as having a limit financial and human resources, if they can purchase a DDoS commercial solution will help them, in the sense that they will not need to abdicate of human resources (which they could not have) to specialize in the implementation of a DDoS solution and perform the adequate maintenance of the solution, which will take some time, therefore with DDoS commercial solution it will allow a fast deployment of the solution compared with the time that will take to train and specialize personnel, as also, they will not need specialized and technical knowledge to implementation the solution. Additionally, the maintenance, updates, and upgrades to the solution it is performed by the vendor, removing the company from this responsibility.

On the other hand, in the case the small/medium companies cannot afford to purchase a DDoS commercial solution, they should opt for Open-source and Freeware solutions because these solutions require less effort to implement, in which we already have the solutions developed (i.e., someone already wrote most of the code), compared with the solution described in the literature, where there is not an usable solution, only its description. Thus, in our perspective, small/medium companies should not prioritize an Other solution described in the literature before implementing a DDoS commercial solution or an Open-source and Freeware solution.

While, for large companies, which have more financial health than the small/medium companies, and ISPs the purchase of the DDoS commercial solution must be a priority, since these companies when attacked by DDoS attacks will be greatly affected, hence having this layer of protection to filter and mitigate DDoS attacks, even if the attacks cannot be completely mitigated, the impact will be reduced. We consider that, for large companies and ISP, not having a DDoS commercial solution is not an option due to the negative effects from DDoS attacks.

But, as we seen before other industries can be targeted, being always changing, hence it is necessary the companies to perform threat intelligence.

As we seen before, we have companies that belong to a set of most targeted industries, which are always targeted by DDoS attacks, such as telecommunications, energy, and gaming/gambling, and industries that in certain periods are the most targeted, as we saw in the Cloudflare articles the changes in the attacked industries, leading to the necessity of large companies to perform threat intelligence, so they can implement additional solutions.

Therefore, the companies in the most targeted industries and in the new targeted industries, should implement, beyond the commercial solutions, additional protection mechanisms from Open-Source and Freeware solutions and/or other solutions described in the literature to cover the weak points of the DDoS commercial solutions, creating a new protection layer. The implementation of a new protection layer is more viable in large companies than small/medium companies because they have more human resources as well as financial health to provide the right training and specializing personnel for not only implementing the solution in the context of the company, but also realize the adequate mitigation actions when facing a DDoS attack.

In the case of ISPs, as these are the first line of defense for many companies and individuals (i.e., home users) against DDoS attacks, since they are the ones that forward the traffic to its destination and provide the access to the Internet, they should implement a 3-layer DDoS protection, as we can see in Figure 6.2, the reason why and the benefits of the proposed 3-layer DDoS protection, using the three categories of DDoS solutions, will be described below.

The DDoS commercial solutions are known to be good at mitigating "*large-but-obvious-to-catch*" DDoS attacks [17], however more sophisticated attacks can bypass these commercial solutions, hence we opted to put this DDoS commercial solution as the first layer, which will mitigate most of the current DDoS attacks, since most of them are UDP Flood and TCP attacks, based on the most recorded attacks by Microsoft [16], and the technical knowledge to implement this solutions is not crucial compared with the other solution categories.

With the first layer most of the attacks will be prevented and mitigated, but some of the attacks will evade its protection mechanisms and thus we need the second layer, where we utilize the Open-source and Freeware DDoS solutions. However, these solutions will need some technical knowledge to perform the implementation to protect the company assets and realizing the necessary code modifications (in the Open-source solutions) for it to prevent and mitigate the sophisticated DDoS attacks, that evaded the DDoS commercial solution protection mechanism, properly.

In the third and last protection layer, it is utilized the other solutions described in the literature, even if most of the attacks can be prevented and mitigated with the DDoS commercial solution and Open-source and Freeware solutions, there can always be DDoS attacks that cannot be prevented and/or mitigated with those solutions, because it uses a novel method that is not cover by the implement solutions, the solutions for some unknown reason cannot mitigate the attack or the solution itself cannot mitigate the attacks (i.e., due to how the solution is implemented), therefore the other solutions presented in the literature, which demonstrate different points of view, where researchers write and demonstrate in detail their ideas of new methods, strategies and/or techniques to mitigate a set of DDoS attacks, this can help the companies cybersecurity agents to development novel mechanisms to protect against DDoS attacks.

The solutions presented in the literature help cybersecurity agents in companies, in the sense that the cybersecurity agents in a company do not have time to perform in depth research and analyzes, due to their day-to-day work and workload, whereas cybersecurity and academic researchers are full-time focused in finding novel methods, strategies and/or techniques to fight DDoS attacks, even if most of them we do not have information about their viability in real-world environments, the explanation behind the development of the solution can help cybersecurity agents to have new perspective and new implementation ideas.

The other solutions presented in the literature demonstrate the research developed by the cybersecurity and academic researchers, but most of the time the functional solution it is not provided, hence the cybersecurity agents need to implement the solution from scratch, having only the information that was written in the document, leading to the need for a higher level of technical skills. Thus, this can be a problem for some companies since they do not have the personnel with the necessary skills and knowledge, consequently it is necessary to perform the training.

For each DDoS solution, presented in sections 4.1, 4.2 and 4.3, we identified what types of DDoS attacks they can detect, prevent and/or mitigate through the information available in the solutions documents, as seen in the Figure 6.3. Therefore, as we do not test the solutions to confirm if they really can prevent, detect and/or mitigate the indicated attacks, we cannot ensure if this really happens. However, since this correlation between the DDoS solution and attacks were gathered from the documents and reports available in the official website of each solution, providing some confidence, but it is up to each company if they will trust this information or not.

In following iterations, the work presented in Figure 6.3 must be proven, that is, test each solution to determine if they can really prevent, detect and/or mitigate the DDoS attacks, in which they indicated to be possible.

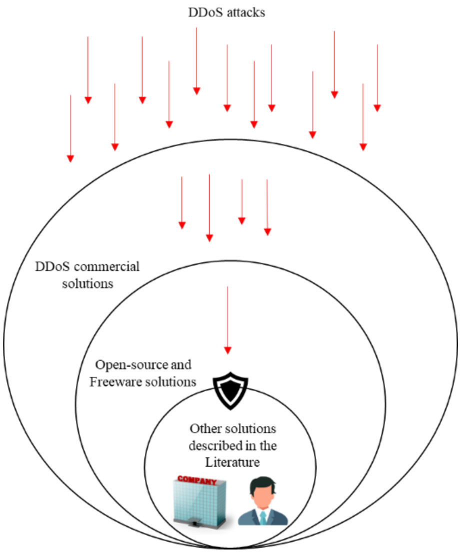

DDoS attacks
DDoS commercial solutions
Open-source and Freeware solutions
Other solutions described in the Literature
COMPANY

Figure 6.2. The 3-layer DDoS protection

Companies can utilize the Figure 6.3 as a starting point and, over time, validate and add different DDoS attacks. With this, in the course of the time, we will have a figure that can be used by every company to decide which solution to utilize, with real information about what DDoS attacks which solution can prevent, detect and/or mitigate.

In Figure 6.3, each circle in front of the DDoS solution means that the solution can prevent, detect and/or mitigate that specific DDoS attack, while the line means that the solution can prevent, detect and/or mitigate all DDoS in that specific category (volume-based attacks, protocol attacks and application attacks), but we will explain in more detail why we put lines in Snort, Suricata, GateKeeper and in the both papers ([184] and [193]).

For the development of the Figure 6.3, we search the information of which DDoS attacks the DDoS Commercial and Open-source and Freeware DDoS solutions can prevent, detect and/or mitigate through their official websites. Nevertheless, in some of the websites the information is presented explicitly, while for others, the websites do not provide that information, hence we realized the following process: we gathered the latest available report and verified which attacks are mentioned in those reports, since the reports present the DDoS attacks most viewed in a specific period, implicitly this means that those attacks were prevented, detected, or mitigated by their solution.

The FastNetMon [224] [225], HAProxy [226] [227], F5 [228], Cloudflare [229], Akamai [230] [231] and Check Point [232] the information of which DDoS attacks they can prevent, detect and/or mitigate is presented explicitly in their websites or solution documents. While NetScout [233] and Radware [234] the information was presented implicitly in reports.

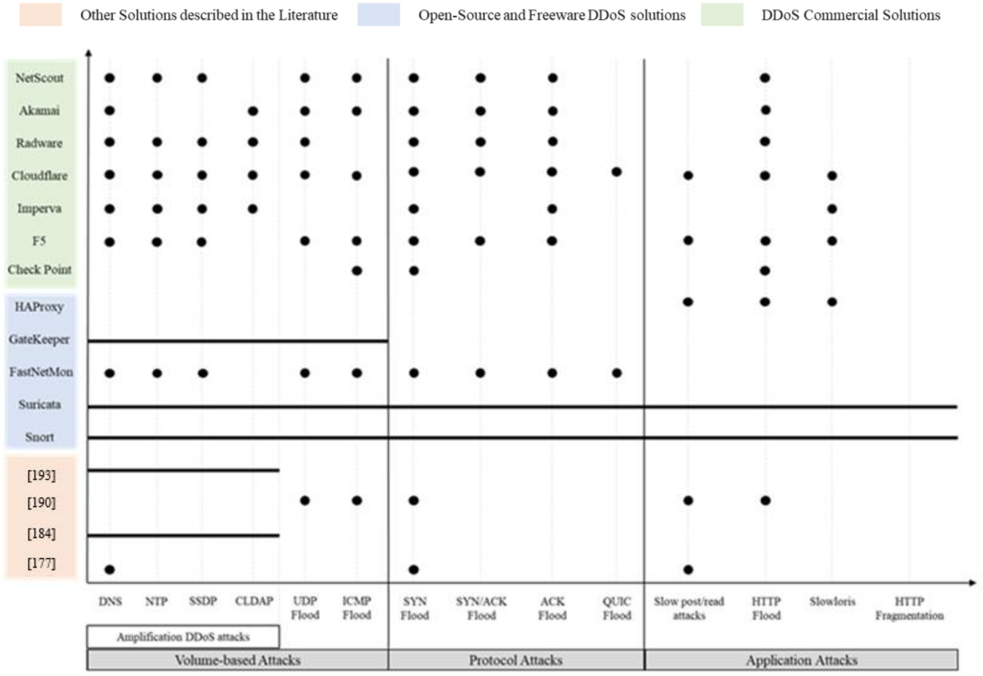
Regarding the other solutions described in the literature, the information about the DDoS attacks that they can prevent, detect and/or mitigate was taken from their papers.

