TARGETING FINANCIAL ORGANISATIONS WITH DDOS

A multi-sided perspective

TU Delft Delft University of Technology

EY Building a better working world

Ryan Cheung
Systems Engineering, Policy Analysis and Management (SEPAM)
Faculty of Technology, Policy and Management (TPM)

This page intentionally left blank

Targeting financial organisations with DDoS: a multi-sided perspective

Comparing patterns in AmpPot data to experts view on target selection in the financial sector

By

R.T.M. Cheung

Student ID: **4096789**

Contact **rtmcheung@gmail.com**

Thesis Committee

Prof. dr. M.J.G. van Eeten	Delft University of Technology
Dr. C. H. G. Gañán	Delft University of Technology
Dr. A.M. Herdeiro Teixeira	Delft University of technology
V. Waart MSc	EY

Preface

This thesis will be my final requirement into becoming a graduated engineer of the master Systems Engineering, Policy Analysis and Management at Delft University of Technology. It is the result of a 7 years journey which has helped my not only academically, but also personally. In these years, I have gained valuable knowledge that I will cherish the rest of my life.

This thesis would not been possible with the help of my formidable thesis committee. I want to take this opportunity to thank Michel, Carlos, and André for their full support, enthusiasm, and constructive feedback. I would also like to thank Arman who has helped me more times than I dare to admit with countless of challenges and the constructing of my thesis in general.

I wish to thank Vincent Waart, my supervisor at EY, who took the time to mentor me, help me see things from a more practical perspective, and helped me finding the right persons to interview. In extension to that, I would like to thank all within EY that made my internship a memorable period, and made me feel part of the team.

Finally, I would like to thank my family and friends whom have supported me not only during the last couple of months, but have been there during countless of challenging times. Special thanks to my parents, whom have strived to give me the best. You have inspired me that with hard work one can accomplish anything. Your love and kindness have made me the person I am today.

R.T.M. Cheung
Zoetermeer, July 2017

"*In the world of cyber security, the last thing you want is to have a target painted on you*"

By Tim Cook

Executive Summary

Introduction and problem description

Since its inception, the Internet has gone through a multitude of developments and rapid expansion worldwide. Just like every other technological revolution, the Internet has its own issues and threats. Cybercrime has become one of the biggest drawbacks that threaten the use of the Internet. Moreover, cyber related crimes have gained increasing undivided attention nationally as well as internationally. Often, these cyber-attacks are causes for major outages and disruptions of services or websites. These outages are caused by one of the oldest techniques for cyber-attacks, namely: Distributed-Denial-of-services (DDoS). These types of attacks overload a system or service through a large sum of illegitimate traffic, to ensure the system is unavailable for users. Recently, these types of attacks have been commoditised and are available for a wide variety of possible attackers. Attacks can be purchased on the Internet and only require an IP address to target, thus increasing the range of possible attackers. With the help of amplification techniques, these attacks have resulted in an increase in size of the attacks. DDoS attack victims generally suffer from large-scale financial losses owing to the disruption of services, efforts for mitigating the attack, damage recovery, and potential threat to customer satisfaction levels and market opportunities.

Due to the advent of the Internet, many services in the financial sector have been providing online resources and information portals. Unfortunately, this has placed the financial organisations in an exposed prey scenario. While they have been battling against other types of cybercrime like hacking and virus attacks, DDoS is still a major threat and has resulted in high financial costs. Researchers argue that the popularity of these attacks can generally be attributed to the failure to locate the source of these attacks. Due to the inability of catching attackers, there is still a large knowledge gap regarding the reasons for these attacks. Furthermore, research has shown that there is a large disproportionate difference in the number of attacks between various financial service organisations (FSOs). In literature, there have been various studies focused on the DDoS phenomenon. Many researchers have done in-depth studies on the technical side of DDoS such as their execution, and mitigation. Less focus has been given to the socio-technical side the influence on the increase in the attack rates. Globally, recent studies have shown that socio-technical measures are required in combatting DDoS attacks. Along similar lines, few studies have also focused on the victim side to sensitize them with the current state of DDoS as a whole. Therefore, this research will specifically focus on the socio-technical factors that influence target selection of DDoS amplification attacks.

Research objective and questions

This research intends to identify factors that influence the target selection of DDoS amplification attacks in the financial sector. To achieve this objective, both quantitative analysis using honeypot data and qualitative analysis using opinion of experts in the financial sector are used. To reach this objective, the following main research question is formulated:

Which factors influence target selection of financial services organisations suffering from DDoS amplification attacks?

To come with a clear answer, four coherent research questions were formulated.

RQ1: Based on what factors do attackers choose their financial target, and how do these attacks influence FSOs according to literature?

RQ2: Which factors influence the target selection via booters according to the AmpPot data, and how can these factors be traced back to FSOs?

RQ3: Which factors influence target selection of DDoS amplification attacks according to experts in FSOs, and how have they coped with those factors?

RQ4: What are the similarities and differences between the target selection factors according to the AmpPot data and the opinion of experts?

To answer the research questions, a mixed method approach, of both quantitative and qualitative research methods was used. Firstly, a literature study on the current DDoS landscape is conducted. Based on these insights, an explorative and statistical analysis on the AmpPot data was done. AmpPot consists of using honeypots that gathered data about DDoS amplification attacks all around the world in the period of 2014 to 2015. In order to acquire the financial data from AmpPot, a list of keywords was used to map the financial organisations in the AmpPot data. For the qualitative analysis nine semi-structured interviews were performed with cyber security experts in the financial sector within the Netherlands. To acquire a diverse group of respondents, interviews with experts of various backgrounds and from small and big organisations were conducted. The results of both the literature study and quantitative analysis were used as an input for qualitative analysis. The quantitative and qualitative analyses are then compared to get a comprehensive overview about the specific factors that influence target selection according to both.

Conclusion and recommendations

The AmpPot data showed that among the researched factors, there are various country-level factors that influence the target selection of cybercriminals. Among them are the ICT development index (IDI), which a number between 1 and 10 that determines the development of the ICT within a country, and the Nominal GDP Per capita. While literature has also shown that the country is a factor for the target selection, few have mentioned specific country-level factors. In addition, the data showed that an increase in IDI and Nominal GDP Per Capita decreases the number of attacks, while most researches have mentioned it the opposite way around. Furthermore, on organizational level, the data showed a significant effect that attackers would target an organisation with a higher market value more often. Also, banks and various investment groups were among the top targeted organisations, while purely IT oriented FSOs were not frequently attacked. Surprisingly, the financial data showed that the weekday does affect the number of attacks. Organisations incur a significant amount of attacks on Fridays compared to other days. The reason for this increase remains unclear. Analysing the opinion of experts, this research found that the organisation size, reputation, media attention, speed of updating, having a capable guardian and employees and the country are target selection factors. While the size of an organisation showed little effect on the number of attacks in the quantitative analysis, experts argue that the media attention and reputation seems to be a secondary factor that is related to the size and target selection.

An overview of the factors that influence target selection is given below:

Quantitative analysis

- Location/Country
- Organisation size
- Type of organisation
- Weekday

Qualitative analysis

- Organisation size
- Reputation
- Media attention
- Patching/updating speed
- Capable guardian
- Capable employees
- Location/country

Based on these findings there are some notable differences compared to current research. First, the weekday can be added as a significant influential factor for target selection. Second, size showed a limited effect on the number of attacks. This research implies that there are secondary factors such as media attention and reputation that influence the target selection more directly. Thirdly, country-level factors such as the IDI and Normal GDP Per Capita influence the target

selection, however, an increase in those factors would reduce the number of attacks. Furthermore, attackers also focus on internal organisation factors which influence the impact such as having a capable guardian, having capable employees, and the speed of patching/updates by an organisation.

In order to utilize these findings, certain actions have to be taken by FSOs. The following recommendations are given:

- Due to the differences in target selection between countries, it is important to work internationally to share knowledge in order to educate less developed organisations/countries.
- Even though size was not an influential factor for target selection, large organisations should be focussing on the factors that trigger criminals to target them. These organisations have the financial means to do research on this particular topic, which helps tackling the DDoS issue as such.
- The financial institutions should allot as such attention to the origins of the attack as to mitigating the damages caused by attacks.
- Based on the qualitative analysis, FSOs should focus more on the motivations of the attacks. It is important to know the motivations behind an attack as this will help to understand why the FSO is being targeted. As the motivation cannot be observed from solely the attack, FSOs should have already probable scenarios in place to exclude unlikely motivations.
- Based on the quantitative analysis, FSOs should be more alert on DDoS attacks on Fridays, due to the higher risk of getting attacked. However, as no clear argument can be given for this development it still has to be studied, how this relate to an organisation.

As DDoS does not limit itself to organisational boundaries, recommendations are also mentioned that are not specific for financial organisations:

- It is important that attackers are caught and prosecuted. This would result in better understanding the attack motivations and thus how to understand target selection. This asks for a close cooperation between organisations and law enforcement institutions.
- As DDoS are increasing in power, inter-sectorial cooperation should be stimulated. An example could be collaboration between ISPs and financial institutions to be able to exclude between traffic from different countries or continents, or tackle the issue of spoofing.
- Sharing knowledge both within and between sectors is encouraged. Organisations should share information about the reasons behind the attack, from which IP the attack is coming from, and the bandwidth.

List of abbreviations

AS	Autonomous system
BAF	Bandwidth amplification factors
BTC	Bitcoin
CHG	CharGen
C&C	Command & Control
DDoS	Distributed Denial of Services
DRDoS	Distributed reflection Denial of Services
DNS	Domain Name System
FACTA	Foreign Account Tax Compliance Act
FFI	Foreign financial institution
FSO	Financial Services Organisation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDI	ICT Development Index
ISACs	Information sharing analysis communities
IP	Internet Protocol
IRS	Internal Revenue Service
LAN	Local Area Network
NTP	Network Time Protocol
OSI	Open System Interconnection
P2P	Peer to Peer
QOTD	Quote of The Day
RAT	Routine activity theory
SLA	Service Level Agreement
SOC	Security Operations Centre
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator

Table of Contents

List of figures

List of Tables

PART I: Introduction and problem statement

1. Introduction

1.1 Introduction to the subject

The biggest innovation in the last 30 years is arguably the arrival of the Internet. With the help of the Internet, globalisation really took off, and new and old companies flourished. The Internet has changed our lives in many ways. It has revolutionized our communication and is involved in almost every little aspect of general human life. However, alongside the positive benefits, numerous opportunistic threats have also risen. Privacy issues, cybercriminals, malware, and other malicious software are subjects we read daily in the media.

Cybercrime has climbed to the top tier in the National Security Strategy of many EU states e.g. France, the Netherlands and the UK, becoming the number one threat above organized crime and fraud generally (Armin et al., 2015). One of the biggest and oldest cyber threats societies currently have to face are the distributed-Denial-of-Services (DDoS) attacks. DDoS attacks are one of the most eminent threats in the cyber landscape according to various researchers (Alvarez, n.d.; Holl, 2015). Recently the techniques of DDoS attacks have changed. Even though DDoS attacks have been around for many years, the use of amplification techniques has transformed the ecosystem of criminals. This shift is related to a new trend, namely, the emerge of DDoS-as-a-service or booters (Jose Jair Santanna et al., 2015). Formerly, DDoS attacks were solely coming from botmasters, which were the controllers of a collection of computers that were infected by malware, also called a botnet. Maintaining a botnet was rather time intensive, risky and technical endeavour. However, these days the services of botnets are put up for rent and are even traded among attackers. These commercial entities are trading in huge numbers of infected computers. Taking those services down is hard since they often hide behind the ambiguous but legal definitions of 'stressers' or 'booters'. These websites provide richly featured toolkits and even distributed networks to execute attacks whenever the attacker wants. The amounts of booters as well as their firepower are rapidly increasing, which makes them a threat for the cyber realm. This increase in firepower is mainly due to so-called amplification or reflection techniques (Kambourakis, Moschos, Geneiatakis, & Gritzalis, 2008). As this research focuses mainly on amplification based DDoS services, purely for the purpose of this research thesis, booters will be used as a synonym to DDoS amplification attacks. It has to be kept in mind that this outside this research, booters can be used for all sorts of DDoS techniques.

1.2 Problem description and research questions

As cybercrime has become an important threat to current societies, it is important to understand the problem at hand. This section provides the problem description and the context in which this research shall take place. While there are many cybercrime activities, DDoS attacks are considered the number one operational threat on the Internet. For many industries, such as e-commerce and online financial services, DDoS attacks are especially devastating. To those industries, DDoS attacks cause millions in revenue losses, reputation damage, and customer attrition (Chromik, Santanna, Sperotto, & Pras, 2015).

A recent change in the DDoS landscape has made DDoS attacks a more apparent threat. Through the Internet, it is now possible to launch a DDoS attack via various websites. The low price and easy access of these websites provide DDoS attacks with the ease of attack at the press of a button. Nowadays almost everybody, regardless of the attackers' IT knowledge, can command a DDoS cyber-attack (Groot, 2015; Karami, Park, & McCoy, 2015). These so-called booters have made it irrelevant to have expert knowledge; even attackers with little knowledge, preparation, and resources can cause a high degree of damage. Until recently these attacks did little to damage more resilient companies, and could essentially cripple SME's for a shorter duration.

However, due to new techniques these DDoS attacks can increase the intensity of attacks, which pose as a greater threat to more resilient companies.

There have already been various in-depth studies on the DDoS landscape as a whole. Numerous studies have focused on the technical side of DDoS. These studies have already classified the type of attacks, the volume of attacks, the damages a DDoS attack can bring both economically and socially, the attack strategies, and the economics of the DDoS service providers such as revenue streams and their customers (Karami & Mccoy, 2013; José Jair Santanna, Durban, Sperotto, & Pras, 2015). These studies have mostly been built around data that was made available by DDoS mitigation providers, honeypots, and estimates by academics. While DDoS has been a technical attack, cyber risks also arise in socio-technical context (Berg et al., 2014). Less research, however, has focused on the more socio-technical side of DDoS attacks such as the impact it has on the victims. Due to difficulties of catching attackers worldwide, there still remains a large knowledge gap in the motivations behind the specific DDoS attacks. Furthermore, studies have shown that there is a disproportionate difference in the number of attacks on the types of financial organisations, with banks being the main targets of DDoS attacks (Pras, Santanna, Steinberger, & Speretto, 2016; Turner, 2014; Zargar, Joshi, Tipper, & Member, 2013). However, accurate and complete research that purely focuses on the implication using DDoS amplification techniques on financial service organisations (FSOs) and how they perceive the DDoS environment as a whole is limited. This research aspires to provide insight into the specific target selection of DDoS amplification attacks from the socio-technical perspective. Therefore this research positions itself between the attacker and the victims with an aim to provide a better understanding of the motivation behind cyber victimization.

1.3 Knowledge gaps

As described in the previous section, there are various research gaps to be understood. The following are addressed in this research:

- Research focused on technical side of DDoS, while socio-technical side is equally important.
- Little research done on the effects of DDoS amplification attacks in the financial sector.
- Not much known about the target selection of DDoS amplification attacks in the financial sector, and the reasons behind those attacks.
- Little research on the security measures of FSOs to defend against or counter DDoS amplification attacks.

1.4 Research objective

Based on the problem description, the main objective of this research is *to identify factors that influence the target selection of DDoS amplification attacks in the financial services sector.* Achieving this research objective will be done using various quantitative and qualitative analysis. The final deliverable will be insight into the DDoS amplification on the financial sector and an advice on which factors financial institutions should focus to influence the attack rate.

1.5 Research questions

This section describes the research questions that need to be answered in order to reach the research objective stated above (identify factors that influence the target selection of DDoS amplification attacks in the financial services sector). To achieve the objective, the main research objective is translated into a single research question and its corresponding sub-questions. Answering the different sub-question provides a certain insight and knowledge that will help answering the main research question. The following main research question has been constructed:

Which factors influence target selection of financial services organisations suffering from DDoS amplification attacks?

Answering this question will be done using a comparison of gathered quantitative DDoS attack data and gathered data from experts through interviews. These qualitative and quantitative data are the central source of information for this research. Both datasets could complement each other as the quantitative data provide factors of DDoS attacks. Due to the complexity of the main research question and navigating from a central question is hard, a set of more specific research questions is formulated. Below the various research questions, their sub-questions, and their corresponding deliverables are presented.

RQ1: Based on what factors do attackers choose their financial target, and how do these attacks influence FSOs according to literature?

SQ1: What is DDoS amplification, and what are their threats?
SQ2: What are the risks and consequences of DDoS amplification attacks for FSOs?
SQ3: What factors influence DDoS target selection according to literature?

Deliverable I: review of the current DDoS amplification landscape and their impact on FSOs.

This research question gives a generic overview of the DDoS attack landscape. Given this overview, a better understanding on how they work, how they operate, and how they affect the financial world according to the literature. This question will be answered using desk research (literature review, and communication with supervisors etc.).

RQ2: Which factors influence target selection via booters according to the AmpPot data, and how can these factors be traced back to the FSOs?

SQ4: What are the proportions of FSOs in the AmpPot data?
SQ5: Which factors are considered a threat according to the AmpPot data?
SQ6: What are the characteristics of the FS0s that are being attacked?

Deliverable II: List of factors that influence the target selection of booters.

This question will focus mainly on the quantitative analysis and provide a list of factors that will influence target selection. These factors will be determined using a DDoS attack datasets received from the TU Delft. To analyse how the variables are correlated, (multiple) linear regression analyses will be done using the programming languages Python and R and various software tools such as RStudio and Pycharm. More information about the AmpPot data can be found in section 2.3.

RQ3: Which factors influence target selection of DDoS amplification attacks according to experts in FSOs, and how have they coped with those factors?

SQ7: How has the threat of DDoS amplification attacks affected victims in FSOs?
SQ8: What are the current practices to defend against DDoS attacks?
SQ9: What factors do attackers focus on in selecting a suitable target according to experts?

Deliverable III: Insight in the knowledge and know-how of various actors in the field of cyber security.

The third question will give insight in what experts in the financial field think of target selection. Using interview techniques an understanding of how organisations defend their organisations against DDoS attacks, and if/how they have anticipated on new DDoS threats and developments. Due to time constraints a small amount of respondents can be interviewed.

RQ4: What are the similarities and differences between the target selection factors according to the AmpPot data and the opinion of experts?

SQ10: What are the similarities between the AmpPot data and the opinion of experts?
SQ12: What are the differences between the AmpPot data and the opinion of experts?
SQ12: How can the previous findings be complemented to each other?

Deliverable IV: Discussion and conclusion on the similarities and differences.

The last question tries to bring all the previous questions together to make a comparison between what happens according to the AmpPot dataset, and what happens in the FSOs. A comparison is very useful to fully understand the possible similarities and differences. The conclusion of this research will discuss the findings, and how this can affect the future of defence against cyber threats. The final deliverable will be a recommendation on how organisations can cope with the target selection factors of DDoS (amplification) attacks. The research questions and their interrelations are visualised in Figure 1.

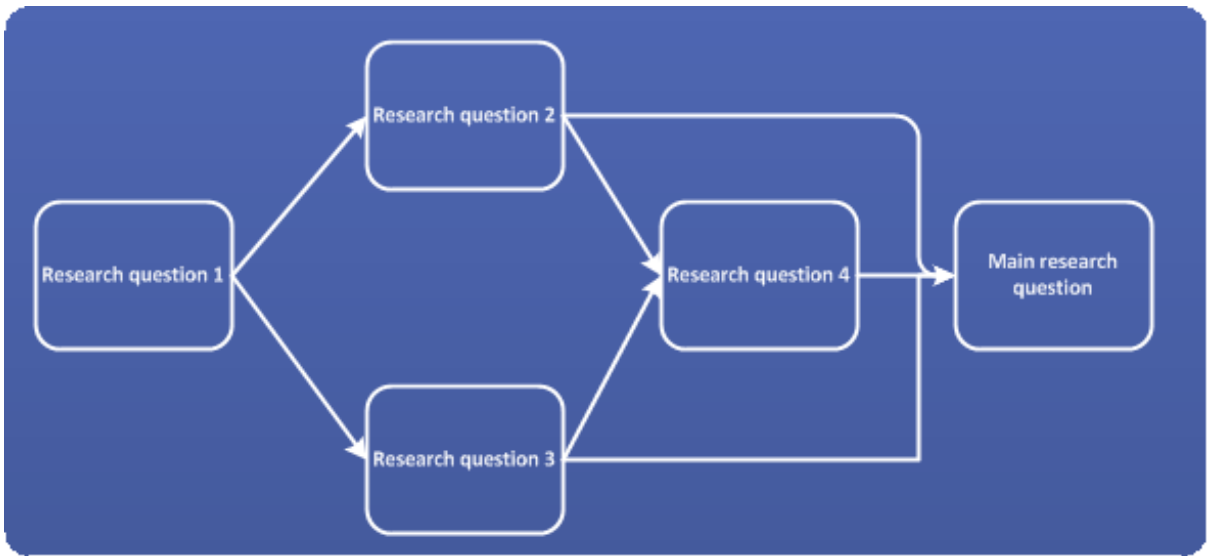

Figure 1: Research questions and their interrelations

1.6 Research design

Concluding, the research design, as can be seen in Figure 2 was set up. The first phase entails the preliminary research and theoretical framework. This phase will include a literature study on DDoS amplification attacks, a literature study on DDoS in the financial world, and a literature study on the known factors that influence target selection. The theoretical framework will shape the answers for the first research question. The theoretical framework is followed by the field research, which note the quantitative and qualitative analysis. The quantitative analysis comprises of analysing the AmpPot dataset. The analysis includes a descriptive analysis to pinpoint possible attack factors. Thereafter, an explanatory analysis will be held, which use statistical analysis, to test for significance of the identified attack factors. Lastly, the results will be discussed and analysed to answer the second research question. After identifying factors from the qualitative analysis, the quantitative analysis will be conducted. For this part, interviews will be constructed and conducted using financial cyber security experts. Questions are partially constructed using the input from the quantitative research. However, it is

important to also find factors that cannot be found in the quantitative data. Therefore the experts are asked to give their unvarnished opinion and view on target selection. The gathered data is then further analysed to understand the viewpoints of experts on DDoS amplification techniques and their influence on targets. The qualitative analysis allows for answering the third research question. Combining and comparing the results of previous results will be executed the following section. Aggregated, these results will lead to the formation of the final conclusions and recommendations. These conclusions correspond with answering the main research question and objective of this study.

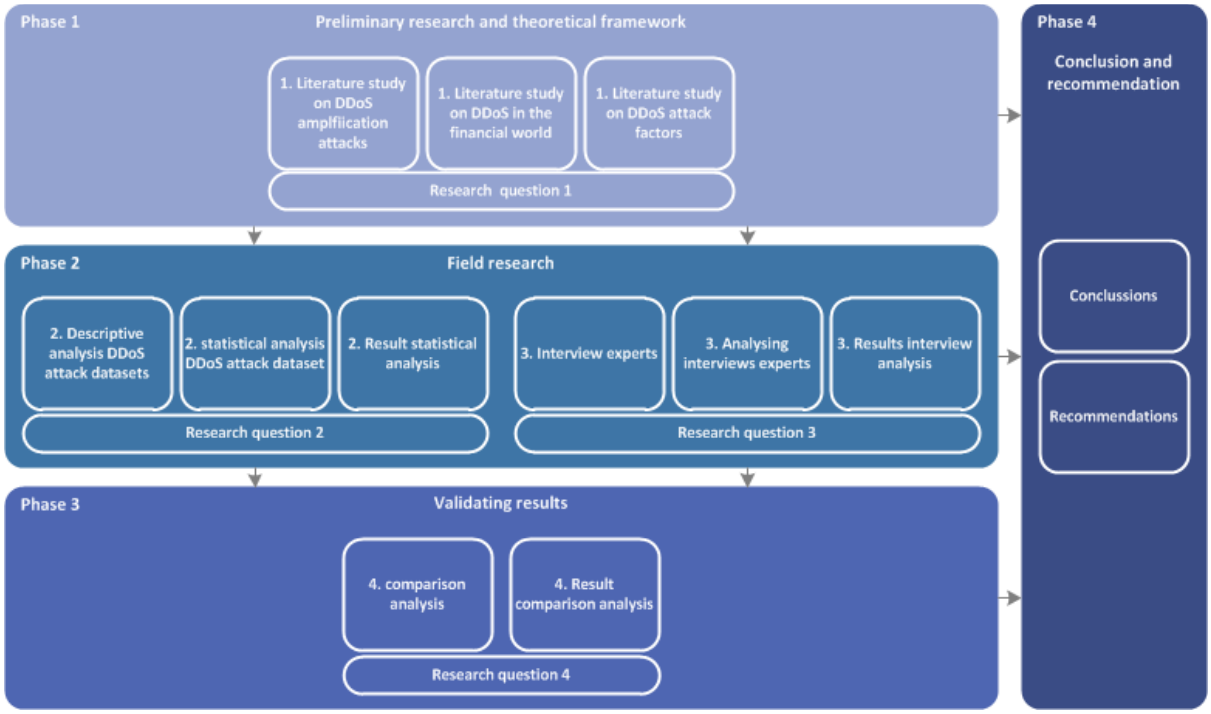

Figure 2: Research design and framework

1.7 Scientific, practical, and societal relevance

From a scientific perspective, this research contributes to scientific knowledge of cyber security. In the current literature, there is little research on target selection of various cyber-attacks. Target selection via booters using amplification techniques is therefore even more limited. This research adds to a limited field of researches that focuses on target selection specifically focused on financial institutions. This insight will provide empirical evidence for a set of factors that are directly related to target selection of financial services, and could thus explain the differences in which financial institutions are being targeted. Moreover, opinions of experts in mainly the Dutch financial sector will provide insights into the perceived threat of DDoS and how well this is managed in practice.

From a more practical view, the results of this research can provide a better understanding of the target selection of booters on FSOs. With knowledge gained from the research, a defender (e.g. EY) or a victim (bank) can respond accordingly with their currently available services, or develop new services if there is a gap with market demand.

Due to booters everybody can be an attacker, and the chance of being attacked is increasing. It is thus important to know what the impact and effects of booters are on the society as a whole and how they can affect financial institutions. As booters are increasing in numbers, the cyber threat landscape, governments, studies and businesses need to understand, the risks of cyber activities, in order to mitigate them. For governments this may imply educating people about

the risks. For business this means mitigating new threats, and for science this means understanding new cyber concepts.

1.8 Scope of the research

To understand the scope of the research, the parameters that define the borders of the research space need to be understood. This research will be conducted, commissioned by the TU Delft and EY IT Risk and Assurance for financial services. Therefore, the first border of this research will be the financial services industry, as this follows from the service line of EY. To conduct the quantitative analysis, the AmpPot honeypot dataset will be used. This dataset can be seen as the second border of this research. This dataset contains entries of attacked IP addresses across the world that was gathered using a set of honeypots. Hence, the third border is the location, which will be internationally. Since the AmpPot dataset do not distinguish an attack by organisation, financial services need to be extracted from the datasets to comply with the first border. While the AmpPot data will be internationally oriented, the experts' opinion will be less internationally oriented. Due to time and travel constrictions, the interviews necessary for the qualitative analyses will mostly be held in the Netherlands and with Dutch experts. The final border will be that of time. The AmpPot data contains attacks from the 2014 till 2015. Therefore most of this research will be utilised from that time frame.