The described solutions from the papers of *Khooi et al. (2020)* [184] and *Liu et al. (2018)* [193], in our perspectives, allows to mitigate every amplification DDoS attack, therefore we put a line in each solution, as seen in Figure 6.3, covering the set of all amplification DDoS attacks. However, as the solution was not tested against real-world DDoS attacks, it cannot be guaranteed. Thus, further analysis of these solutions is required. The papers description can be found in the section 4.3.

We indicated in the Figure 6.3, that GateKeeper solution can detect and mitigate all Volume-based DDoS attack, because it ensures that 5% of the path bandwidth is reserved only for requests, this means that, when an attacker performs a volumetric attack, only 5% of these packets will be received by the victim, not causing great damage to them, based on the information presented in [167], and supposing that the solution is implemented properly (i.e., the aggregated bandwidth of all Gatekeeper servers should be higher than the current biggest DDoS attack)

Snort and Suricata are signature-based solutions, therefore with the correct signature all DDoS attacks can be prevented, detected, and mitigated, for this reason, in Figure 6.3, Snort and Suricata have lines that cover all three DDoS attacks categories. We know it is not possible to have the information to create the signatures for all DDoS attacks, however, with threat intelligence will help in the creation and implementation of that are currently being used by the attackers. The key point for Snort and Suricata to work in a real-world environment is to have a good threat intelligence.

It is important to note that with the Figure 6.3, companies can verify which solutions can protect against a specific DDoS attack. Thus, a company that is being targeted by DNS amplification attacks can utilize any of the DDoS commercial solution, excluding Check Point, any Open-source and Freeware DDoS solution, excluding HAProxy and can be used the solution described in papers [177], [184] and [193]. While a company that want to protect against QUIC Flood attacks can only utilize Cloudflare, FastNetMon, Suricata and Snort.



	DNS	NTP	SSDP	CLDAP	UDP Flood	ICMP Flood	SYN Flood	SYN/ACK Flood	ACK Flood	QUIC Flood	Slow post/read attacks	HTTP Flood	Slowloris	HTTP Fragmentation
NetScout	●	●	●		●	●	●	●	●			●		
Akamai	●			●	●	●	●	●	●			●		
Radware	●	●	●	●	●		●	●	●			●		
Cloudflare	●	●	●	●	●	●	●	●	●	●	●	●	●	
Imperva	●	●	●	●			●		●				●	
F5	●	●	●		●	●	●	●	●		●	●	●	
Check Point						●	●					●		
HAProxy											●	●	●	
GateKeeper	━	━	━	━	━	━								
FastNetMon	●	●	●		●	●	●	●	●	●				
Suricata	━	━	━	━	━	━	━	━	━	━	━	━	━	━
Snort	━	━	━	━	━	━	━	━	━	━	━	━	━	━
[193]	━	━	━	━										
[190]					●	●	●				●	●		
[184]	━	━	━	━										
[177]	●						●				●			

Figure 6.3. A set of DDoS attacks that can be prevented, detected and/or mitigated by each DDoS solution

6.4. Proposed Framework Usage Exemplification

Our framework usage exemplification will describe the examples from the perspective of a person who is not part of the company, therefore we do not have any information about the company. But this does not mean that the framework cannot be used by people inside the company.

We start by gathering information about the company that want to be protected, information relatively to Phase 1 of the framework. This information can be gathered through the public information available online (i.e., on the Internet) or questioning the personnel within the company.

If with the information gathered in Phase 1, we verify that the company is inserted in the category of small/medium companies and their core business is the gaming industry.

After completing the first phase, we move forward to the Phase 2, where it is necessary to determine the assets needed to be protected and its attack surface. This information needs to be provided by company and cannot be find on the Internet, as the information in Phase 1, because they are the ones who know what they want to protect.

If the information we received in Phase 2, indicate that the company wants to protect a website deployed in a cloud provider, then we know that the attack surface of the asset are attacks that directly target the website and attacks targeting the cloud provider. However, cloud providers have large amounts of bandwidth, being hard to disrupt their services, but it is not impossible. In this example, we will only focus on the attacks that target the website directly.

With the information gathered from Phase 1 and Phase 2 of the framework, we can now move to the last phase, Phase 3, where we verify if the company have a financial budget for a DDoS commercial solution.

Due to the fact that the company is in the gaming industry, which is one of the most targeted industries by attackers, we need to take this in consideration when deciding which DDoS solution to implement in the company. Therefore, it is necessary solution that can be implemented fast, so we need to implement a DDoS commercial solution, since these are the fastest DDoS solutions to implement.

However, small/medium companies due to their limited financial budget to spend in DDoS commercial solutions, considering that they have a budget, we should opt for the solutions which provides competitive prices and in the case of the DDoS commercial solutions we presented in this work, the best option is the Cloudflare solution, which offers a competitive pricing [78].

On the other hand, in the case they do not have a financial budget, we should demonstrate to the company owners the importance of a DDoS solution that can be fast implemented and deployed, since the company’s business is in the gaming industry (i.e., present and indicate that the gaming industry are one of the most attacked industries, hence there is a high probably of being attacked).

Even so, after presenting the problems of not implementing a DDoS commercial solution, they still do not provide a financial budget, then we do not have another option than to use Open-source and Freeware DDoS solutions. Not only because it is easier to implement, since we already have most of the code written, but also faster to learn, comparatively to the other solutions described in the literature.

Nevertheless, if the small/medium company business is not in one of the most target industries, then the implementation and deployment of a DDoS solution does not need to be fast (i.e., the probably of being attacked is lower), hence an Open-source and Freeware DDoS Solutions and/or other solutions described in the literature can be used.

For Layer 7 DDoS attacks, that are the attacks carried out on websites, the Open-source and Freeware DDoS solutions that can be chosen are the HAProxy, Suricata and Snort. Therefore, an option is to utilize HAProxy solution for detection and mitigation, whereas Suricata or Snort be used only for prevention, as we can see in the Table 4.2.

Not forgetting that Suricata and Snort are signature-based solutions, consequently it is necessary to implement the right rules to block the malicious traffic.

As we can see with the description of this example, where we use our proposed framework, is that when a company want to protect themselves (i.e., their business), there are different points that we need to have in consideration before deciding whether to implement a DDoS Commercial solution or just Open-source and Freeware DDoS solution are enough.

6.5. Chapter Summary

We presented a framework which can be divided into three phases, in which the first we need to understand the industry and size of the company, second, we need to know what assets we will protect, and the last phase decide which DDoS solution will the company implement, based on the information gathered in the first and second phases, as well as their financial and resource power.

With the development of this chapter, we can answer to the second question in in section 1.1, in which we determined that there are various techniques, methodologies and/or frameworks (i.e., DDoS commercial solutions, Open-source and Freeware DDoS solutions and Other solutions described in the literature) that can help organizations, regarding to prevention, mitigation, detection and tolerance against DDoS attacks.

Our developed framework has the objective to guide organizations in deciding which DDoS solutions to implement, help them in the prevention, detection, mitigation, and tolerance of DDoS attacks.

In the following chapter, we will present the conclusion that we obtained with the development of this work and the next steps (i.e., future work).

Chapter 7
Conclusion

DDoS attacks has been around for many years and are still one of the most utilized cyberattacks by malicious actors, due to its disruptive power which causes serious damages to their victims. There are multiple different types of DDoS attacks, which in the end have the same objective, to prevent the provision of the victims' services to their customers, through the exhaustion, consumption and/or flood the available resources of the victims.

Over the years, these attacks are always evolving to face the changes of the technological world and new types of DDoS attacks (i.e., Zero-days DDoS attacks) are found by cybersecurity companies. Therefore, this means that, the DDoS attacks does not have a standard framework, in which companies can resort to, so they can protect themselves against DDoS attacks.

An example is the COVID-19 pandemic that changed the lives of many people, where one of the changes was where and how these persons will perform their work.

The significant increase in the number of people working remotely led that the attackers also increase the number of cyberattacks, including DDoS attacks. The COVID-19 demonstrated that the companies need to continuously develop their security mechanisms.

Therefore, the objective of this work is the development of a framework that can be used by the companies, due to the necessity of the companies to protect themselves against DDoS attacks and the lack of a framework to help the companies.

Our work started with the definition of the state of the art of DDoS attacks through the description of the concepts related to DDoS attacks, presenting 27 different types of DDoS attacks and how these attacks are performed by malicious actors. With this, we can understand the current state of the DDoS attacks and helping to perform the bridge for our contributions.

As there is not standard categorization of the different types of DDoS attacks, we presented two different categorizations mentioned in the literature and we choose the one we considered to have the easier interpretation of the different categories. With the chosen categorization we classified the 27 types of DDoS attacks and explained the reasons why we put that specific DDoS attack in respective category.

After explaining what DDoS attacks are and classifying the different types of these attacks, we presented the solutions/mechanisms that the companies can utilize to protect against DDoS attacks. Dividing them in three categories: DDoS commercial solutions, Open-source and Freeware DDoS solutions and Other solutions described in the literature.

For us to understand how different cybersecurity agents fight against real-world DDoS attacks, since we do not have practical knowledge and how DDoS attacks are protected in real-world scenarios, we decided to utilize a questionnaire to gather the information.

From the 18 questionnaires sent, we received 7 answers. With the results we observed that all participants who responded to the questionnaire utilize DDoS commercial solutions, hence we can verify that currently companies rely on these solutions to defend against DDoS attacks.

Furthermore, with the result we can also identify that the DDoS attacks that were not detected by the DDoS solutions are CLDAP Reflection/Amplification attacks and slow volume DDoS attacks. Another result, that we verified is that most of the companies that participated in the questionnaire only perform a communication to the public about the attack, when the attack have already did catastrophic damages and cannot be mitigated in a reasonable time and not right after being hit by the attack.

With the results that we gathered from the responses of the questionnaire, we determined that the companies can build their robustness and resilience against DDoS attacks through the usage of DDoS solutions.

The different topics that we mentioned and described in this work, such as DDoS attack types, the different DDoS solutions categories, and the results of the questionnaire, had the objective to provide the knowledge of what are DDoS attacks, what is used to defend against these attacks and what it is done in a real-world environment, understanding and knowing this we could develop our base framework to help companies when deciding which DDoS solutions they will implement.

Our proposed framework it is divided into three phases, in which the first phase is where we study and understand the background of the company, the second phase we verify the assets the company want to protect against DDoS attacks. However, depending on which asset the company want to protect, it will have different attack surface and different associated risks, hence in this phase we need to perform this analyze carefully.