For the purpose of this research, the various concepts used will be defined hereafter. Noroozian et al. (2016) have defined an attack as a series of at least 100 consecutive query packets that a single host send to an AmpPot, where consecutive means that there was no gap of more than 600 seconds between two packets. The same definition will be used in this research. Victim is defined as the entity (or entities) that the attacker intended to affect. This may be a person, organization, service, or machine (Noroozian et al., 2016). As this research is focused on FSOs, the target for the financial data is a financial institution. Since the data consists of IP addresses, and the attackers intention is not observable, the term target is used and refers to the IP addresses.

Table 1: Definitions

Term	Definition
Attack	*Series of at least 100 consecutive query packets that a single host send to an AmpPot*
Booter	*A website by means it is possible to deliberately launch a DDoS attack in exchange for a monetary value.*
Cybercrime	*Any crime that is facilitated or committed using a computer, network, or hardware device.*
Target	*The targeted IP addresses of a DDoS attack*
Target selection	*The attack choices by the cyber criminal regarding which institutions to attack.*
FSO	*All organisations that operate and provide services in the financial sectors of wealth and asset management, banking & capital markets, and insurance.*
Victim	*The entity (or entities) that the attacker intended to affect. This may be a person, organization, service or machine* (Noroozian et al., 2016)*. In the case of the financial data, a victim will be the IP address and the associated financial organisation.*

2. Research approach and methodology

This section will give an explanation of the research approach and methodology. First the approach, which provides the framework of the research, will be discussed. Second the theory used to define target selection will be mentioned. In addition, there are certain challenges in gathering the data. The third section provides insight into the processing of the quantitative and qualitative data. Lastly, the limitations of the research approach and the data will be discussed.

2.1 Mixed method approach

Due to the nature of this research, involving numerous datasets, a multi method research approach will be used. More specifically, the research mixes qualitative and quantitative data, methods, methodologies, and thus a mixed method research will be the main approach used. As data will mainly be gathered from the quantitative data, a quantitative driven approach/design will be used. The quantitative data will be supplemented by qualitative data to improve the quantitative study by providing an added value and deeper, wider, and fuller answer to the research question.

While this approach seems logical in a sense that quantitative data has already been gathered, a mixed method approach is not inevitably per se the best approach. However, this method seems useful in a sense that this research emphasizes both the technical and socio-technical characteristics that influence target selection of amplification attacks. Adding the qualitative data to the quantitative data can add enormous potential for generating new ways of understanding the complexities and context of social experience (e.g. cyber threat) and for enhancing the capacities for social explanation and generalisation (Mason, 2006). A mixed method approach will lead to a more multi-dimensional approach that will improve the understanding of what influence target selection.

2.2 Quantitative research

For the quantitative analysis, the AmpPot data will be used as input. The main dataset for this research will consist of a small part of the total AmpPot data as mainly on financial organisations will be the focus. In order to analyse the data, the modelling language R will be used. This language is especially useful for analysing large datasets. To get acquainted with the data, and find initial patterns, a descriptive analysis will be done. The second part of the quantitative analysis will be an explanatory analysis on the results of the descriptive analysis. For the explanatory analysis, various statistical analyses (e.g. (generalized) linear regression) will be used to understand the relation between identified factors and the target selection of DDoS amplification attacks.

2.3 Honeypot data: AmpPot

The fundamental data for this research is provided by the AmpPot data (an example of the data can be found in Appendix C). This dataset will be mainly used for the quantitative analyses part. AmpPot provides data about 5.721.432 IP addresses, captured over the two years (2014-2015) via amplifier-honeypots or AmpPots. This data was gathered and researched by Kramer et al. (2015). Kramer et al. focused their research on exploring attackers preparing and launching amplification DDoS attacks in the wild. This research has focused on the victimization of various victims in general. This dataset contains, among others, the following variables: target IP, date, sensor ID, service, start/stop time of attacks, duration, and the autonomous system numbers of entities routing traffic from the attacked IPs.

2.4 Extracting the financial data form AmpPot

As AmpPot does not map the attacks on organisations level, these financial organisation data existing in the data needs to be retrieved manually. Throughout this section, the process of

extracting the financial data from the AmpPot will be discussed. The goal of this section is to ensure the validity of the extracted data and to counter limitations as mentioned in section 2.7.

In order to map the financial organisations, the first step was to match the targeted IPs to the associated organisations. To do so, an additional database by MaxMind was used. This database contained a list of organisations and their IPs given a certain time frame. As the domain names and thus their associated IP can vary over time, it is important to find the right organisation during the time of attack. Therefore, a GeoIP look-up IP was used to match an organisation in the MaxMind database to the targeted IP in the AmpPot database. This researched used the toolkit Pandas to assign he organisations to the targeted IP (see Appendix D). Pandas is a toolkit based on the programming language Python, and specifically designed for analysing large datasets.

The next step involved the search procedure to map all the financial organisations found in the total AmpPot data, and export them to a single dataset. This procedure was based on a set of keywords that filtered all the financial data via a Python script. The keywords used for the search query were developed in two ways; the first approach was via personal conversations with employees from the IT Risk Assurance for FSO department of the EY accounting firm. During these personal conversations, various FSOs were identified as well as a set of universal keywords that are often used by financial services in their names (e.g. investment). The second approach consisted of using various Internet sources such as Fortune500, Gartner and Forbes, to find additional keywords. An extensive list of the keywords is presented in Appendix A. The universal keywords consist of non-specific words that do not relate to a single organisation, while the more specific keywords (organisation keywords) are used to find specific organisations. To cope with the international nature of the dataset, the universal keywords were translated to various languages (e.g. English, Spanish, and French). Keywords in non-western languages (Chinese & Arabic) were not used. The reason for this is that these keywords had an English counterpart. It is important to note that the search script used for mapping the financial data was case insensitive, thus no additional keywords had to be developed in order to catch different capitalisations.

The extracting resulted in a far smaller datasets consisting of organisations with names matching to the keywords. However, naturally, several of these cases were falls positives due to one of the keywords being related to a non-financial organisation name. In addition, also duplicated cases were found due to multiple keywords existing in one organisation name, such as “financial bank”. To correct for these issues, duplicated and non-financial related attack cases were deleted using queries in RStudio. An example in that regard was the organisation “Softbank” (a software company), which was largely represented in the extracted data. The final result being a financial dataset consisting of 10795 cases on which financial organisations have been attacked. These cases build the basis for the data analysis in section 5. Important to mention is that these are cases and not organisations, as an organisation can be attacked multiple times. Note that the extraction of the financial data and deleting of non-financial data in the financial data was done by hand. Therefore, financial related cases could have been missed out during the extracting, as well as, non-financial cases could still be present in the financial data.

In order to validate the dataset, and understand how well this data represents the financial market, the extracted financial dataset is contrasted to a MaxMind dataset that contains a list of all organisations found in 2015. To do so, this research uses the same keywords to find financial organisations in the MaxMind data. In addition, the keywords are also used in an established list of FSOs that was composed by the US Internal Revenue Service (IRS). This list contains 288,128 entries related to FSOs. The results provide an overview of how well the keywords can map the financial sector. For more information on the results of the proportions and crosschecking, refer to section 5.1.

2.5 Qualitative research

In addition to the datasets provided by the TU Delft, also qualitative data will be used. This data will be gathered from various interviews with cyber security experts. While the data provided by the TU Delft provide an overview of the attack side of the DDoS attacks, the interview give a more detailed overview of the victim side. In contrast to the previous datasets, the data needed for the qualitative analysis need to be gathered using interviews. Due to time constraints, 9 experts were consulted.

2.6 Comparing the results of the quantitative and qualitative research

After thorough analysis, both the results of the quantitative and qualitative data are being compared. In this regard, several limitations of the mixed method have to be taken into account. Not all quantitative and qualitative results can be used together. This has to do with the scoping of the studies. While the quantitative dataset is purely focused on the technical characteristics of DDoS attacks, the qualitative data will be more focused on the victim side and the socio-technical factors. In addition, issues regarding interpreting conflicting results will need to be taken into account as well.

2.7 Drawbacks and constraint on research methods

Limitations of the mixed method approach

Although this approach seems useful and logical for the research, the mixed method approach has its own limitations. These limitations have to be considered when conducting this methodology. A clear limitation is that not all quantitative and qualitative results can be used together. In addition, cultural and monetary issues affect the view of experts, and thus results in biased responses. In addition, a mixed method approach is a very time consuming process since multiple methods and approaches need to be applied to mix both types of datasets correctly. Furthermore, it might be difficult to interpret conflicting results (Johnson Onwuegbuzie AJ, 2004).

Data limitation

As mentioned in the previous section, there the data used for this research is not without limitations. However, it is important to understand the implications of these limitations as the data forms the basis for this research. The limitations can be separated into limitations of the quantitative analysis (AmpPot data) and the limitations of the qualitative data (experts' opinion).

The limitations for the AmpPot data can be categorised in two groups: AmpPot limitations and data extraction limitations. The AmpPot limitations are associated with the information that can be gathered from the AmpPot data. The major issue is that the data utilized for this research is not based on primary research but rather a secondary research method. The data was not gathered to analyse on organisational level but more on an infrastructural level. Thus, adding new variables to the data is inevitable to stay within boundaries of the research scope. Also, as the data is dated from 2014 to 2015, meaning that there is a scope difference between the quantitative and qualitative analyses. This issue is limited as much as possible through focussing on the total DDoS landscape of an organisation, and not solely the last couple years. Furthermore, as mentioned in the previous section, issues arise when extracting the financial data from the AmpPot data. The AmpPot data does not provide classifications based on the type of organisation. Therefore, there is no other way than using keywords to manually extract the financial data. The biggest issue here is that cases could be lacking from the financial dataset due to unknown financial keywords, language barriers, or organisation that have non-financial related names. To counteract this limitation, multiple sources were consulted to find financial organisations and reduce this limitation as much as possible (see section 2.4).

Likewise, the qualitative analysis is not without limitations. The limitations for data used in the qualitative analysis can also be categorised into two groups: data gathering limitations, data interpretation limitations. In order to retrieve the necessary data, experts have to be interviewed. However, due to boundaries within the researchers' personal environment and travel boundaries, mainly Dutch experts could be interviewed. To countermeasure this limitation, experts from different countries have tried to be reached and interviewed with the help of Skype. In addition, due to the reputation of the respondents and the physical presence of the researcher during data gathering, it is unavoidable that responses can be affected and thus a more subjective response will be given. To limit this as much as possible, the data is anonymised throughout the research. Interpretation limitations are associated with the interpretation of the responses from the researchers' side. Due to bias of the researcher and it is unavoidable that responses can be interpreted differently than was intended by the respondent. To countermeasure this limitation, a summary of the gathered data from each respondent will be send after the interview by e-mail to validate the data.

2.8 Purpose and research guide

This research intends to contribute to the understanding of victimization and target selection of DDoS attacks on organisations on a global scale. In particular DDoS attacks services (DDoS-as-a-service) using amplification techniques that attack FSOs. To meet the purpose of this research, empirical data analyses are done using various datasets gathered from quantitative and qualitative studies. In the current literature, there is little knowledge on the factors that influence DDoS amplification attacks in the financial sector, the reason behind those attacks, and on the effects of such a cyber-attack. Hence, this research aims at identifying factors that influence the target selection of DDoS amplification attacks. Understanding these factors can help in understanding why certain organisations are being attacked more often then others, and in what way these attack rates can be reduced or mitigated.

2.9 Research guide

To apply the mixed method approach, this research is divided into four parts that are (Figure 3): The problem statement; literature study; quantitative, qualitative data analysis, and comparison of the data analyses; and finally the conclusion.

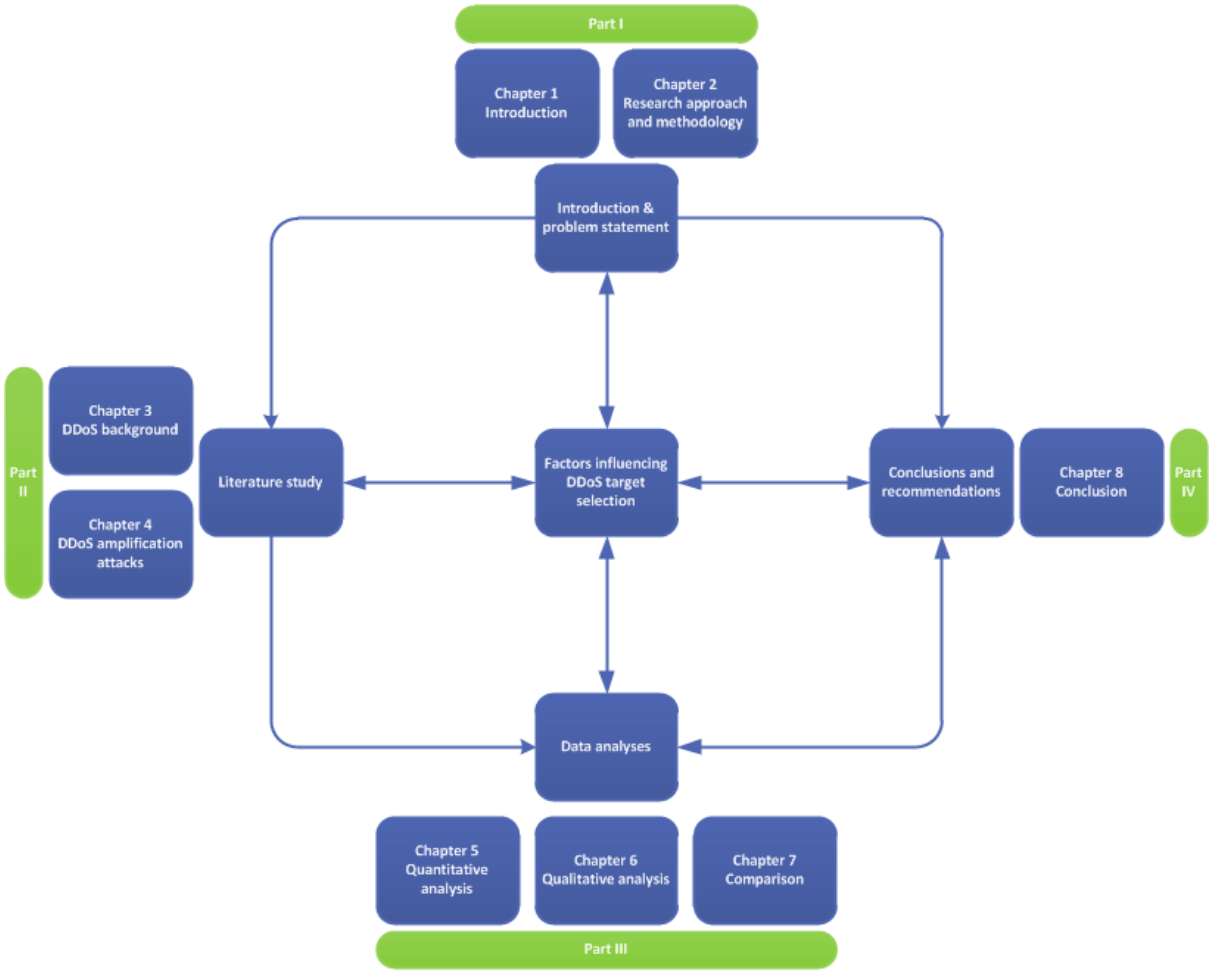

Figure 3: Research guide

2.10 Thesis outline

Part I

The first part of this thesis will elaborate on the introduction, problem statement. It will gave a basic insight into the topic of this research and identifies the issues regarding DDoS. Furthermore, this part notes the research objective, knowledge gaps, research questions and the research approach.

Part II

The second part provides general literature study on DDoS attacks. This part will give basic insights into the DDoS topic as a whole to have a better general understanding, as well as an understanding of its relation with financial organisations. Furthermore, this part provides a more in-depth understanding of DDoS amplification attacks. Throughout this part, the first research question will be answered through literature study and desk research.

Part III

The third part is the core of this research and will focus entirely on the data analysis. Section 5 will describe the data analysis according to the AmpPot dataset. In this part the quantitative data is analysed to determine which factors influence target selection of DDoS amplification techniques, thus answering the second research question. The findings of this analysis will be partially used as input for the next section.

Section 6 will continue on the factors found of the previous section, but from the perspective of experts in the financial and/or cyber security field. It uses the factors identified in the previous

section as a baseline for further research. This allows for new insights into target selection of DDoS attacks. The results provided by this section will allow for answering the third research question

Section 7 will bring the previous findings together and shapes the last section of the data analysis. This section will compare the results of the previous analysis, and note the differences are between the quantitative data and the qualitative data and how they can complement each other. This section provides answers to the last research question.

Part IV

Part IV will compose of the conclusion of the thesis. As such, the results of the research questions and main question will be answered through the results found during the thesis as well as recommendations for both financial organisations as recommendations in general. Furthermore, this section will elaborate on suggestion for future research

PART II: Literature study

3. The background

Understanding Cybercrime is central to understanding the threats that current financial organizations face. The term "cybercrime" has been defined in numerous ways by differing opinions of researchers around the globe. A primary problem is therefore the absence of a consistent global definition (Yar, 2005). In the following section, an attempt is made to comprehend a few of them.

Nagurney uses the definition given by Petee et al. (2010). They state that cybercrime is "any criminal offense that is committed or facilitated through the use of the communication capabilities of computers and computer systems". Raghavan & partihban (2014) and Yar (2005) use a definition by Thomas and Loader (Thomas & Loader, 2000) who define cybercrime as "computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties". Bougaardt & Kyobe (2011) define cybercrime as criminal activities involving the use of electronic devices and may lead to incidents such as theft of information; Sabotage of data of networks; loss of information due to eavesdropping; financial fraud; denied access to information; and damage due to virus attacks. Brenner (2007) uses a more generic approach that encompasses both traditional and emerging cybercrimes. It also encompasses any use of computer technology, not merely the use of networked computer technology. She defines cybercrime as: "To engage in activity that threatens a society's ability to maintain internal order". These definitions all define cybercrime as criminal activities through a computer or computer network. Therefore the overarching definition by Gordon & Ford (2006) will be used. They define Cybercrime as: "any crime that is facilitated or committed using a computer, network, or hardware device".

While there has not been a definitive list of what cybercrime constitutes, there has been consensus on what falls within the scope of the offences that occur in cyberspace (Broadhurst & Choo, 2009). A list of the different fields of cybercrime has been shown below:

- Telecommunications Theft & Illegal Interception
- Piracy Copyright Theft
- Cyber Stalking
- Electronic money laundering and Tax evasion
- Electronic Vandalism, Cyber-Terrorism, Denial of Service, Extortion
- Sales and Investment Fraud, Forgery (Classic Pyramid schemes)
- Electronic Funds Transfer Fraud and Counterfeiting (Carding, Identity Theft and Misrepresentation)
- Content Crime - Offensive Materials
- Espionage
- Resource Theft - illegal use of personal computers (PCs) or other digital devices

3.1 Consequences of cybercrime

Cyberspace has provided criminals a safe haven in developing countries that enhances their organisational and operational capabilities, because information security and associated laws and policies are less developed in emerging economies. As a result, criminal activities can be conducted at lower risk but still have the potential of impacting advanced economies (Broadhurst & Choo, 2009). As has been seen in the past, the consequences of cybercrime have been huge and are increasing every day. According to Forbes, the British insurance company Lloyd's estimated that cyber-attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business (Morgan, 2016). It is estimated by Juniper that the cybercrime costs will even increase further. Due to rapid digitization of consumer's lives and enterprise records, the costs of data breaches will increase to $2.1 trillion by 2019 globally, increasing almost four times the estimated cybercrime

costs in 2015. As Armin et al. (2015) mentions, there is no lack of reporting of the cost of cybercrime, these reports make the headlines on a regular basis. However, these consequences are currently still hard to quantify when the costs are inspected on a closer level. Therefore, the estimated costs of cybercrime is highly contested (Armin et al., 2015). There are various studies that investigated the consequences of cybercrime. From a financial perspective, Anderson et al. (2012) states that the economic cost of cybercrime can be separated into four categories:

Criminal revenue: gross receipts from a crime.
Direct losses: losses, damage, or other suffering felt by the victim as a consequence of a cybercrime.
Indirect losses: losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out.
Defence costs: cost of prevention effort.

The economic and financial losses incurred by the victim organizations directly depend on how well the organisation has adapted cyber security into their organisational and operational activities. The over-spending on defence measures and chronic under-reporting can drive up the cost of cybercrime, while under spending or not investing in defence costs can increase the direct and indirect losses and thus the overall cost of cybercrime significantly when attacked (Lagazio, Sherif, & Cushman, 2014).

However, not all consequences of cybercrimes can be fully understood and assessed from an economic perspective. For instance, in ideological cyber-attacks, revenge and other crimes of passion, the economic considerations are less prominent (Lagazio et al., 2014). In this regard, both tangible (financial losses and cost) and more intangible drivers (trust, loyalty, and society utility) of cost are important and sizeable consequences of cybercrime. These intangible drivers and their consequences cannot be ignored, but make it hard to assess the consequences of cybercrime due to their abstract nature.

3.2 Cybercrime and FSOs

The consequences of cybercrime mentioned in the previous section can be generalised and understood for many organisations in all different sectors. However, not all industries and economic sectors are affected equally by cybercrime. According to the PriceWaterhouseCoopers 2014 Global Economic Crime Survey (PWC, 2014), 39% of financial sector respondents said they had been victims of cybercrime, compared with only 17% in other industries, with cybercrime now the second most commonly reported economic crime affecting financial services firms. Wilson (2013) noted “every minute, of every hour, of every day, a major financial institution is under attack”. The financial sector has witnessed various forms of cybercrimes with different impacts like ATM frauds, Phishing, identity theft, and Denial of Service.

Crime and organisations in the financial sector have been together since the beginning. While this ‘marriage’ of crime and FSOs has not changed, the landscape in which this occurs has. Until the mid-1990s, the financial sector was relatively simple and reliable (Raghavan & Parthiban, 2014). To reach more customers, organisations have shifted to more technology advanced services. Logically, the landscape in which criminals operate has also shifted to the technology landscape. By relying on the Internet for their services, FSOs have opened up their technical infrastructures to more risks.

While there have been numerous studies and implementations to reduce the risks for FSOs, the forecast is that cybercrime will only increase in the upcoming years (EY, 2014; Nagurney, 2015). The increase in cybercrime is a real threat for FSOs. The business continuity of FSOs is highly dependent on user-trust (Verschuur, 2012), and with the recent development to provide more services online (e.g. online banking and wireless transactions), new developments in the

cyber security sector have to be followed up closely. Among the various sectors, FSOs are among the top 3 sectors that are being attacked most often by cybercriminals (see Figure 4).

As this thesis will focus on the DDoS attacks targeting FSOs, other cybercrime mentioned in the beginning of this section will be discarded. The trend surrounding the increase of DDoS attacks is similar to all the trends relating to cybercrime for FSOs. Financial services share the second place of being mostly targeted by cybercriminals in terms of DDoS (see Figure 4). In 2014, financial services held the fifth place, and thus has moved up into a three-way tie for second place with government and hosting (Arbor Networks, 2015b). Among the demand for DDoS services, FSOs score the highest (see Figure 5) with government and cloud/hosting providers as second and third place respectively. This concludes that FSOs are still investing a lot in anti-DDoS protection services.

In the figures below, the targeted sectors are shown.

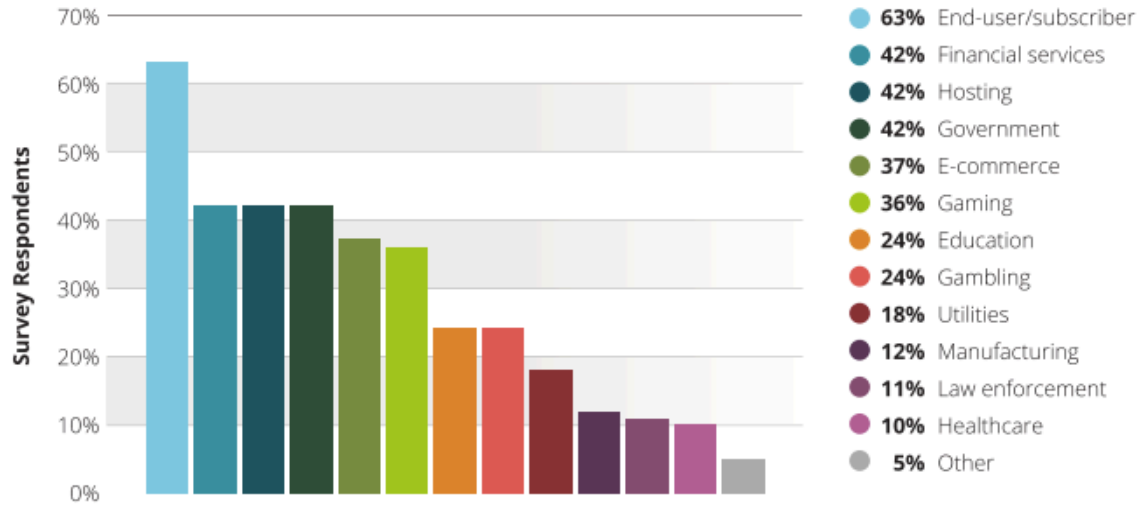

Figure 4: Attack target Customer Vertical (adapted from Arbor Networks (2015b))

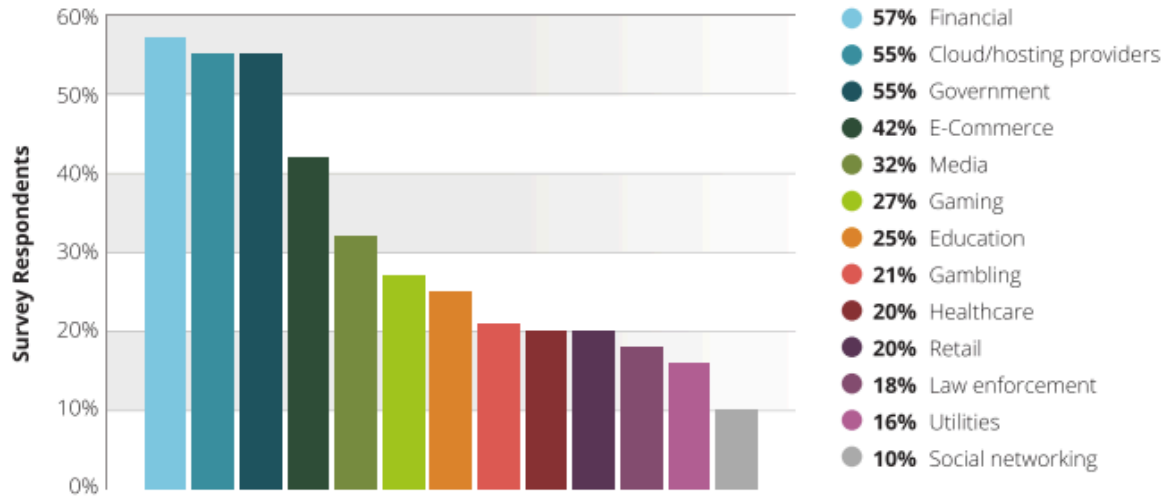

Figure 5: Business Verticals for DDoS Services (adapted from Arbor Networks (2015b))

3.3 What is DDoS?

To understand the DDoS landscape, it is first essential to understand the basic properties and categories of DDoS attacks. A DDoS attack, also known by its full name 'distributed-denial-of-service' attack is a large scale, coordinated attack generated by using multiple machines on the availability of services on a victims' system or network resources (Holl, 2015; Hoque, Bhattacharyya, & Kalita, 2015). The services that are being attacked are the services of the

victim, which is also known as the 'primary victim'. The compromised machines that are used for the launch of a DDoS attack are known as the 'secondary victim'. The secondary victims are (mis)used to wage a larger and more disruptive attack, while also ensuring that the primary victim cannot trace back the origin of the attack.