Finally, the third phase is where we decide the DDoS solutions which best suits the company needs, this is possible since in the previous two phases we analyzed the necessary information about the company. Nonetheless, when deciding the DDoS solution, we need to consider the company available resources, which are, the financial budget and the human resources to learn how to implement noncommercial DDoS solutions.

Companies can benefit from the proposed framework from which they can decide the most suitable solution for their needs, based on the industries they are inserted and the asset they want to protect. For example, telecommunication and gaming/gambling industries are one of the industries most attacked by DDoS attacks, hence these companies should follow our framework and the information we presented, so they can develop their robustness and resilience against DDoS attacks.

Furthermore, the framework analyzes the companies' resources and based on their resources (i.e., the company size) we guide the company in implementing the solution which is the most adequate solution for their needs and capabilities.

Therefore, our proposed framework guides the companies in choosing and implementing the DDoS solutions that are the most ideal for their context and resources.

We also analyzed, develop, and presented in a figure, for each DDoS solution, which DDoS attack types they can prevent, detect and/or mitigate. Concluding, that this figure can help companies by guiding them, through each DDoS solution, indicating what types of DDoS attacks they can protect and making companies perform an initial triage of the DDoS solutions that are the most adequate for their business, more easily.

It is worth to mention, that our proposed framework is still at an early stage and needs improvements, which will be mentioned in the next section. However, we could not find a framework, in peer review papers neither in white papers available on the Internet, that provides and specifies the crucial phases that companies need to perform when choosing which DDoS solutions, they should implement. Therefore, our framework contributed by being a starting point for the creation of an universal framework to combat DDoS attacks and help companies improving their robustness and resilience against DDoS attacks.

7.1. Future Work

The framework that we proposed in this thesis, proposes a flow that companies can perform when deciding which DDoS solutions, they should implement. However, for us to have the confidence in which solution to choose, it is necessary to test the solutions, and, in our case, we did not test any DDoS solution, since we do not have an implemented infrastructure that can support the DDoS solution.

We developed the Figure 6.3, through the analysis of the information gathered on the Internet about the different DDoS solutions, which indicates the DDoS attack types that can be prevented, detected and/or mitigated by each DDoS solution. Therefore, for our proposed framework to be more reliable for the companies, it is necessary to utilize and test the solutions in a real-world environment, with the objective of determining/confirming if the solutions really can prevent, detect and/or mitigate the attacks specified in the information gathered on the Internet and verify if it can prevent, detect and/or mitigate others DDoS attack types, in addition to the types already presented.

By testing of DDoS solutions in a real-world environment and updating the information presented in Figure 6.3, it will provide a higher level of reliability and viability to the companies, since it was performed the validation of which attacks the DDoS solutions can prevent, detect and/or mitigate, facilitating the companies to choose the DDoS solution that will attend their needs. For example, if a company is attacked more frequently by SYN Flood attacks and by CLDAP Amplification attacks, then with the validated Figure 6.3, companies can, with confidence, implement any DDoS solution that can prevent, detect, and mitigate those attacks.

In other iterations of our work should be added more DDoS attack types that the DDoS solutions can prevent, detect and/or mitigate, since in Figure 6.3 does not present every DDoS attack. Therefore, when testing each DDoS solution, the information in Figure 6.3 should be updated in parallel, indicating which DDoS attacks can be protected by the solution and which ones can bypass their security mechanisms.

Additionally, building a table with the information of the prices of the different DDoS Commercial solutions, will be very useful for companies, since they will not need to send to every DDoS solution vendor the information about their assets (i.e., the information that Imperva asked, as we can see in Figure B.10), so we can get the information about the respective price of the solution, as well as, we will not need to wait for the responses from the DDoS vendor sales department, which can take some time (i.e., 1 or 2 weeks). Therefore, a table with the prices for the different characteristics (i.e., 1 asset with 100 mb/s of clean traffic, 2 assets with 200 mb/s of clean traffic, …), will help companies to better chose their DDoS solutions, taking into account their needs.

According with the article from the CNN [235], a set of companies, which involves Amazon, Cloudflare and IBM, are developing single standard to detect cyberattacks, called Open Cybersecurity Schema Framework (OCSF), this will normalize data and allowing that this data to be read and processed by every tool (i.e., from different vendors/companies). Therefore, in the future we need to be attentive of what will be developed, since this can renew the world of cybersecurity solutions, including DDoS solutions, where solution from different companies can communicate between each other, leading to faster detection and allowing implementation of the adequate defense mechanisms. However, this is speculative since we do not have more information.

Bibliography

[1] Radware, "DDoS Attacks History," 2017. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/. [Accessed 19 06 2022].

[2] S. Weisman, "What are Denial of Service (DoS) attacks? DoS attacks explained," 2020. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html. [Accessed 19 06 2022].

[3] F. Lau, S. H. Rubin, M. H. Smith and L. Trajkovic, "Distributed denial of service attacks," in *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0,* 2000.

[4] S. T. Zargar, J. Joshi and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE communications surveys & tutorials,* vol. 15, p. 2046–2069, 2013.

[5] D. Asturias, "The Most Notorious DDoS Attacks in History," 2021. [Online]. Available: https://www.cloudbric.com/blog/2021/04/most-notorious-ddos-attacks-in-history-2021-update/. [Accessed 19 06 2022].

[6] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer,* vol. 50, p. 80–84, 2017.

[7] Cloudflare, "Famous DDoS attacks | The largest DDoS attacks of all time," [Online]. Available: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/. [Accessed 19 06 2022].

[8] O. Yoachimik, "Cloudflare thwarts 17.2M rps DDoS attack — the largest ever reported," 2021. [Online]. Available: https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/. [Accessed 19 06 2022].

[9] C. D. Team, "Meris Botnet," 2021. [Online]. Available: https://radar.cloudflare.com/notebooks/meris-botnet. [Accessed 19 06 2022].

[10] CVE, "CVE-2018-14847," 2018. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14847. [Accessed 19 06 2022].

[11] O. Yoachimik, "Cloudflare blocks an almost 2 Tbps multi-vector DDoS attack," 2021. [Online]. Available: https://blog.cloudflare.com/cloudflare-blocks-an-almost-2-tbps-multi-vector-ddos-attack/. [Accessed 19 06 2022].

[12] D. Goodin, "Microsoft fends off record-breaking 3.47Tbps DDoS attack," [Online]. Available: https://arstechnica.com/information-technology/2022/01/microsoft-fends-off-record-breaking-3-47-tbps-ddos-attack/. [Accessed 19 06 2022].

[13] A. Toh, "Azure DDoS Protection—2021 Q3 and Q4 DDoS attack trends," [Online]. Available: https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/. [Accessed 19 06 2022].

[14] ENISA, "ENISA Threat Landscape 2021," 2021. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. [Accessed 19 06 2022].

[15] NexusGuard, "DDoS Threat Report FHY 2021," 2021. [Online]. Available: https://blog.nexusguard.com/threat-report/ddos-threat-report-fhy-2021. [Accessed 19 06 2022].

[16] Microsoft, "Microsoft Digital Defense Report," 2021. [Online]. Available: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report. [Accessed 19 06 2022].

[17] Y. a. G. Y. a. T. R. a. H. Q. a. L. Z. Cao, "Understanding internet DDoS mitigation from academic and industrial perspectives," *IEEE Access,* vol. 6, pp. 66641--66648, 2018.

[18] A. T. Tunggal, "UpGuard," 15 06 2022. [Online]. Available: https://www.upguard.com/blog/vulnerability. [Accessed 30 07 2022].

[19] OWASP, "Who is the OWASP® Foundation?," [Online]. Available: https://owasp.org/. [Accessed 19 06 2022].

[20] O. I. S. Team, "Internet of Things (IoT) Top 10," 2018. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf. [Accessed 19 06 2022].

[21] OWASP, "OWASP," [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed 31 07 2022].

[22] G. Nick, "How Many IoT Devices Are There in 2022? [All You Need To Know]," 2022. [Online]. Available: https://techjury.net/blog/how-many-iot-devices-are-there/. [Accessed 19 06 2022].

[23] NIST, "COMPUTER SECURITY RESOURCE CENTER - NIST," [Online]. Available: https://csrc.nist.gov/glossary/term/attack_surface. [Accessed 30 07 2022].

[24] Fortinet, "Fortinet," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/attack-surface. [Accessed 02 08 2022].

[25] NIST, "CSRC NIST," [Online]. Available: https://csrc.nist.gov/glossary/term/cyberspace. [Accessed 30 07 2022].

[26] NIST, "CSRC NIST," [Online]. Available: https://csrc.nist.gov/glossary/term/Cyber_Attack. [Accessed 30 07 2022].

[27] Cisco, "Cisco," [Online]. Available: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html. [Accessed 30 07 2022].

[28] Imperva, "Imperva," [Online]. Available: https://www.imperva.com/learn/application-security/phishing-attack-scam/. [Accessed 30 07 2022].

[29] Fortinet, "Fortinet," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/ddos-attack. [Accessed 03 08 2022].

[30] Cloudflare, "Smurf DDoS attack," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/. [Accessed 19 06 2022].

[31] EUROCON, "DoS attacks and countermeasures," 2021. [Online]. Available: https://sites.google.com/a/pccare.vn/it/security-pages/dos-attacks-and-countermeasures. [Accessed 03 12 2021].

[32] Radware, "Fraggle Attack," 2021. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/fraggle-attack/. [Accessed 19 06 2022].

[33] Radware, "Radware - DDoSpedia," [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/teardrop-attack/. [Accessed 31 07 2022].

[34] T. Mahjabin, Y. Xiao, G. Sun and W. Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques," *International Journal of Distributed Sensor Networks,* vol. 13, p. 1550147717741463, 2017.

[35] Cloudflare, "R U Dead Yet? (R.U.D.Y.) attack," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/r-u-dead-yet-rudy/. [Accessed 19 06 2022].

[36] Cloudflare, "Slowloris DDoS attack," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/. [Accessed 19 06 2022].

[37] Cloudflare, "What is the OSI Model?," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/. [Accessed 19 06 2022].

[38] Cloudflare, "Ping (ICMP) flood DDoS attack," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/. [Accessed 19 06 2022].

[39] Radware, "UDP Flood Attack," 2021. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/udp-flood/. [Accessed 19 06 2022].

[40] C. &. I. S. Agency, "DNS Amplification Attacks," 2013. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/TA13-088A. [Accessed 19 06 2022].

[41] GeeksforGeeks, "GeeksforGeeks," 24 01 2022. [Online]. Available: https://www.geeksforgeeks.org/network-time-protocol-ntp/. [Accessed 05 08 2022].