To understand the more fundamental and different types of DDoS one has to understand the different layers in data communication. The different layers are best described using the Open Systems Interconnection model (OSI model), developed by ISO. The OSI model is a theoretical model for network communication to have better interoperability between various network systems. Since the introduction of the OSI model, it is the most used model for standard protocols for communication systems. Due to their direct connection to network protocols, the model gives a clear overview of the various targeted layers for DDoS attacks. The model consists of 7 layers, which can be categorized into two types, application layers and infrastructure layers (see left-hand side of Figure 6). The Application layer takes care of the operating system or the application in use, while the infrastructure layer takes care of all things needed to support the application layer (Zimmermann, 1980).

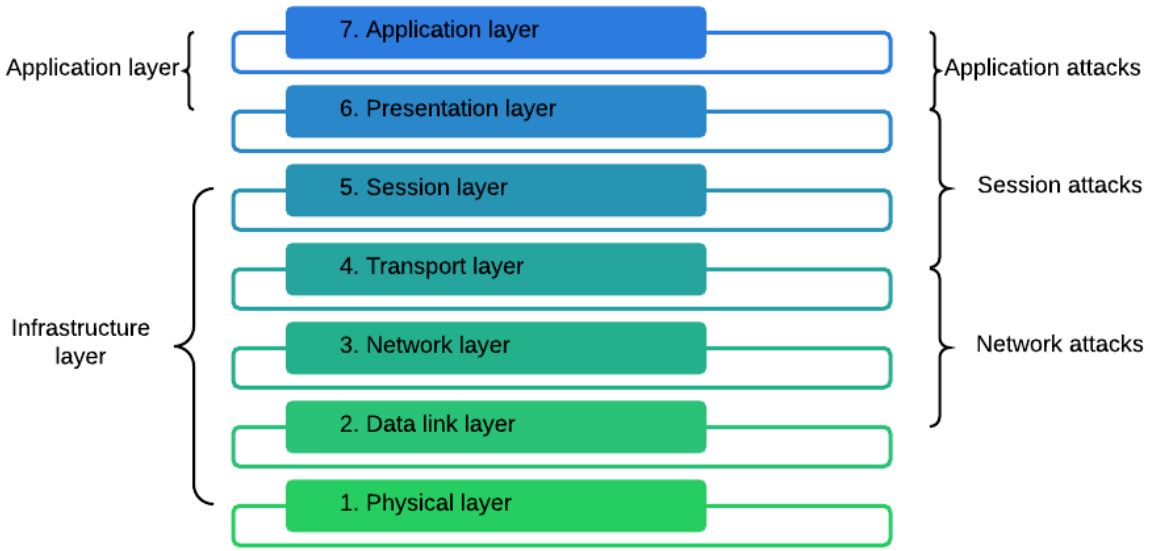

Figure 6: 7 Layers of OSI model

Physical layer - The physical layer describes how bits of data that are sent and received are moved along the network. For example which cable and bandwidth are used.
Data link layer - The data link layer provides the functionalities that are needed to securely send data over between devices. IT uses MAC addresses of hardware devices to send the data to the right receiver.
Network layer - The network layer performs the routing, flow control and error processing. Routers use Internet Protocol (IP) addresses to handle the traffic between various networks. Therefore the important protocol used in this layer is the IP.
Transport layer - The transport layer handles all the end-to-end issues of the transportation of the data. This layer provides standards to ensure that software (e.g. in the application layer) do not have to account for the correctness and timing of the data transmission. The most important protocol in this layer is the Transfer Control Protocol (TCP).
Session layer - While the third and fourth layers are concerning the packages, this layer is the first layer that is dealing with the software the network is using. This layer allows, maintains, and disables sessions between programs.
Presentation layer - The presentation layer is used as the translation of the data. This formatting is necessary for the receiving system to understand the data that was being send.

Application layer - The application layer is the layer that is being used by network programs. Therefore, this layer is the highest layer and closest to the human interaction of the model. Examples are Internet browsers or e-mail programs. This is the layer in which the applications request for and receive data.

On the right hand side the possible DDoS attacks on the various layers are shown. Attacks on the application, which are the minority of the DDoS attacks, are focused on targeting the weaknesses and exhausting resources of applications (more detail below). On infrastructural level, DDoS occurs on the 3rd (network) and 4th (transport) layer of the OSI model. Infrastructure attacks consist for the majority of the total DDoS attacks, circa 83% of the total attacks (Arbor Networks, 2015b). One of the reasons that these attacks occur more often is that amplification DDoS attacks now make up a considerable fraction of network-layer DDoS incidents (Arbor Networks, 2015b). Attackers send a request to amplifiers (or reflectors) and spoof the source IP address, so that that the amplifiers responses are directed to the victim. There are a whole range of protocols that can be abused for amplifications in addition to the millions of machines that run these protocols (Rossow, 2014). A detailed description of DDoS amplification attacks will be given in section 4.

3.4 DDoS Attack motivation

Even though any individual or organisation can be target of a DDoS attack, the attackers often have a specific motivation such as extortion of money or disruption of the operations of organisations. Understanding the motivation of attackers is important to establish effective methods of mitigating the impact of DDoS attacks. The attackers motivation can be categorized into five main categories (Zargar et al., 2013):

Financial/economical gain - These attacks are the most eminent threat for organisations. The attackers with these motives are, due to the nature of these attacks, usually the most technical and most experienced attackers. These attacks are often the most dangerous and difficult to stop.
Revenge - These attackers are often frustrated individuals, which have a dispute with the target, and have often less technical skills. Such an attack is often carried out in response to a perceived injustice.
Ideological belief/hacktivism - Attackers with this incentive have a belief and hope to achieve that believe with a DDoS attack. This motivation is currently an important incentive for attackers to launch a DDoS attack.
Intellectual challenge - These attackers launch an attack in order to experiment and learn how to launch an attack. The attackers are often enthusiastic young individuals that want to show off their skills. Nowadays also less skilled individuals can launch an attack, thus high capabilities are not necessary anymore.
Cyberwarfare - Attackers with this incentive often have a political motivation. These attackers often belong to the military or terrorist organisations of a country. The potential targets of these attackers can vary to all targets that will harm a country. These attackers can be considered as highly skilled and sophisticated individuals with advanced resources. The impact of a cyber-attack

Historically, “ideological hacktivism” has been the top motivations. The report by Arbor Network from 2015 has shown that “demonstrating DDoS capabilities” is the top motivation for criminals, followed by “gaming” and “criminal extortion attempts” (see Figure 7). The reason for rise of “criminals demonstrating their capabilities” can possibly be explained by the ease in which DDoS attacks can be produced and carried out for any and all reasons. In addition, the growth of booters is a growing problem.

In 2015 the demographics of motivations for a DDoS attack have shifted. Online gaming is seen as the leading motivation, while "ideological hacktivism" has receded to the second place, and "criminals demonstrating attack capabilities" has alleviated to the third place (see Figure 8). Criminals demonstrating attack capabilities is indicative for the armature of DDoS attacks through easy-to-obtain services. The availability of booter/stresser services remains a growing problem in the DDoS landscape. DDoS extortion attempts round out the fifth place, making it still significant for various organisations (Arbor Networks, 2016).

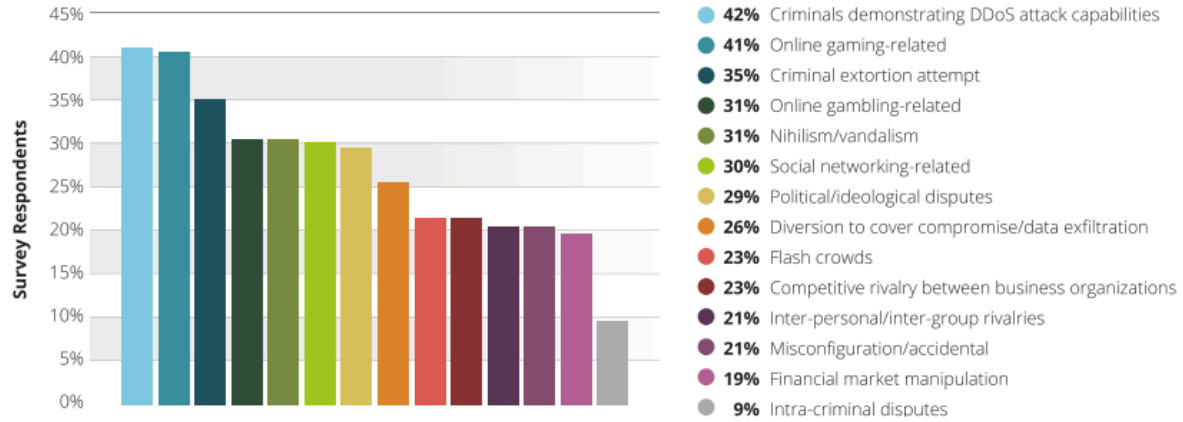

Figure 7: DDoS attack motivations 2015 (adapted from Arbor Networks (2015b))

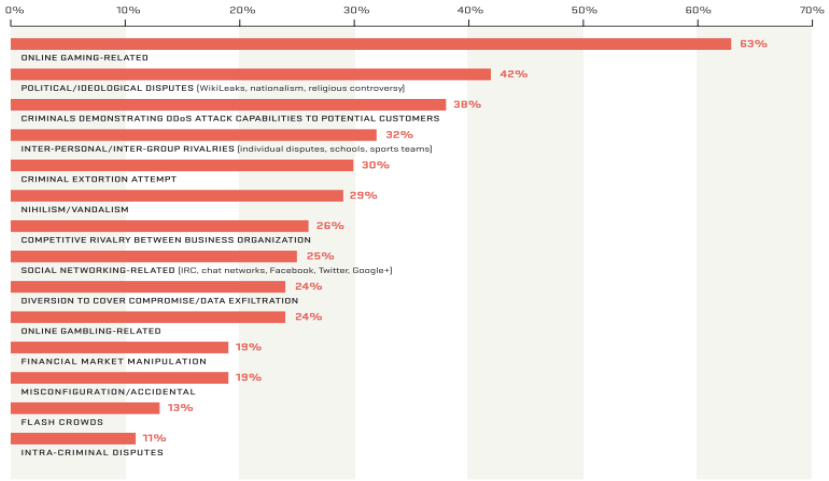

Figure 8: DDoS attack motivations 2016 (adapted from Arbor Networks (2016))

3.5 Commoditisation of DDoS

With the current technological improvement and new methods of DDoS attacks, the threat landscape is expanding. Even though DDoS attacks have been around for many years, DDoS attacks have become a commoditized service. There seems to be a disproportionate increase in attacks on the infrastructure layer. In these layers, DNS amplification accounts for 60% of all the attacks. For layer 4, SYN flood attacks, seems to be especially popular (Czyz et al., 2014; Krämer et al., 2015). This increase can be related to the overall increase of the usage of amplification attack methodology (Czyz et al., 2014; Krämer et al., 2015). As this methodology uses spoofed IP addresses to forward traffic to victims, it is hard to trace back the actual attacker. As the attack does not need a large infrastructure to launch a relatively large attack, and DNS (amplifiers) can easily be abused without the need to hack the system, these attacks are extremely popular. When using a botnet, the attack can even be increased further. Due to the efficiency, relatively low cost, scalability, building a powerful infrastructure is rather simple. Adding the low chance of getting caught, these attacks are the perfect choice for criminals.

Karami and Mccoy (2015) argue that a large number of DDoS attacks are generally orchestrated by highly unsophisticated attackers. This shift is related to the rise of a various services operated by profit-motivated adversaries, namely, the rise of DDoS-as-a-service or booters (Karami, 2016). These services provide platforms that make it possible to launch an attack with the press of a button. The customer may choose from a wide variety of packages or even custom-tailored attacks. Traditionally, DDoS attacks were solely coming from botmasters, which were the controllers of a collection of computers that were infected by malware, also called a botnet. Maintaining a botnet was rather time intensive, risky and technical endeavour. However, these days the services of botnets are put up for rent and are even traded among attackers. These commercial entities are trading in huge numbers of infected computers. These websites provide richly featured toolkits and even distributed networks to execute attacks whenever the attacker wants. The amounts of booters as well as their firepower are rapidly increasing, which makes them a threat for the cyber realm (Karami et al., 2015) . The adversaries operating the booters have control over a large number of compromised hosts and have made the DDoS infrastructure conveniently accessible for a majority of potential attackers for minimal costs. Customers usually pay for the attack type or combination of different protocols, the bandwidth and duration of the attack (Imperva, 2016). Payment often occurs using PayPal or cryptocurrencies such as Bitcoin (BTC). Nowadays it is also possible to use different payment methods such as Paysafecard, which is similar to PayPal. Cryptocurrencies provides a sense of privacy, protecting both the service provider and the customer. This has contributed to the increase of DDoS attacks in recent years (Karami, 2016). Taking those services down is hard since they often hide behind the ambiguous but legal definitions of 'stressers' or 'booters'. In addition, due to know-how of the adversaries the C&C servers along with the abused systems (often called amplifiers) are concealed and hard to trace. In addition, the ISPs hosting the booter websites are often unaware of the illegal activities going on their network.

3.6 How booters work

The traditional and more technical way of launching a DDoS attack consisted of four steps: write virus that will send ping packets to a target network or website; Infect as many systems as possible to make them into a zombie; Launch an attack by waking up the zombies/abused systems; Attack the targeted system using the zombies, abused systems until the network is disinfected. However, booters have made it possible to skip the first two steps (most technical) to only launching an attack at '*the press of a button'*. Thereby increasing the capacities of low-technical individuals to launch attacks.

Research demonstrates numerous ways of defining booters. Karami and McCoy (2015) refers to booters as low-cost DDoS-as-a-service phenomenon. Michael Krebs (2016a), an acknowledged cyber security journalist, refers to booters as services hired to knock websites and individual users offline. A leading security company Akamai (Akamai, 2014), refers to booters as part of the DDoS-for-hire market allowing low-level, non-technical actors to threaten organisations. The main message of all these definitions is that DDoS services are nowadays widely available. An schematically representation of how booters work is given below (see Figure 9).

First the attacker subscribes to a booter (1). Using PayPal or Bitcoin, the attacker can subscribe to various services offered by the booter service (2). The attack then uses the front-face of the website to set specification for the attack and launch the attack. The request is send to the concealed back-end servers (4). The back-end server sends spoofed requests packets to a set of pre-identified amplification servers (5). As the source (IP address) of the request is spoofed (victim's IP address) the amplifiers send their request to the victim, which increases the traffic towards the victim resulting in an overload (6).

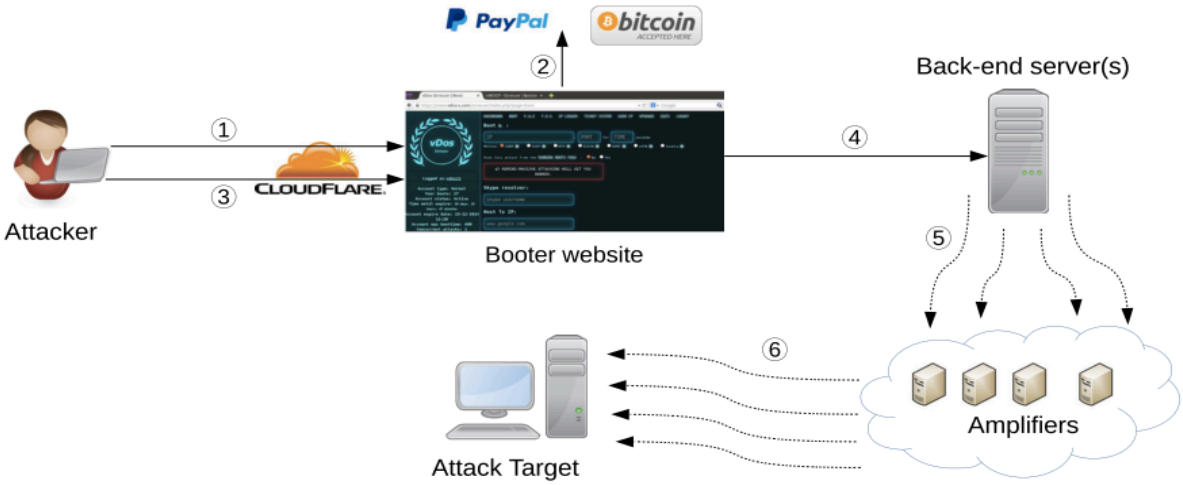

Figure 9: Structure of a booter using amplification DDoS (adapted from Karami et al. (2015))

As there are various DDoS types, booters also have a wide range of attack types. In general, booters offer two categories of attacks, which target three layers of the OSI model (Kuhrer, Hupperich, Rossow, & Holz, 2014). First, there are the types that attack the 3rd (network) and 4th (transport) layer of the OSI model. These attacks overload the network resources by overflowing the bandwidth of a link, or target a specific host by exhausting resources of the specific host. Second, 6th and 7th layer (application) attacks target a specific application on the victim system. These types of attacks are performed through exhausting the resources of solely the application, meaning that all the other applications on the victim's system are still operational.

To deliver their ordered services, booters use volumetric amplification attacks. This is due to the fact that amplification attacks are very effective, Using amplifiers an attack can increase its request up to 556,9 times (Rossow, 2014). Currently the attack intensity of DDoS has been increasing. However, the characteristics of malicious traffic generated by such an attack is basically the same if the attack is launched by a booter service or not. Therefore this research will focus on amplification attacks in general and not particular amplification attacks launched by booter services.

4. DDoS amplification attacks

In section 3.1, the overall consequences of DDoS attacks have been covered as well as a short description of DDoS amplification has been given. This section will provide a more in depth analysis of DDoS amplification attacks. Firstly this section will discuss how DDoS amplification works. Secondly the risks and consequences of DDoS amplification attacks for FSOs will be discussed. Thirdly, the factors that influence target selection according to the literature will be elaborated. Lastly, the proportion of the FSO will be discussed in this section.

4.1 How does DDoS amplification works?

DDoS amplification attacks are DDoS attacks by using an extra level that amplifies the initial traffic. In order to amplify an attack, open Internet servers are used. Often used Internet services are DNS servers or NTP servers. To amplify the attack, traffic is send to an amplifier or reflector. By spoofing the IP address of the traffic, the response (amplified traffic) is send to the spoofed IP address, or the IP address of the target (Krupp, Backes, & Rossow, 2016). In a more comprehensive way, amplification attacks are attacks in which an attacker abuse UDP-based network protocols to launch DDoS attacks that exceed hundreds of Gbps in traffic volume. These attacks are achieved using reflective DDoS attacks (DRDoS) where the attacker does not send the traffic directly to the victim, but sends spoofed network packets to a large number of systems that reflect traffic to the victim (reflectors). The attacker often chooses reflectors that send back responses that are significantly larger than the request (amplified).

In order to launch a DDoS amplification Attack, attackers mainly use two techniques. Firstly, the attacker amplifies its DDoS attack using UDP-based Internet services that reflect traffic. An attacker can for example abuse an open DSN resolver to trigger responses to DNS lookups. The attacker can choose a particular DNS query, resulting in a response that is much larger than the request. Secondly, the attacker spoof the source IP address of the traffic so that the response will be send to the target instead of the attacker. Such an attack requires amplifiers that are vulnerable to amplification DDoS (Krämer et al., 2015). According to Rossow (2014), there are 14 UDP-based protocols that could be abused for a DDoS attack. Attackers have to actively search for amplifiers on the Internet to launch an effective amplification DDoS attack. Therefore, for many of these protocols, attackers use Internet-wide scans to identify millions of amplifiers. Once discovered, an attacker uses a subset of the amplifiers as part of their attack. A schematic picture of a DDoS amplification attack is shown below (See Figure 10).

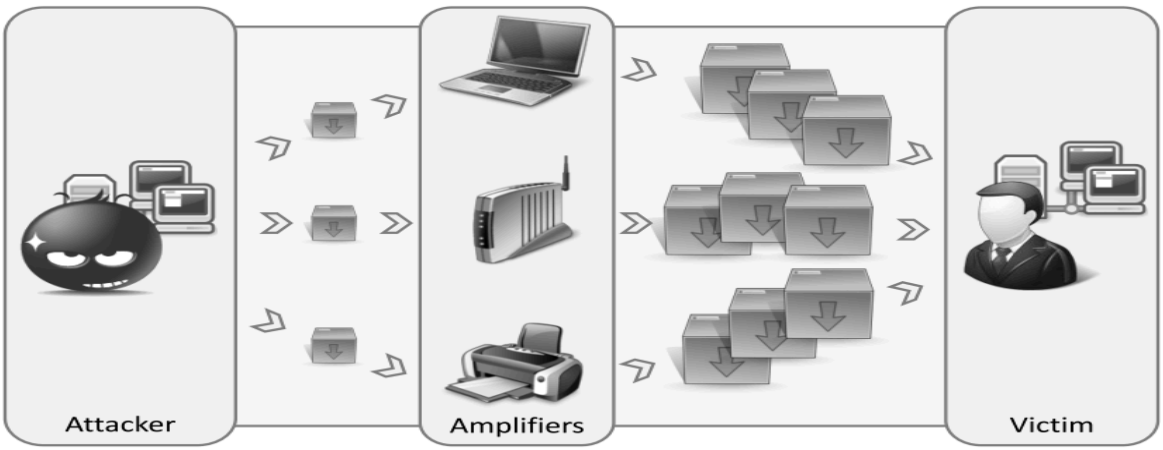

Figure 10: General threat model amplification DDoS (adapted from Rossow (2014))

4.2 Types of amplification protocols

The types of amplification attacks can be separated into two groups dependent on the type of communication protocol is used. The first and more widely used protocol is the UDP-based amplification attacks (connectionless), which is often used for discrete oriented data transfer (e.g. video calls). Multimedia streaming uses often UDP since data loss is possible. Second, TCP-based amplification attacks uses the TCP protocol, which is connection oriented (e.g. text messages, jpeg, video). The TCP protocol is more secure than UDP protocols, but the downside of this protocol is the bigger bandwidth that is needed.

4.2.1 UDP-based

User Datagram Protocol (UDP) is one of the core members of the Internet Protocol suite. UDP uses a simple connectionless transmission model with minimum of protocol mechanism, which makes it relatively easy to abuse. In the UDP protocol, packets are send separately, from which the packets have no knowledge of the preceding or following packet. UDP packets can arrive out of order or not at all. The recipient does not acknowledge packets, so the sender does not know whether a transmission was successful or not. The UDP protocol does not have provisions for the flow control. Packets can be received faster than they can be used. Due to this, the protocol is called connectionless because the packets have no relationship to each other and because there is no packet state. Rossow (2014) has identified 14 UDP-based protocols that could be abused in amplification DDoS. The most important protocols will be discussed below. A summary of the various protocols and their corresponding BAF are given in Table 2.

The BAF is determined based on the use of all the found servers. In practice, the attacker can use only the amplifiers with the highest BAF to launch an attack. Thus, the attacker can increase the attack by using only a subset of all the found amplifiers. In the table the BAF is shown for all the amplifiers, or the most severe 50% or 10% of the amplifiers, respectively (Rossow, 2014).

DNS - The Domain Name Systems network protocols traditionally has a low amplification rate. However, most of the DNS servers adopted a DNS extension (EDNS0) that allow for UDP responses of up to 4096 bytes (Karami, 2016; Krämer et al., 2015; Jose Jair Santanna et al., 2015). Without this extension the UDP response would be limited to 512 bytes. An attacker can abuse a DNS server by an *ANY* request with EDNS0 that returns all the known DNS record types for a given domain. This extension is used for expanding the size of various parameters of the DNS protocol that have size restrictions.

There are two variants of DNS amplification attack. An attacker can abuse the DNS open resolver as amplifier, by resolving ANY requests from domains that result in large responses. An attacker can even configure a domain he controls such that its authoritative name server responds with exactly 4096-byte-wide responses. As the amplifier caches these responses, the attacker's domain would have only little load. Based on the queried domain name length and the maximum EDNS0 size a resolver supports, DNS open resolver amplification can induce a payload by a factor between 28.7 and 64.1

As network operate have become aware of the abuse of open resolvers, the DNS resolver abuse is gradually decreasing. As an alternative, attackers are increasingly using authoritative name servers that include large resource records as responses. An important cause of this is the use of DNSSEC, in which a 1024-bit-wide signature in a special RRSIG record is added to the resource record. In this case, an attacker sends an ANY request to an authoritative name server. The payload of a DNS name server attack is much higher than a DNS open resolver. The BAF is 54.6 and can be as high as 98.3 for the top 10% of DNS systems. The amplification of using DNS name servers is much higher than the amplification of DNS open resolver even when attackers can control and maximize the contents of the response to an ANY request. The difference is due to

the fact that in most cases, DNS open resolver did not support EDNS0, which reduced the response to 512 bytes. For DNS name servers this was not the case.

SNMP – The Simple Network Management Protocol supports so-called *getBulk* operations. The *getBulk* operation returns a list of SNMP identifiers that can be monitored. This request can be used to iterate all monitoring values. The exact size depends on the number and length of the identifier in the returned list, but the BAF various from 6.3 to as high as 11.3 if 10% of the most severe amplifiers are used (Rossow, 2014).

SSDP - An attacker can use the Simple Service Discovery Protocol using the *discovery* request. The request returns a one-reply packet per service that the host has configured. The size of the response depends on the configured services and the length of the service name (USN). On average the BAF is 30.8. As some of the amplifiers responded with a few reply packets only as the offered less services. The attacker can achieve a BAF of as high as 75.9 if the 10% severe amplifiers are used.

CharGen (CHG) – The CharGen servers responded with random characters to a request. When a single byte was send as a request, the response was 358.8 bytes on average from the CharGen server. Due to lack of statistical significance, the BAFs of the top-10% and top-50% was not calculated by Rossow

QOTD – the Quote of the Day server is operates similar to CharGen in a sense that it send replies to UDP datagrams of any length (Böttger et al., 2015). The average size of the response was 140.3.

NTP – Network Time Protocol is the protocol that lets Internet-connected machines synchronize their internal clock. In older version of NTP, the protocol supports a monitoring service that enables administrators to query a given NTP server for a traffic count. This command, *monlist,* sends the requester a list of the last 600 hosts that connected to the queried server. The response the requester gets is much larger than the initial request. Rossow (2014) has found that most NTP servers implementations accept a short form of only 8 bytes. The response the requester receives the recent clients in up to 100 UDP datagrams with 440 bytes payload each. On average, monlist requests amplify the request traffic by factor 556.9–4670.0. NTP also allows for other features that may be abused for attacks with significantly lower amplification rates.

NetBIOS – the Network Basic Input Output System protocol is used to communicate within a Local Area Network (LAN). In order to set this communication a system responds with its current network and host name configuration. This protocol resulted in the highest amplification using a name lookup. The average amplification factor was 3.8. The response is influenced by the host names and network setup of the amplifier.

BitTorrent – BitTorrent can be abused using the hash searches, which are primarily used to find peers that serve a specific file(Böttger et al., 2015; Rossow, 2014). Using the hash searches can result in a large response, thus having the properties of an amplifier. In basic the peers only return a list of neighbouring. However, BitTorrent trackers also include two 265-byte-wide bloom filter arrays. As not all the peers know and share this information, the BAF varies among the amplifiers. On average, the BAF is only 3.8, but a BAF of 10.3 can achieved by abusing the top 10% of the amplifiers.

KAD – With KAD it is possible to gain a BAF between 16.3 and 22.7. The Kademilia client can shares between 15 and 31 peers (35 byte), which consist of an ID (16 byte), IP address (4 byte) and UDP port (2 byte), a header and metadata. The BAF for KAD is higher than the BAF of BitTorrent due to the smaller requests (Rossow, 2014).