[42] L. Constantin, "Attackers use NTP reflection in huge DDoS attack," 2014. [Online]. Available: https://www.computerworld.com/article/2487573/attackers-use-ntp-reflection-in-huge-ddos-attack.html. [Accessed 19 06 2022].

[43] D. Balaban, "Are you Ready for These 26 Different Types of DDoS Attacks?," 2020. [Online]. Available: https://www.securitymagazine.com/articles/92327-are-you-ready-for-these-26-different-types-of-ddos-attacks. [Accessed 19 06 2022].

[44] T. W. Group and others, "SNMP Reflected Amplification DDoS Attack Mitigation," *SNMP Reflected Amplification DDoS Attack Mitigation (August 1, 2012),* 2012.

[45] C. D. Team, "DDoS Attack Trends for Q4 2021," 2022. [Online]. Available: https://radar.cloudflare.com/notebooks/ddos-2021-q4. [Accessed 19 06 2022].

[46] DDOS-GUARD, "MS SQL Reflection Attack," [Online]. Available: https://ddos-guard.net/en/terminology/attack_type/ms-sql-reflection-attack. [Accessed 19 06 2022].

[47] Akamai, "Attackers Using New MS SQL Reflection Techniques," 2018. [Online]. Available: https://myakamai.force.com/customers/s/article/Attackers-Using-New-MS-SQL-Reflection-Techniques?language=en_US. [Accessed 19 06 2022].

[48] J. J. C. Gondim, R. de Oliveira Albuquerque and A. L. S. Orozco, "Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols," *Future Generation Computer Systems,* vol. 108, p. 68–81, 2020.

[49] Wireshark, "Simple Service Discovery Protocol (SSDP)," 2021. [Online]. Available: https://wiki.wireshark.org/SSDP. [Accessed 19 06 2022].

[50] V. Koutsonikola and A. Vakali, "LDAP: framework, practices, and trends," *IEEE Internet Computing,* vol. 8, p. 66–72, 2004.

[51] J. A. &. W. Mejia, "CLDAP Reflection DDoS," 2017. [Online]. Available: https://www.akamai.com/our-thinking/threat-advisories/cldap-reflection-ddos. [Accessed 19 06 2022].

[52] DDOS-GUARD, "Attack types," 2021. [Online]. Available: https://ddos-guard.net/en/terminology/attack_type?page=2&per-page=10. [Accessed 19 06 2022].

[53] S. Karat, "The Top 5 DDoS Attack Types We Saw in 2015," 2021. [Online]. Available: https://blog.radware.com/security/2016/01/top-ddos-attacks-2015/. [Accessed 19 06 2022].

[54] A. Langley, A. Riddoch, A. Wilk, A. Vicente, C. Krasic, D. Zhang, F. Yang, F. Kouranov, I. Swett, J. Iyengar and others, "The quic transport protocol: Design and internet-scale deployment," in *Proceedings of the conference of the ACM special interest group on data communication*, 2017.

[55] Cloudflare, "What is a DNS flood? | DNS flood DDoS attack," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack. [Accessed 19 06 2022].

[56] Radware, "DNS Flood Attack (DNS Flooding)," 2021. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/dns-flood/. [Accessed 19 06 2022].

[57] D. Guard, "DNS Amplification Attacks," 2021. [Online]. Available: https://ddos-guard.net/en/terminology/attack_type/ntp-flood.

[58] Cloudflare, "HTTP flood attack," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/. [Accessed 19 06 2022].

[59] Radware, "HTTPS Flood," 2021. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/https-flood/.

[60] Imperva, "The Top 10 DDoS Attack Trends," 2015. [Online]. Available: https://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf .

[61] Radware, "HTTP Fragmentation Attack," 2021. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/http-fragmentation-attack/. [Accessed 19 06 2022].

[62] Cloudflare, "What is a low and slow attack?," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/ddos-low-and-slow-attack/. [Accessed 19 06 2022].

[63] Radware, "Radware Cybersecurity Alert," 2020. [Online]. Available: https://www.radware.com/getattachment/Security/Threat-Advisories-and-Attack-Reports/2253/Alert-RDDoS-Attacks-Update-oct-2020-FINAL-v2.pdf.aspx/?lang=en-US/. [Accessed 19 06 2022].

[64] Radware, "Ransom DDoS Update: The Hunt For Unprotected Assets," 2021. [Online]. Available: https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/ransom-ddos-update-hunt-for-unprotected-assets/. [Accessed 19 06 2022].

[65] D. Guard, "Zero Day DDoS Guard," [Online]. Available: https://ddos-guard.net/en/terminology/attack_type/zero-day-ddos-attack-0day-ddos-attack. [Accessed 31 07 2022].

[66] Radware, "ZeroDay Radware," [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/zero-day-zero-minute-attack/. [Accessed 31 07 2022].

[67] K. Cruz, "The Anatomy of a Blended Attack," 2017. [Online]. Available: https://www.cloudbric.com/blog/2017/07/blended-attack-anatomy//. [Accessed 19 06 2022].

[68] K. a. A. Bock, A. a. Fax, Y. a. Hurley, K. a. Wustrow and D. Eric and Levin, "Weaponizing Middleboxes for," *30th USENIX Security Symposium (USENIX Security 21),* pp. 3345-3361, 2021.

[69] S. I. R. Team, "Akamai," 01 03 2022. [Online]. Available: https://www.akamai.com/blog/security/tcp-middlebox-reflection. [Accessed 19 06 2022].

[70] K. M. Prasad, A. R. M. Reddy and K. V. Rao, "DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey," *Global Journal of Computer Science and Technology,* 2014.

[71] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication systems,* vol. 73, p. 3–25, 2020.

[72] M. M. Salim, S. Rathore and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," *The Journal of Supercomputing,* vol. 76, p. 5320–5363, 2020.

[73] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE communications surveys & tutorials,* vol. 18, p. 602–622, 2015.

[74] S. Dong, K. Abbas and R. Jain, "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments," *IEEE Access,* vol. 7, p. 80813–80828, 2019.

[75] J. a. B. S. Singh, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Computer Science Review,* vol. 37, p. 100279, 2020.

[76] P. Kamboj, M. C. Trivedi, V. K. Yadav and V. K. Singh, "Detection techniques of DDoS attacks: A survey," in *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)*, 2017.

[77] K. N. Mallikarjunan, K. Muthupriya and S. M. Shalinie, "A survey of distributed denial of service attack," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, 2016.

[78] A. a. M. V. a. V. R. a. H. S. a. C. M. Bhardwaj, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Computer Science Review,* vol. 39, p. 100332, 2021.

[79] CAIDA, "CAIDA," [Online]. Available: https://www.caida.org/catalog/datasets/ddos-20070804_dataset/. [Accessed 18 08 2022].

[80] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review,* vol. 34, p. 39–53, 2004.

[81] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer networks,* vol. 44, no. 5, pp. 643-666, 2004.

[82] M. Chhabra, B. Gupta and A. Almomani, "A novel solution to handle DDOS attack in MANET," 2013.

[83] M. De Donno, N. Dragoni, A. Giaretta and A. Spognardi, "Analysis of DDoS-capable IoT malwares," in *2017 Federated Conference on Computer Science and Information Systems (FedCSIS),* 2017.

[84] X. Li, O. R. Zaiane and Z. Li, Advanced Data Mining and Applications: Second International Conference, ADMA 2006, Xi'an, China, August 14-16, 2006, Proceedings, vol. 4093, Springer, 2006.

[85] STEPS, "TAXONOMY OF DDOS ATTACK," [Online]. Available: https://www.stepskochi.com/blog/taxonomy-of-ddos-attack/. [Accessed 19 06 2022].

[86] P. Putman, "uscybersecurity," [Online]. Available: https://www.uscybersecurity.net/script-kiddie/. [Accessed 01 08 2022].

[87] H. Griffioen and C. Doerr, "Examining mirai's battle over the internet of things," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security,* 2020.

[88] netsplit, "IRC Networks - Top 10 in the annual comparison," 2021. [Online]. Available: https://netsplit.de/networks/top10.php?year=2021. [Accessed 19 06 2022].

[89] J. Nazario, "DDoS attack evolution," *Network Security,* vol. 2008, p. 7–10, 2008.

[90] H. Al-Alami, A. Hadi and H. Al-Bahadili, "Vulnerability scanning of IoT devices in Jordan using Shodan," in *2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes & Systems (IT-DREPS)*, 2017.

[91] L. Markowsky and G. Markowsky, "Scanning for vulnerable devices in the Internet of Things," in *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2015.

[92] Q. Gu and P. Liu, "Denial of service attacks," *Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications,* vol. 3, p. 454–468, 2007.

[93] V. Yegneswaran, P. Barford and J. Ullrich, "Internet intrusions: Global characteristics and prevalence," *ACM SIGMETRICS Performance Evaluation Review,* vol. 31, p. 138–147, 2003.

[94] P. K. Manna, S. Chen and S. Ranka, "Inside the permutation-scanning worms: Propagation modeling and analysis," *IEEE/ACM Transactions On Networking,* vol. 18, p. 858–870, 2009.

[95] nmap, "Nmap," [Online]. Available: https://nmap.org/. [Accessed 19 06 2022].

[96] G. Jevtic, "How to Scan & Find All Open Ports with Nmap," 2019. [Online]. Available: https://phoenixnap.com/kb/nmap-scan-open-ports. [Accessed 19 06 2022].

[97] Tenable, "Nessus," [Online]. Available: https://www.tenable.com/downloads/nessus. [Accessed 19 06 2022].

[98] C. B. Lee, C. Roedel and E. Silenok, "Detection and characterization of port scan attacks," *Univeristy of California, Department of Computer Science and Engineering,* 2003.

[99] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "AOCD: An Adaptive Outlier Based Coordinated Scan Detection Approach.," *Int. J. Netw. Secur.,* vol. 14, p. 339–351, 2012.

[100] G. O. System, "GNU Wget," [Online]. Available: https://www.gnu.org/software/wget/. [Accessed 19 06 2022].

[101] Avast, "Worm vs. Virus: What's the Difference and Does It Matter?," [Online]. Available: https://www.avast.com/c-worm-vs-virus. [Accessed 19 06 2022].

[102] Cisco, "What Is the Difference: Viruses, Worms, Trojans, and Bots?," [Online]. Available: https://tools.cisco.com/security/center/resources/virus_differences. [Accessed 19 06 2022].