ZeroAccess – The ZeroAccess P2P botnet supports three message types. From these message types the peer list and the command exchange offer the highest amplification. For a request of 16 bytes, the bot return 16 neighbours of 8 bytes each, and information about the currently active malicious modules, including a 128-byte-wide RSA signature by the botmaster. This results in a BAF between 36.0 and 41.1(Rossow, 2014).

Sality – Sality also offers three message types as part of their C&C communication. As Sality is a malware downloader and bots can exchange URL lists of files that bots should install on the infected system, which also includes a 256-byte wide RSA signature. A BAF of 37.3-38.4 can be achieved using Sality (Rossow, 2014).

Gameover – The Gameover malware is one of the most well known banking Trojan. The Gameover P2P bot uses the peer list and proxy list exchange mechanism to achieve amplification. For a request (52-byte-wide) the Gameover bot replies with a list of up to 10 neighbouring peers. Furthermore, the bot sends 4 additional datagrams with a list of proxies that can be used to upload data (usually stolen banking credentials). The Bot may even issue counter requests to amplification victims. The Gameover bot offers a BAF of approximately 46.0 (Andriesse et al., 2013; Rossow, 2014).

Quake3 – The Quake3 game servers can be abused through asking for its current state (15-byte-wide request). The server replies with a large response, which includes the detailed server configuration and a list of the current players. Quake3 offers a BAF of 63.9 and can go as high as 82.8 for the top 10% servers with many active players and complex server configurations (Rossow, 2014).

Steam – Similar to the Quake3 protocol, the Steam game protocol can also be abused asking servers for their current state. However, the BAF is significant lower since the response does not contain a list of the current active players. The Steam protocol offers an average BAF of 5.5 and can go as high as 14.7 (Rossow, 2014).

Table 2: Bandwidth Amplification factor

BAF				
Protocol	All	50%	10%	Scenario
DNS_{ns}	54.6	76.7	98.3	ANY lookup at author. NS
DNS_{or}	28.7	41.2	64.1	ANY lookup open resolver
SNMP v2	6.3	8.6	11.3	get*Bulk* request
SSDP	30.8	40.4	75.9	SEARCH request
CharGen	358.8	n/a	n/a	Character generation request
QOTD	140.3	n/a	n/a	Quote request
NTP	556.9	1083.2	4670.0	Request client statistics
NetBIOS	3.8	4.5	4.9	Name resolution
BitTorrent	3.8	5.3	10.3	File search
KAD	16.3	21.5	22.7	Peer list exchange
ZeroAcces	36.0	36.6	41.1	Peer list and cmd exchange
Sality	37.3	37.9	38.4	URL list exchange
Gameover	45.4	45.9	46.2	Peer and proxy exchange
Quake3	63.9	74.9	82.8	Sever info exchange
Steam	5.5	6.9	14.7	Server info exchange

From this table above, it can be seen that NTP produces the highest BAF. NTP amplification attacks can thus be considered as the most dangerous attacks there is today.

4.2.2 TCP-based

In the previous section it is shown that UPD-based protocols can be abused due to the connection-less nature of the protocols. On the contrary, Transmission Control Protocol (TCP) is a connection-oriented protocol in which the IP addresses (during the so-called handshake) of both communication parties are implicitly verified via initially random TCP sequence numbers. Thus, UDP-based protocols are relatively unsecure compared to TCP-based protocols due to the lack of a proper handshake. The lack of a proper handshake makes it possible to use a spoofed IP address, which is not possible for TCP-based protocols as IP address spoofing is restricted to the start of the TCP handshake. While the TCP handshake is suitable for reflection, it does not allow for easy amplification (Rossow, 2014). However, TCP can be used as an alternative source for amplification, despite its three-way-handshake protocol. According to Kührer et al. (2014) there are millions of TCP systems that can be abused to amplify TCP traffic by a factor of 20 or even higher. This is due to the fact that certain TCP stacks retransmit SYN/ACK packets multiple times (some 20x times or more) when they presume that the initial SYN/ACK segment was lost.

Abusing TCP can be a benefit from the viewpoint of an attacker. Firstly, providers cannot easily block or filter TCP traffic related to well-known protocols (e.g. HTTP), as compared to protocols that are less critical such as CharGen, QORD, or SSDP. Secondly, TCP-based attacks are hard to distinguish from normal traffic in a stream of TCP control segments, while for many UDP-based protocols provides can deploy payload-based filters. Thirdly, the amount of TCP amplifiers is huge, fixing the problem therefore seems infeasible (Kührer et al., 2014). As the TCP will not be relevant for this research since AmpPot did not gather amplification attacks that abused the TCP protocol, no further research will be done on TCP protocols.

4.3 Risks and consequences of DDoS (amplification) attacks

Financial services currently hold a lot of data and are increasing their online services. Therefore DDoS can be an important threat to their business continuity. However, the consequences and risks do not particular differ from other high-tech sectors. A problem lies in the commoditisation of DDoS attacks due to booters. Booters that use amplification techniques can cause damage to entire online industries, especially SaaS and e-commerce that are built on user-trust and constant availability (Verschuur, 2012). Well-known cases are the extortion of financial services by the Armada collective, and the more recent Kadyrovtsy actor (Shadows, 2016). Thus the threat landscape is increasing with a lot of new possible attackers.

4.3.1 Risk of DDoS

Operational risk – As DDoS attacks are designed to make services unavailable. Therefore, depending on the type of DDoS, an attack can have a significant impact on customer and employee's productivity. Due to an DDoS attack, an organisation is incapable of providing various services that the organisations provides, this can result in significant revenue losses if services are unavailable for a long period of time or if key services cannot be provided. Additionally if the company is unable to deliver services and thus violates service level agreement (SLA), it can also result in revenue loss.

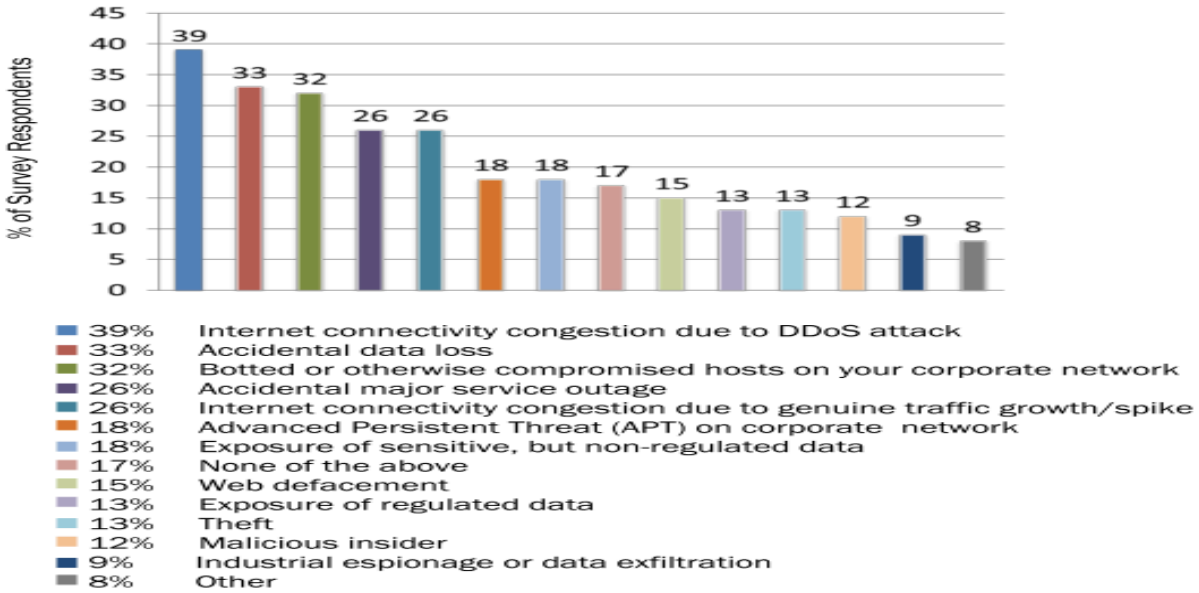

Figure 11: significant operational threats (adapted from Arbor Networks (2015a))

Zooming into the operational threats, the most obvious operational threat is the loss of Internet connectivity congestion. In addition, according to Arbor Networks, the second most significant threat is the accidental data loss followed by bottled or otherwise compromised hosts on the third spot (see Figure 11).

Reputational risk – Due to DDoS, customers encounter unavailability of services and can be affected negatively. Therefore the dissatisfaction among customers increases, which is an important risk for organisations. In fact, the cyber security company Kaspersky (Kaspersky Lab, 2015) research that 37% of 5000 companies that were targeted by DDoS attacks encountered reputational loss. Of all the risks, companies perceive losing the trust and confidence of customers the most damaging consequence of DDoS attacks. According to the survey by Kaspersky, 39% of the respondents said losing clients and suffering reputational damage was one of the most feared consequences of a DDoS attack. This percentage was higher than costs incurred in fighting and recovering from an attack (28%), or the loss of revenue and business caused by the associated downtime (26%) (Kaspersky Lab, 2015).

Data integrity risk – The study of Kaspersky showed that 26% of business that were attacked by a DDoS attack also suffered from business data loss or were unable to access business data. A DDoS attack can result in a disruption or delay of the connection between various data sources. The disruption or delay will impact the data integrity; as a result the data is not accurate anymore.

Fraud risk – The risk of fraud is usually overlooked when researching the consequences of DDoS attacks. The fraud risk occurs when an attacker uses DDoS attacks as a smokescreen, while the actual intent is to perform some fraudulent activity. The study by Kaspersky found that when an organisation was targeted by a DDoS attack, the organisations also faced threats such as losses and exploits through mobile devices (81%), the actions of other organisations (78%), phishing scams (75%) and even the malicious activity of internal staff (75%). The majority (87%) were also victims of targeted attacks (Kaspersky Lab, 2015).

Extortion risk – A more recent risk is the use of DDoS as a tool for extortion. Similar to ransomware, an attacker (usually a gang) sends a message to the target, which states that a DDoS attack will be launched if a certain amount of money is not transferred. Attacks were usually targeting business-critical websites in order to increase the likelihood of payment and

can have crippling effects on organisations (Shadows, 2016). An attack typically consists of a three-stage process:

- An email is sent to a targeted company or organization, with a sum of the demanded amount of money.
- Payment is demanded to an anonymised account number (BTC address/Paysafecard), in order to avert the threat of a sustained DDoS attack that would impact the targeted organization's ability to generate revenue.
- In some cases, the attacker adds pressure to payment by using negative publicity associated with service downtime as a threat.

The specific tactics and tools that are often used by the extortion actors include DDoS attacks that use SYN flood, NTP amplification, WordPress amplification, SSDP amplification, and UDP flood. If a service was protected by DDoS protection, the extortion actors tried to bypass the protection by targeting other infrastructures within the same datacentre in an effort to take the entire datacentre offline.

4.3.2 Cost of DDoS attacks

In the previous section, the financial consequences of cybercrime in general have been touched upon. In this part, the costs specifically for DDoS will be discussed. Three costs from the previous section are related to DDoS, the direct losses and the indirect losses explained in the operation costs section. The defence costs explained in the investment costs section.

Operational costs – As a result of the overall impact of DDoS, the business impact consist of 49% on operational expenses (see Figure 12) and nearly 40% indicates reputation or customer loss. Looking more closely into the bar plot, it shows that the costs are comprised of operational costs and revenue costs. DDoS attacks with a low impact and a low duration may result only in added operation costs. High impact and long duration DDoS attacks will also negatively affect revenues as business operations are partially or fully weakened (Arbor Networks, 2015b). In addition, due to the loss of trust and lost opportunities for the organisation, the organisation also needs to incur indirect costs. The elements that contribute to the costs of DDoS are the following:

- Personnel time spent addressing and recovering from the outage
- Incremental help desk expenses
- Lost sales
- Customer credits and refunds
- Lost employee productivity
- Cost of customer defections and lost or missed sales
- Degradation of reputation resulting in higher customer acquisition costs and a lower rate of business growth

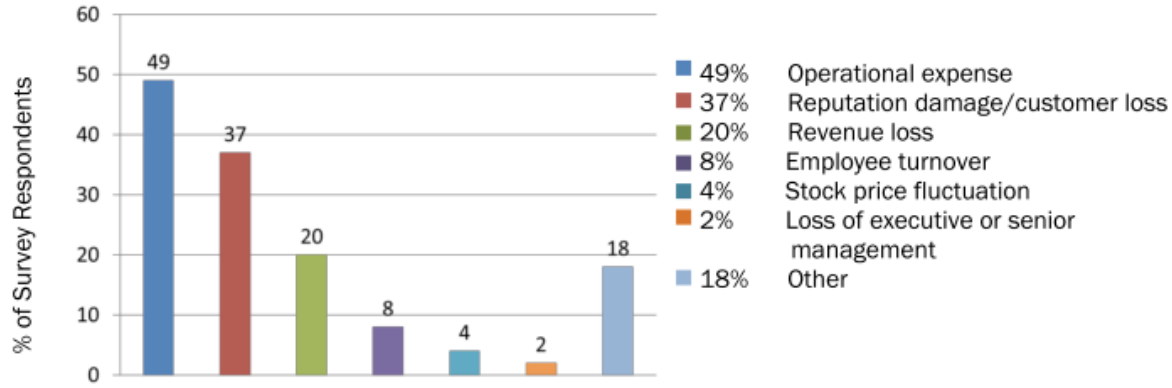

Figure 12: Business impact of DDoS attacks (adapted from Arbor Networks (2015a))

Investment costs – The volume, intensity, and frequency of DDoS attacks all continue to grow. Consequently, organisations with a significant web presence or that is reliant on the Internet connectivity for business continuity is a potential target and should try to cope with the risk of DDoS by implementing various mitigation tools and security mechanisms. Due to the risks of DDoS and the consequences of a successful DDoS attacks, more than half of the IT professionals believe that investing in DDoS to prevent or mitigate DDoS would be worth the investment (see Figure 13). One of the important aspects in mitigating DDoS effectively is hiring qualified personal. However, there is a disproportional mismatch between the supply and demand for cyber security experts. Subsequently, the lack of expertise results in not using the cyber security applications to its full potential. However, given the high bandwidth capacity needed to handle today's volumetric attacks, the cost and complexity of DDoS protection, and the expertise needed to stay up to date on the latest threats, challenging DDoS attacks one its own can be a tough challenge for an organisation (Arbor Networks, 2015a). In that regard, prevention of DDoS is mostly handled using a third party service. Outsourcing does not only effectively reduce damage, it also frees up IT personal.