[103] Malwarebytes, "Computer Virus," [Online]. Available: https://www.malwarebytes.com/computer-virus. [Accessed 19 06 2022].

[104] Kaspersky, "What is a Trojan horse and what damage can it do?," [Online]. Available: https://www.kaspersky.co.uk/resource-center/threats/trojans. [Accessed 19 06 2022].

[105] keycdn, "What Is a Botnet?," [Online]. Available: https://www.keycdn.com/support/what-is-a-botnet. [Accessed 19 06 2022].

[106] M. J. Molesky and E. A. Cameron, "Internet of Things: An analysis and proposal of white worm technology," in *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019.

[107] M. Eslahi, R. Salleh and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," in *2012 IEEE International Conference on Control System, Computing and Engineering*, 2012.

[108] G. Vormayr, T. Zseby and J. Fabini, "Botnet communication patterns," *IEEE Communications Surveys & Tutorials,* vol. 19, p. 2768–2796, 2017.

[109] G. Ollmann, "Botnet communication topologies," *Retrieved September,* vol. 30, p. 2009, 2009.

[110] Cloudflare, "What is a DDoS botnet?," [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/. [Accessed 19 06 2022].

[111] I. D. Ben, "Imperva," 10 2016. [Online]. Available: https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/?msclkid=a54b84a4ad2211ec832cf767e732556f. [Accessed 18 06 2022].

[112] Jerry, "Gigacycle Computer Recycling News," 28 08 2017. [Online]. Available: https://news.gigacycle.co.uk/mobile-wirex-ddos-botnet-neutralized-by-collaboration-of-competitors/. [Accessed 01 08 2022].

[113] J. Cochran, "Cloudflare," 28 08 2017. [Online]. Available: https://blog.cloudflare.com/the-wirex-botnet/. [Accessed 18 06 2022].

[114] NJCCIC, "NJCCIC," 30 08 2017. [Online]. Available: https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/wirex. [Accessed 18 06 2022].

[115] C. D. Team, "Cloudflare," 08 11 2021. [Online]. Available: https://radar.cloudflare.com/notebooks/meris-botnet). [Accessed 18 06 2022].

[116] H. W. Alex Turing, "Netlab," 23 12 2019. [Online]. Available: https://blog.netlab.360.com/mozi-another-botnet-using-dht/. [Accessed 18 06 2022].

[117] Europol, "Serious and Organised Crime Threat Assessment (SOCTA)," 2021. [Online]. Available: https://www.europol.europa.eu/publications-events/main-reports/socta-report. [Accessed 19 06 2022].

[118] Europol, "Internet Organised Crime Threat Assessment (IOCTA)," 2021. [Online]. Available: https://www.europol.europa.eu/publications-events/main-reports/iocta-report. [Accessed 19 06 2022].

[119] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville and A. Pras, "Booters—An analysis of DDoS-as-a-service attacks," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM),* 2015.

[120] Cloudflare, "What is a DDoS booter/IP stresser? | DDoS attack tools," [Online]. Available: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/#: :text=Booters%2C%20also%20known%20as%20booter%20services%2C%20are%20on-demand,the%20attacking%20server%20by%20use%20of%20proxy%20servers.. [Accessed 19 06 2022].

[121] Radware, "DDoS Attacks via DDoS as a Service Tools," 2016. [Online]. Available: https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/ddos-as-a-service/. [Accessed 19 06 2022].

[122] K. N. O. W. L. E. D. G. E. BRIEF, *Arbor Networks is Recognized as the 2017 Market and Technology Leader in the Global DDoS Mitigation Market,* 2017.

[123] NetScout, "Horizon NetScout," [Online]. Available: https://horizon.netscout.com/. [Accessed 21 06 2022].

[124] Cloudflare, "Cloudflare," [Online]. Available: https://radar.cloudflare.com/. [Accessed 21 06 2022].

[125] C. D. Team, "2021 Q2 DDoS Report," 2021. [Online]. Available: https://blog.cloudflare.com/ddos-attack-trends-for-2021-q2/. [Accessed 19 06 2022].

[126] A. Zand, G. Modelo-Howard, A. Tongaonkar, S.-J. Lee, C. Kruegel and G. Vigna, "Demystifying DDoS as a service," *IEEE Communications Magazine,* vol. 55, p. 14–21, 2017.

[127] Eyetro, "Anonymous kickstarts DDoS protest against Zimbabwe's government," 2019. [Online]. Available: https://www.eyetrodigital.com/2019/01/19/anonymous-kickstarts-ddos-protest-against-zimbabwes-government/. [Accessed 19 06 2022].

[128] K. Graewe, "DDoS Attacks 2019: A look back at the Developments over the Year," 2019. [Online]. Available: https://www.link11.com/en/blog/threat-landscape/ddos-attacks-2019-a-look-back-at-the-developments-over-the-year/. [Accessed 19 06 2022].

[129] F. Mudzingwa, "Anonymous Claims To Have Taken Down Zimbabwean Government Sites In Protest Against Unrest In The Country," 2019. [Online]. Available: https://www.techzim.co.zw/2019/01/anonymous-claims-to-have-taken-down-zimbabwean-government-sites-in-protest-against-recent-unrest-in-the-country/. [Accessed 19 06 2022].

[130] R. Hollier, "CRIMINOLOGY: WHY DO PEOPLE COMMIT CRIMES?," 2016. [Online]. Available: https://www.thelawproject.com.au/criminology-why-do-people-commit-crimes. [Accessed 19 06 2022].

[131] M. De Donno, A. Giaretta, N. Dragoni and A. Spognardi, "A taxonomy of distributed denial of service attacks," in *2017 International Conference on Information Society (i-Society),* 2017.

[132] A. Asosheh and N. Ramezani, "A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification," *WSEAS Transactions on Computers,* vol. 7, p. 281–290, 2008.

[133] T. Peng, C. Leckie and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Surveys (CSUR),* vol. 39, p. 3–es, 2007.

[134] M. A. M. Yusof, F. H. M. Ali and M. Y. Darus, "Detection and defense algorithms of different types of DDoS attacks," *International Journal of Engineering and Technology,* vol. 9, p. 410, 2017.

[135] E. Chickowski, "Types of DDoS attacks explained," 2020. [Online]. Available: https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained. [Accessed 19 06 2022].

[136] Cloudflare, "What is a DDoS attack?," 2021. [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. [Accessed 19 06 2022].

[137] G.-C. Labs, "The most dangerous DDoS attacks of our time," 2020. [Online]. Available: https://gcorelabs.com/blog/the-most-dangerous-ddos-attacks-of-our-time/. [Accessed 19 06 2022].

[138] J. Graham-Cumming, "Cloudflare Blog," 25 09 2017. [Online]. Available: https://blog.cloudflare.com/no-scrubs-architecture-unmetered-mitigation/. [Accessed 08 08 2022].

[139] D. Holmes, J. Blankenship, A. Bouffard and P. Dostie, "DDoS Mitigation Solutions," Forrest Wave, 2021.

[140] NetScout, "Arbor AED," [Online]. Available: https://www.netscout.com/product/netscout-aed. [Accessed 06 08 2022].

[141] NetScout, "NetScout - Arbor Cloud," [Online]. Available: https://www.netscout.com/product/arbor-cloud. [Accessed 06 08 2022].

[142] NetScout, "NetScout Hybrid," [Online]. Available: https://www.netscout.com/sites/default/files/2022-04/NETSCOUT%20-%20An%20On-Premises%20Defense%20is%20the%20Foundation.pdf. [Accessed 06 08 2022].

[143] NetScout, "NetScout Atlas," [Online]. Available: https://www.netscout.com/product/atlas-intelligence-feed-aif. [Accessed 06 08 2022].

[144] Q. K. Solutions, "NetScout," 2019. [Online]. Available: https://www.netscout.com/report/market-outlook-ddos-mitigation-2019-2024-worldwide. [Accessed 17 08 2022].

[145] Akamai, "Akamai Prolexic," [Online]. Available: https://www.akamai.com/resources/product-brief/prolexic-routed-product-brief. [Accessed 06 08 2022].

[146] Cloudflare, "Cloudflare," [Online]. Available: https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/. [Accessed 06 08 2022].

[147] 2Connect, "2Connect," 28 05 2017. [Online]. Available: https://www.leasedlineandmpls.co.uk/virtual-leased-lines/. [Accessed 06 08 2022].

[148] A. Liska, "O´REILLY," [Online]. Available: https://www.oreilly.com/library/view/threat-intelligence-in/9781492049302/ch04.html. [Accessed 07 08 2022].

[149] Radware, "Radware DefensePro," [Online]. Available: https://www.radware.com/products/defensepro/. [Accessed 07 08 2022].

[150] Radware, "Radware cloud solution," [Online]. Available: https://www.radware.com/products/cloud-ddos-services/. [Accessed 07 08 2022].

[151] Radware, "Radware SSL protection," [Online]. Available: https://www.radware.com/solutions/ssl-protection/. [Accessed 07 08 2022].

[152] Cloudflare, "Cloudflare," [Online]. Available: https://www.cloudflare.com/ddos/. [Accessed 08 08 2022].

[153] Cloudflare, "Cloudflare," [Online]. Available: https://www.cloudflare.com/products/argo-smart-routing/. [Accessed 08 08 2022].

[154] Imperva, "Imperva," [Online]. Available: https://www.imperva.com/products/ddos-protection-services/. [Accessed 08 08 2022].

[155] F5, "F5," [Online]. Available: https://www.f5.com/products/security/silverline/ddos-protection. [Accessed 08 08 2022].

[156] F5, "F5," [Online]. Available: https://www.f5.com/pdf/solution-profiles/f5-distributed-cloud-ddos-mitigation.pdf. [Accessed 08 08 2022].

[157] F5, "F5," [Online]. Available: https://www.f5.com/pdf/products/silverline-ddos-datasheet.pdf. [Accessed 08 08 2022].

[158] C. Point, "Check Point," [Online]. Available: https://www.checkpoint.com/downloads/products/ddos-protector-appliance-datasheet.pdf. [Accessed 08 08 2022].

[159] Snort, "Snort," [Online]. Available: https://www.snort.org/downloads. [Accessed 09 08 2022].

[160] Z. a. O. R. a. G. S. a. Z. A. a. S. M. a. o. Hassan, "Detection of distributed denial of service attacks using snort rules in cloud computing \& remote control systems," in *2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*, 2018.

[161] B. a. N. D. a. H. P. Karan, "Detection of DDoS attacks in software defined networks," in *2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS)*, 2018.

[162] Suricata, "Suricata," [Online]. Available: https://suricata.io/. [Accessed 09 08 2022].

[163] D. a. K. J. a. H. D. a. J. J. P. Hyun, "SDN-based network security functions for effective DDoS attack mitigation," in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, 2017.

[164] Pavel-odintsov, "Github FastNetMon," [Online]. Available: https://github.com/pavel-odintsov/fastnetmon. [Accessed 10 08 2022].

[165] FastNetMon, "FastNetMon," [Online]. Available: https://fastnetmon.com/price/. [Accessed 10 08 2022].

[166] J. a. F. Y. a. L. J. Mirkovic, "Measuring changes in regional network traffic due to covid-19 stay-at-home measures," in *arXiv preprint arXiv:2203.00742*, 2022.

[167] AltraMayor, "Github," [Online]. Available: https://github.com/AltraMayor/gatekeeper/wiki. [Accessed 10 08 2022].

[168] HAProxy, "GitHub," [Online]. Available: https://github.com/haproxy/haproxy/blob/master/doc/intro.txt. [Accessed 10 08 2022].

[169] HAProxy, "HAProxy," [Online]. Available: http://www.haproxy.org/#desc. [Accessed 10 08 2022].

[170] A. a. F. E. a. C. K. Ezenwe, "Mitigating Denial of Service Attacks with Load Balancing," *Journal of Robotics and Control (JRC)*, vol. 1, no. 4, pp. 129-135, 2020.

[171] R. R. a. Z. S. R. a. S. A. B. a. S. H. M. a. A. O. M. a. J. K. Zebari, "Distributed denial of service attack mitigation using high availability proxy and network load balancing," in *2020 International Conference on Advanced Science and Engineering (ICOASE),* 2020.

[172] A. a. B. S. M. a. S. S. A. Akbar, "Leveraging the sip load balancer to detect and mitigate ddos attacks," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT),* 2015.

[173] N. a. S. R. Kilari, "A novel approach to protect cloud environments against DDOS attacks," in *Big Data Analytics*, Springer, 2018, pp. 515-523.

[174] P. Szynkiewicz, "Signature-Based Detection of Botnet DDoS Attacks," in *Cybersecurity of Digital Service Chains*, Springer, 2022, pp. 120-135.

[175] I. a. C. D. a. B. E. Ko, "Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain," *ETRI Journal,* vol. 41, no. 5, pp. 574-584, 2019.

[176] Z. a. G. A. a. G. B. a. H. H. a. N. N. Zhou, "A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic," *Neural Computing and Applications,* pp. 1-14, 2021.

[177] L. a. Z. Y. a. X. Y. a. Z. T. Zhou, "A novel feature-based framework enabling multi-type DDoS attacks detection," *World Wide Web,* pp. 1-23, 2022.

[178] I. a. C. D. a. B. E. Ko, "Recurrent autonomous autoencoder for intelligent DDoS attack mitigation within the ISP domain," *International journal of machine learning and cybernetics,* vol. 12, no. 11, pp. 3145-3167, 2021.

[179] F. a. F. A. C. a. P. F. a. C. F. a. T. M. Musumeci, "Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks," *Journal of Network and Systems Management,* vol. 30, no. 1, pp. 1-27, 2022.

[180] S. a. H. M. R. a. M. M. a. B. V. a. S. V. Vattikuti, "DDoS Attack Detection and Mitigation using Anomaly Detection and Machine Learning Models," in *2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS),* 2021.

[181] M. a. S. A. a. P. A. Jonker, "DDoS Mitigation: A Measurement-Based Approach," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, 2020.

[182] J. a. L. X. a. J. J. a. Y. S. Li, "Too Expensive to Attack: Enlarge the Attack Expense through Joint Defense at the Edge," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2021.

[183] S. a. V. A. Sahu, "DDoS attack detection in ISP domain using machine learning," in *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA),* 2019.

[184] X. Z. a. C. L. a. D. D. M. a. K. M. S. Khooi, "DIDA: Distributed In-Network Defense Architecture Against Amplified Reflection DDoS Attacks," in *2020 6th IEEE Conference on Network Softwarization (NetSoft),* 2020.

[185] W. a. J. L. a. L. J. a. Z. R. You, "Scheduling DDoS Cloud Scrubbing in ISP Networks via Randomized Online Auctions," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, 2020.

[186] B. a. F. C. a. R. M. Rashidi, "A scalable and flexible DDoS mitigation system using network function virtualization," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, 2018.

[187] G. A. a. G. M. Sophia, "Stealthy DDoS detecting mechanism for cloud resilience system," in *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, 2017.

[188] B. K. a. S. V. J. a. G. A. V. a. S. T. Devi, "Classifying and Predicting DoS and DDoS Attacks on Cloud Services," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2018.

[189] W. J.-W. a. T. J. J. W. a. P. J. a. C. E.-C. Tann, "Filtering DDoS Attacks from Unlabeled Network Traffic Data Using Online Deep Learning," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021.

[190] F. S. d. a. S. F. A. a. d. M. B. J. A. a. V.-S. G. a. S. L. F. Lima Filho, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," *Security and Communication Networks,* vol. 2019, 2019.

[191] M. P. a. C. L. F. a. L. J. a. P. M. L. Novaes, "Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment," *IEEE Access,* vol. 8, pp. 83765-83781, 2020.

[192] R. a. B. G. a. Z. Z. a. D. H. Sahay, "Towards autonomic DDoS mitigation using software defined networking," in *SENT 2015: NDSS workshop on security of emerging networking technologies*, 2015.

[193] Z. a. C. Y. a. Z. M. a. G. W. Liu, "Umbrella: Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services," *IEEE Transactions on Information Forensics and Security,* vol. 14, no. 4, pp. 1098-1108, 2018.

[194] Z. a. J. H. a. H. Y.-C. a. B. M. Liu, "Practical Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control," *IEEE/ACM Transactions on Networking,* vol. 26, no. 4, pp. 1948-1961, 2018.

[195] Q. a. Y. F. R. a. G. Q. a. L. J. Yan, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," *IEEE communications surveys & tutorials,* vol. 18, no. 1, pp. 602-622, 2015.

[196] J. a. L. Q. a. G. G. a. C. J. a. Y. D. K. a. W. J. Zheng, "Realtime DDoS defense using COTS SDN switches via adaptive correlation analysis," *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 7, pp. 1838-1853, 2018.

[197] Y. a. L. K. a. Z. W. Xiang, "Low-rate DDoS attacks detection and traceback by using new information," *IEEE transactions on information forensics and security,* vol. 6, no. 2, pp. 426-437, 2011.

[198] S. a. Z. W. a. D. R. a. J. W. Yu, "Traceback of DDoS attacks using entropy variations," *IEEE transactions on parallel and distributed systems,* vol. 22, no. 3, pp. 412-425, 2010.

[199] P. a. T. M. a. N. A. a. C. M. a. L. C. Kumar, "SAFETY: Early detection and mitigation of TCP," *IEEE Transactions on Network and Service Management,* vol. 15, no. 4, pp. 1545-1559, 2018.

[200] V. a. I. P. R. a. M. D. a. F. M. M. de Miranda Rios, "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms," *Computer Networks,* vol. 186, p. 107792, 2021.

[201] Y. a. L. K. a. G. Z. a. W. Y. Gu, "Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm," *IEEE Access,* vol. 7, pp. 64351-64365, 2019.

[202] M. a. A. R. Suresh, "Evaluating machine learning algorithms for detecting DDoS attacks," in *International Conference on Network Security and Applications,* 2011, pp. 441-452.

[203] NIST, "NIST," [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. [Accessed 21 06 2022].

[204] Vodafone, "Vodafone Portugal alvo de ciberataque," 08 02 2022. [Online]. Available: https://www.vodafone.pt/press-releases/2022/2/vodafone-portugal-alvo-de-ciberataque.html. [Accessed 02 07 2022].

[205] Google, "Google Forms," [Online]. Available: https://www.google.com/forms/about/. [Accessed 04 08 2022].

[206] LimeSurvey, "LimeSurvey," [Online]. Available: https://www.limesurvey.org/pt/. [Accessed 04 08 2022].

[207] SurveyPlanet, "SurveyPlanet," [Online]. Available: https://surveyplanet.com/. [Accessed 04 08 2022].

[208] EUSurvey, "EUSurvey," [Online]. Available: https://ec.europa.eu/eusurvey/. [Accessed 04 08 2022].

[209] EUSurvey, "EUSurvey," [Online]. Available: https://ec.europa.eu/eusurvey/. [Accessed 22 06 2022].

[210] Variti, "Variti," [Online]. Available: https://variti.io/ddos-protection. [Accessed 06 06 2022].

[211] NetScout, "NetScout," [Online]. Available: https://www.netscout.com/. [Accessed 26 06 2022].

[212] FireEye, "FireEye," [Online]. Available: https://www.fireeye.com/cyber-map/threat-map.html. [Accessed 25 06 2022].

[213] Kaspersky, "Kaspersky," [Online]. Available: https://cybermap.kaspersky.com/. [Accessed 25 06 2022].

[214] S. Server, "Shadow Server," [Online]. Available: https://www.shadowserver.org/. [Accessed 25 06 2022].

[215] Shodan, "Shodan," [Online]. Available: https://www.shodan.io/. [Accessed 25 06 2022].

[216] Eintracht, "Eintracht," 15 03 2022. [Online]. Available: https://en.eintracht.de/news/eintracht-beendet-partnerschaft-mit-kaspersky-140037. [Accessed 25 06 2022].

[217] J. Brunoli, "Techzine," 18 03 2022. [Online]. Available: https://www.techzine.eu/news/security/75214/italian-government-to-cease-using-russian-anti-virus-software/. [Accessed 25 06 2022].

[218] O. Yoachimik, "Cloudflare," 06 07 2022. [Online]. Available: https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2/. [Accessed 20 08 2022].

[219] O. Yoachimik, "Cloudflare," 12 04 2022. [Online]. Available: https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/. [Accessed 20 08 2022].

[220] Eurostat, "Eurostat," [Online]. Available: https://ec.europa.eu/eurostat/web/structural-business-statistics/small-and-medium-sized-enterprises. [Accessed 22 08 2022].

[221] Eurostat, "Eurostat," [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Enterprise_size. [Accessed 22 08 2022].

[222] AWS, "AWS," [Online]. Available: https://aws.amazon.com/pt/?nc2=h_lg. [Accessed 23 08 2022].

[223] Google, "Google Cloud," [Online]. Available: https://cloud.google.com/. [Accessed 23 08 2022].

[224] FastNetMon, "FastNetMon," [Online]. Available: https://fastnetmon.com/ddos-detection-and-mitigation/. [Accessed 26 08 2022].

[225] FastNetMon, "FastNetMon," [Online]. Available: https://fastnetmon.com/docs/detected_attack_types/. [Accessed 26 08 2022].

[226] C. Lavoie, "HAProxy," 09 11 2018. [Online]. Available: https://www.haproxy.com/blog/application-layer-ddos-attack-protection-with-haproxy/. [Accessed 26 08 2022].

[227] B. Assmann, "HAProxy," 10 02 2016. [Online]. [Accessed 26 08 2022].

[228] F5, "F5," [Online]. Available: https://www.f5.com/pdf/white-papers/mitigating-ddos-attacks-tech-brief.pdf. [Accessed 26 08 2022].

[229] Cloudflare, "Cloudflare," [Online]. Available: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/. [Accessed 26 08 2022].

[230] Akamai, "Akamai," [Online]. Available: https://www.akamai.com/our-thinking/ddos. [Accessed 26 08 2022].

[231] C. Sparling, "Akamai," 27 07 2022. [Online]. Available: https://www.akamai.com/blog/security/largest-european-ddos-attack-ever. [Accessed 26 08 2022].

[232] C. Point, "Check Point," [Online]. Available: https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/35013/FILE/CP_DDoS_protection_on_the_Gateway_BestPractices.pdf. [Accessed 26 08 2022].

[233] NetScout, "NetScout," [Online]. Available: https://www.netscout.com/sites/default/files/2022-03/ThreatReport_2H2021_WEB.pdf. [Accessed 26 08 2022].

[234] Radware, "Radware," [Online]. Available: https://www.radware.com/getattachment/ba8a3263-703b-4cc7-a5d0-741dc00e9273/H1-2022-Threat-Analysis-Report_2022_Report-V2.pdf.aspx. [Accessed 26 08 2022].

[235] B. Fung, "CNNBusiness," 10 08 2022. [Online]. Available: https://edition.cnn.com/2022/08/10/tech/companies-data-sharing-cyberattacks/index.html. [Accessed 30 08 2022].

Appendices

Appendix A
Imperva’s response email to the demo request

In this appendix, we will present different figures that demonstrates the attack flows of different types of DDoS attacks.

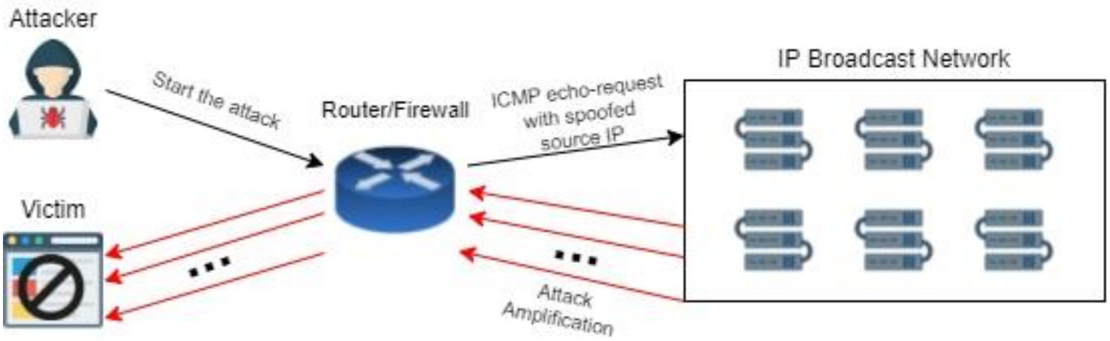


Figure A.1. Smurf Attack

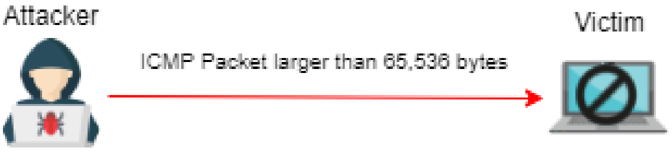


Figure A.2. Ping of Death Attack

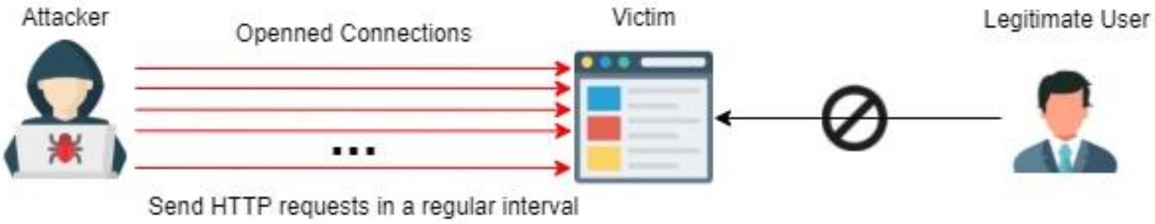


Figure A.3. Slowloris Attack

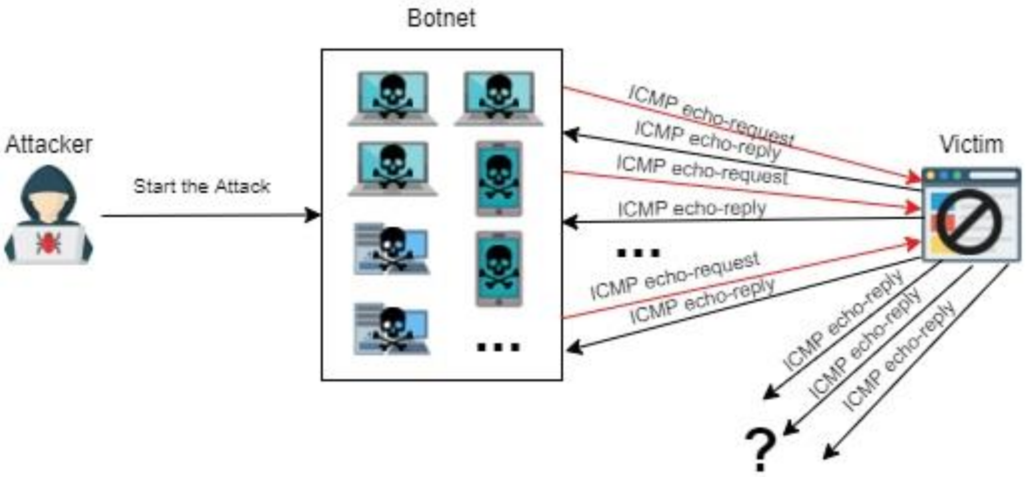


Figure A.4. ICMP Flood Attack

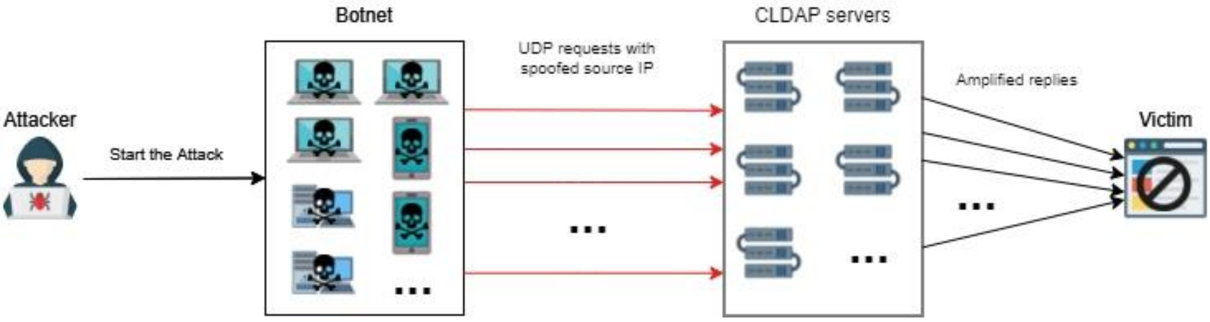


Figure A.5. CLDAP Amplification Attack

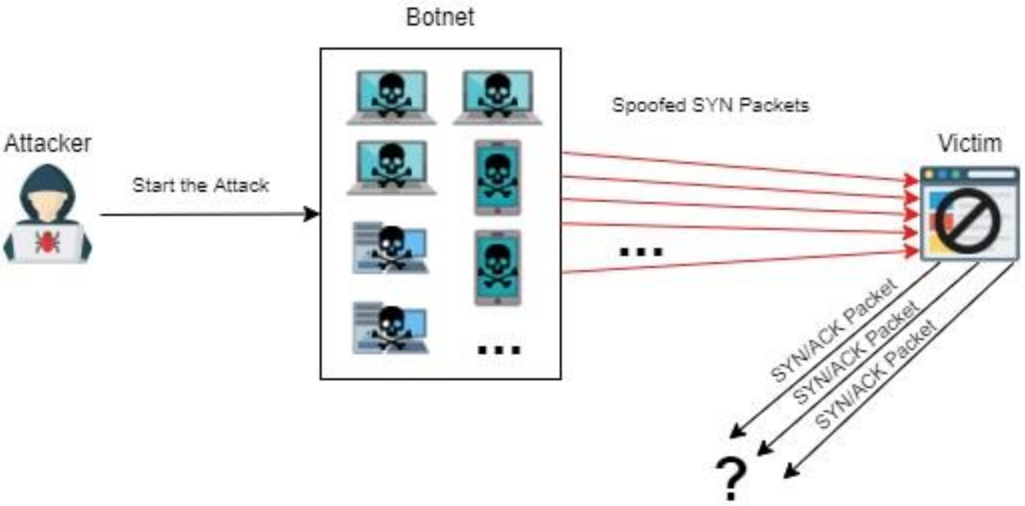


Figure A.6. SYN Flood Attack

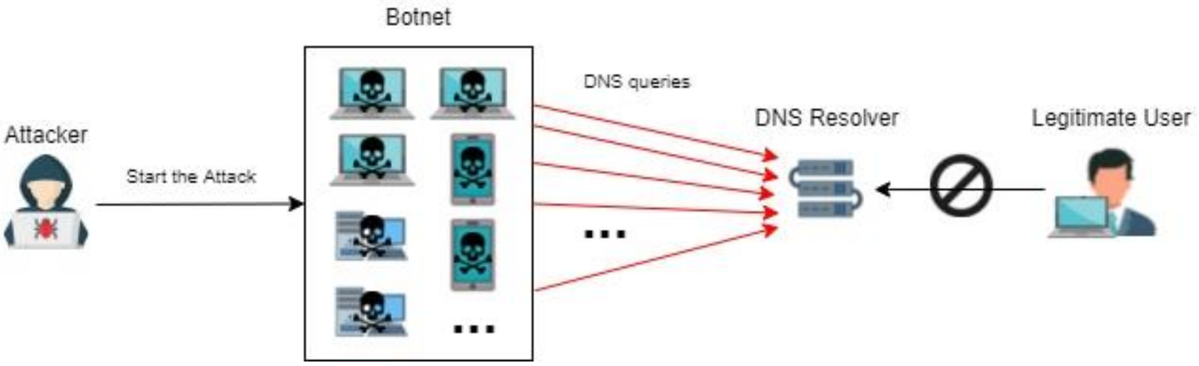


Figure A.7. DNS Flood Attack

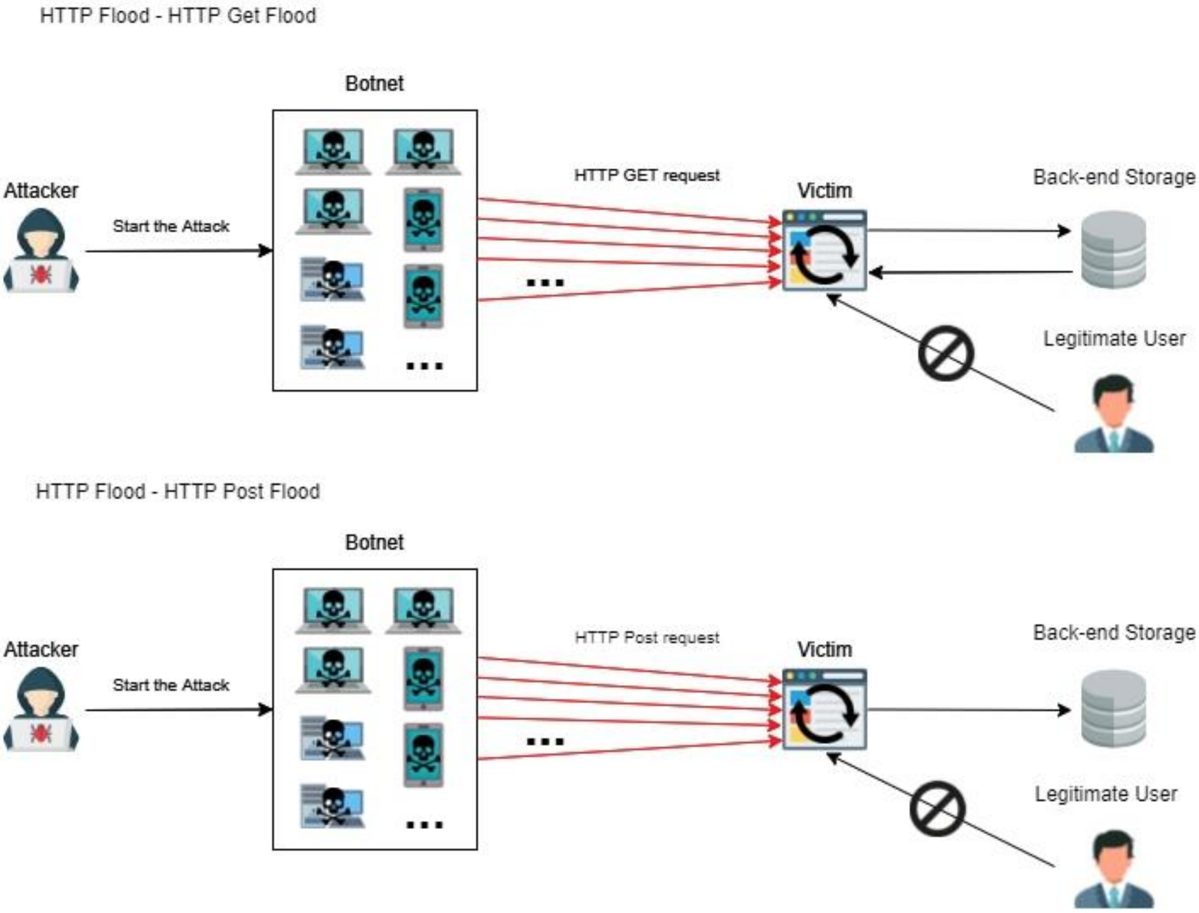


Figure A.8. HTTP Flood Attack (GET and POST)

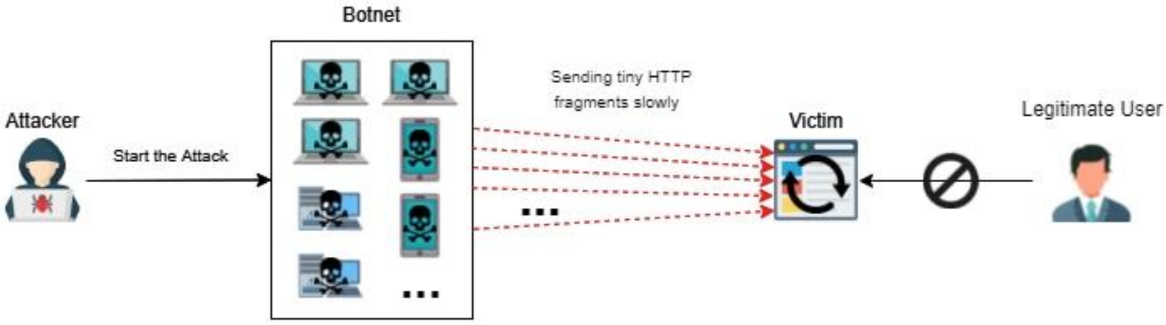
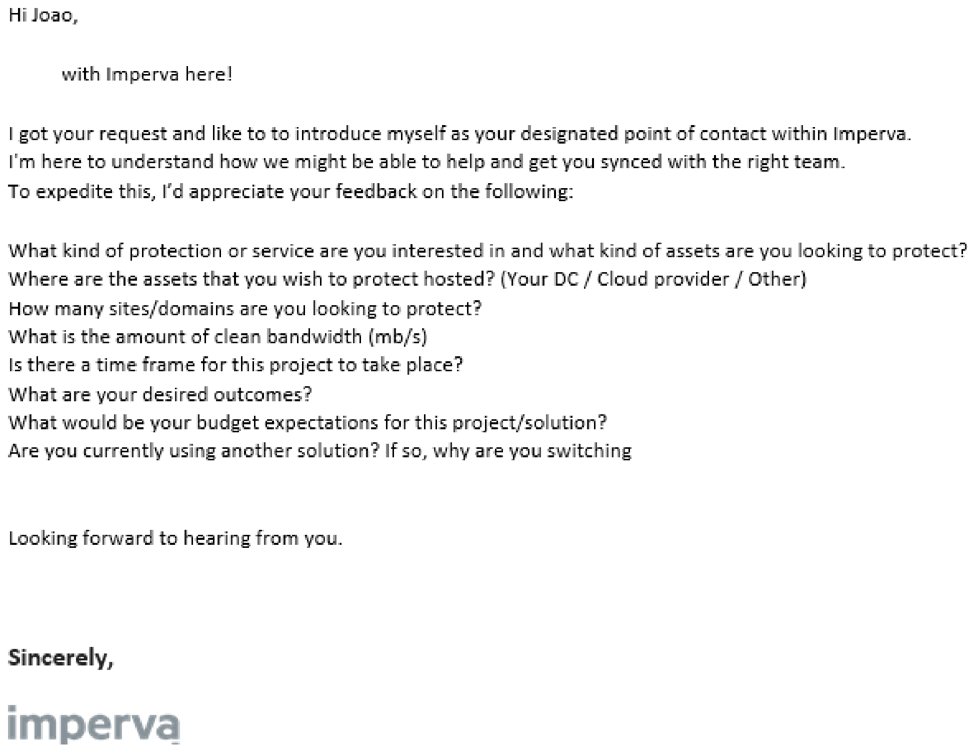


Figure A.9. HTTP Fragmentation Attack

Appendix B
Imperva’s response email to the demo request



Hi Joao,

with Imperva here!

I got your request and like to to introduce myself as your designated point of contact within Imperva.
I'm here to understand how we might be able to help and get you synced with the right team.
To expedite this, I’d appreciate your feedback on the following:

What kind of protection or service are you interested in and what kind of assets are you looking to protect?
Where are the assets that you wish to protect hosted? (Your DC / Cloud provider / Other)
How many sites/domains are you looking to protect?
What is the amount of clean bandwidth (mb/s)
Is there a time frame for this project to take place?
What are your desired outcomes?
What would be your budget expectations for this project/solution?
Are you currently using another solution? If so, why are you switching

Looking forward to hearing from you.

Sincerely,

imperva

Figure B.10. Imperva email with the questions they need, so they can provide the solution demonstration

Appendix C
The 22 Solutions described in the Literature

Table C.1. Types of DDoS protection that each of the 22 other solutions described in the literature provides

Papers	Prevention	Detection	Mitigation	Tolerance
Signature-Based Detection of Botnet DDoS Attacks [174]		✓	✓	
Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain [175]		✓	✓	
A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic [176]		✓		
A novel feature-based framework enabling multi-type DDoS attacks detection [177]		✓		
Recurrent autonomous autoencoder for intelligent DDoS attack mitigation within the ISP domain [178]			✓	
Machine-Learning-Enabled DDoS Attacks Detection in P4 Programmable Networks [179]		✓	✓	
DDoS Attack Detection and Mitigation using Anomaly Detection and Machine Learning Models [180]		✓	✓	
DDoS Mitigation: A Measurement-Based Approach [181]		✓	✓	
Too Expensive to Attack: Enlarge the Attack Expense through Joint Defense at the Edge [182]	✓			
DDoS attack detection in ISP domain using machine learning [183]		✓	✓	
DIDA: Distributed In-Network Defense Architecture Against Amplified Reflection DDoS Attacks [184]		✓	✓	
Scheduling DDoS Cloud Scrubbing in ISP Networks via Randomized Online Auctions [185]	✓	✓	✓	
A scalable and flexible DDoS mitigation system using network function virtualization [186]		✓	✓	

Stealthy DDoS detecting mechanism for cloud resilience system [187]		✓		
Classifying and Predicting DoS and DDoS Attacks on Cloud Services [188]	✓	✓		
Filtering DDoS Attacks from Unlabeled Network Traffic Data Using Online Deep Learning [189]		✓	✓	
Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning [190]		✓		
Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment [191]		✓	✓	
Towards autonomic DDoS mitigation using Software Defined Networking [192]		✓	✓	
Umbrella: Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services [193]			✓	
Practical Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control [194]	✓			
Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges [195]				✓