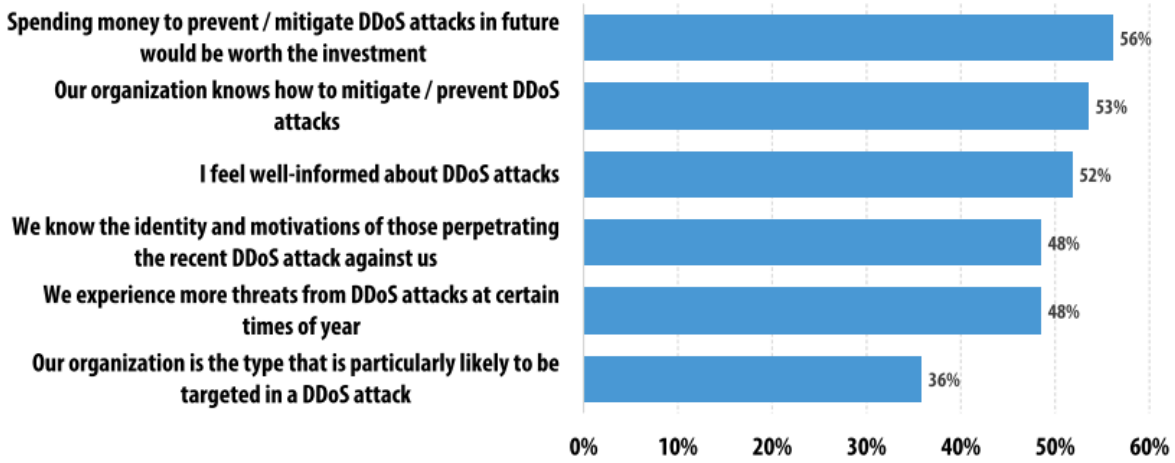

Figure 13: worth investing (adapted from Kaspersky lab (2015))

4.4 Factors influencing DDoS target selection

In literature there have been some discussions about the possible factors that can influence the target selection of a cyber-attack or DDoS attack. This section provides insight into those factors. These factors fuel the focus of the upcoming quantitative and qualitative analyses. The factors have been classed into external and internal factors. The external factors are the factors that fall outside the scope of the management of an organisation, while internal factors can be

changed by the management. Important to note that this list is by no means an exhaustive list of all the factors.

In order to identify these factors, it is important to understand how these factors were gathered. As studies have discussed little on target selection, the list of factors is limited. Therefore, to get a more detailed overview, this research will also identify factors that are related to minimizing the impact of DDoS attacks. The assumption is that attackers are trying to find new ways to maximize damage (Hoque et al., 2015). While this assumption seems intuitive, little research has focused on whether attackers base their target selection on the impact their attack brings to financial services. To analyse whether attackers use these impact factors also in order to select their target, these factors will be discussed below and analysed as well.

4.4.1 External factors

Organisation size – while organisations of all sizes are being targeted attacks are often worse for large organisations (Matthews, 2014). Organisations that have more than 500 employees are more likely to experience a DDoS attack, incur higher attack costs, and require more employees to mitigate the threat (Arbor Networks, 2016; Briney & Prince, 2002; Matthews, 2014). Tajalizadehkhoob et al. (2014) argue that for financial malware, the size of a financial service providers influences the target selection. They state that whether a bank gets attacked is related to its size. With size quantified as customer base and wealth of the customer base. However, the size should be above a certain threshold. Beyond the threshold, size does no longer seem to be a factor. However not all studies agree that size has an effect on the amount of incidents. According to Torres (2014) organizational size has little effect on the prevalence of experiencing an incident.

Type of organisation – The type of organisation and the sector they operate in are factors that can influence whether an organisation gets attacked. For instance, malware is often targeted at financial institutions as these organisations hold a large amount of money. According to a report by security company Arbor, the online gaming industry have been targeted frequently lately as well as the financial and telecom sector (Arbor Networks, 2016).

Context of the organisation – The context of the organisation is related to the country in which the organisation resides. In Krämer et al, (2015) they conclude that amplification DDoS attacks are a global problem, however most victims are located in the US or China. Also Noroozian et al. (2016) observed differences between and within countries. They conclude that in a number of countries the victimization for ISPs is lower than for others. One of the explanations was that country-level effects and institutional factors partially explain the differences. Two of their country-levels they observed were the ICT development index (IDI) and the gross domestic product at purchasing power parity (GDP PPP). The IDI is an indicator for the development of a country's development regarding its IT, ranging from 1 to 10 with higher values for more developed countries. There was a correlation for both explanatory variables, but limited. In addition, many reports show that well-developed countries do incur more DDoS attacks than others (Arbor Networks, 2015b, 2016; Jose Jair Santanna et al., 2015).

Technical innovativeness - Obviously, organisations that have many operations online and do have a digital infrastructure can be targeted, while old-fashioned organisations with no online operations able to be victimized. Updating software or firmware allows for new functionality or new features. An attacker may be able to exploit such updates (Preyadharsini & Deepa, 2016). When FSOs moved from traditional banking to online banking, the threat of DDoS occurred. Currently, cloud computing have been the new innovations banks are heading towards, but Cloud computing-based services are also among the favourites targets of DDoS attackers (Bakshi & Yogesh, 2010; Somani, Gaur, Sanghi, Conti, & Buyya, 2016). With each digital door, a

financial institution opens to better serve of clients, but also new vulnerabilities. Yet, digitalization is necessary to meet consumer demands for 24/7 access (Geyres & Orozco, 2016).

Presence of a capable defender – According to Routine Activity Theory (RAT), crime results when three different variables converge in time and space: a likely offender, a suitable target, and the absence of a capable guardian (Choo, 2011; Cohen & Felson, 1979). The theory states that a crime occurs when an offender comes into contact with a suitable target, when there is no capable guardian around to prevent the offender in committing the crime. In addition, the theory claims that there is causality between the increase in crime rates and the supply of suitable targets and capable guardians (Ngo & Paternoster, 2011).

4.4.2 Internal factors

Presence of experts – As DDoS often impacts critical business services; the response to a DDoS attack must take into account minimizing additional disruption to those and other services. Therefore, organisations require dedicated and in-house expertise with business knowledge (Krämer et al., 2015; Pescatore, 2014). These experts need to be capable to countermeasure the attack and In order to minimize financial and reputation losses (Bougaardt & Kyobe, 2011) and be able to detect the attack as soon as possible. As DDoS results in high waste of resources, DDoS attacks have to be detect as near as possible to their source (Jin & Yeung, 2004; Zargar et al., 2013). Not only on operational level, expertise is required, also cyber security expertise in organisation boards is necessary (Pierrakis & Collins, 2013).

Communication structure – Security has been and viewed as a nuisance for the business, but this can be changed with better communication and alignment (Kark, Dines, Balaouras, & Coit, 2010). The manner in which information security is communicated can strongly influence how it is influenced and whether and how it is acted upon (Parsons, 2010). The essential part of acting on these actions is especially important during an attack, communication is then key to mitigate swiftly, to start the mitigation or start the incident response plan (Lagazio et al., 2014; Pescatore, 2014).

Shared responsibilities- Many security responsibilities cannot be performed by single person or a dedicated security person (Pescatore, 2014). Having shared responsibilities is therefore necessary and have proven to be quite satisfactory in practice (Brenner, 2007). Having shared responsibilities can result in better communication and cyber governance. However, shared responsibility is appropriate for organisations that do have a DDoS plan in place before a DDoS Event (Hall et al., 2015; Kark et al., 2010).

Speed of updating, patching – As DDoS attacks can exploit software errors, it is important to make certain that defences are kept updated on latest and evolving threats as they emerge (Alieyan, Kadhum, Anbar, Rehman, & Alajmi, 2016). Patching is an important factor that can limit the amount of live botnets, and thus also limits the amount of DDoS attacks (Wueest, 2014; Yu et al., 2012). However, attackers are eager to find new exploits and counter every attack effort made in patching vulnerabilities by exploring other weaknesses that can be exploited. Therefore, it is important to update and patch the software frequently and as soon as possible. Rescorla (2005) found weak evidence that finding security defects is a useful security activity and leads to a measureable effect of the software security defect rate. A major reason why vulnerabilities are still hazardous after patches are available is because the adoption of the organisation is slow (Rescorla, 2003).

(General) knowledge of DDoS –While having in-house experts can help in mitigation DDoS attack successfully, the general knowledge of DDoS among staff is also important (Kraemer, Carayon, & Clem, 2009). Bougaardt & Kyobe (2011) argue that insufficient knowledge or

awareness of IT risks and computing limitations are a major factor inhibiting small organisations from engaging in effective cyber countermeasures.

Centralized security – Whether the security inside an organisation should be centralized or decentralized depends on various factors. For organisations with unique and independent business units, a centralized security model could be useful. However, there are a number of core security functions that work better in a decentralized environment and the other way around. Usually, the IT risk and architecture are best handled in a centralized environment, while operational roles can be decentralized to the business units. For many organisations a complete decentralized security organisation is only ideal with extremely autonomous business units that have very different security needs. While for most firms a centralized security organisation will provide greater inconsistency, influence, and control(Kark et al., 2010; Kraemer et al., 2009).

Budget on cyber security – The budget organisations have, or are willing to spend on cyber security, determines the target selection of many cyber-attacks, including DDoS. Therefore, currently many small and medium-sized enterprises (SMEs) are being targeted due to their lack of mitigation tools. Controlling the costs is extremely important for SMEs as they have many limitations on their budget. For them it is therefore important to prioritise on what to invest. Somani et al. (2016) argues that the DDoS attack mitigation costs should ideally be less than the losses inquired by an DDoS attack without mitigation. Next to the expensive mitigation tools it is also important to spend resources on training and awareness. However, for SMEs resources and funds may not always be available to provide extensive awareness, training and education to all employees in all areas, it is necessary to prioritise on what to invest (Parsons et al., 2010; Wilson, M., & Hash, 2003).

Crisis/DDoS plan – As preventing a DDoS attack is almost impossible; having a crisis plan is the most important step to mitigate the impact of DDoS on the business (Kelley, 2016; Wueest, 2014). This plans ensures that organisations understand how the organisation will respond when it suffers a DDoS attack. Besides having a plan, the plan should be regularly tested. Often, however, establishing plans are impeded by conflicts over responsibility for the plan or budgetary concerns (Pescatore, 2014).

Presence incident response team – Closely related to the presence of experts and the crisis plan, is the presence of a security task force, or incident response team. When a security incident occurs, it is critical for an organisation to have an effective way to identify something has happened and to conduct a response (Ruefle et al., 2014).

In the table below, a list of the discussed factors is provided.

Table 3: Factors influence target selection according to literature

Influential factors	**Mentioned in**
External	
Organisation size	Briney & Prince (2002) Arbor Networks (2016) Tajalizadehkhoob et al. (2014) Torres (2014) Matthews (2014)
Type of organisation	Arbor network (2016)
Context of the organisation	Arbor Networks (2015b/2016) Jose Jair Santanna et al. (2015) Krämer et al. (2015) Noroozian et al. (2016)

Technical innovativeness	Preyadharsini & Deepa (2016) Geyres & Orozco (2016)
Presence of a capable defender for security and crisis management	Choo (2011) Cohen & Felson (1979) Ngo & Paternoster (2011)
Internal	
Presence of experts	Bougaardt & Kyobe (2011) Kraemer et al. (2009) Pescatore (2014) Pierrakis & Collins (2013)
Communication structure	Kark et al. (2010) Parsons (2010) Lagazio et al. (2014) Pescatore (2014)
Shared responsibilities	Kark et al. (2010) Pescatore (2014) (Hall et al., 2015) (Brenner, 2007)
Speed of updating/patches of third parties	Alieyan et al. (2016) Wueest (2014) Yu et al. (2012) Rescorla (2003; 2005)
(General) Knowledge of DDoS	Bougaaardt & Kyobe (2011) Kraemer et al. (2009)
Centralized security	Kark et al. (2010) Kraemer et al. (2009)
Budget on cyber security	Parson et al. (2010) Wilson & Hash (2003) Somani et al. (2016)
Crisis/DDoS Plan	Kelley (2016) Pescatore (2014) Wueest (2014)
Presence of a security task force	Ruefle et al. (2014)

4.5 Conclusion literature study DDoS amplification attack

SQ1: What is DDoS amplification, and what are their threats?

DDoS amplification attacks are a special kind of DDoS, which uses an extra level that can amplify the initial traffic. In order to do so, the criminal abuses open Internet serves such as DNS or NTP for their amplification. The attacker does not directly send traffic to the victim. Instead, the attacker sends spoofed traffic to a large number of systems (amplifiers or reflectors). The systems send back a response that is usually significant higher than the request to the victim. Due to the commoditization, DDoS is becoming a relatively easy cyber-attack for cyber criminals to use. While advanced technical skills were necessary to launch an attack, nowadays attacks can be launched with the press of a button and little to no financial means. In combination with amplification protocols, these attacks can be increased to large sophisticated attacks. This means that everybody using the Internet could be a potential threat to business, governments, and other individuals.

SQ2: What are the risks and consequences of DDoS amplification attacks for FSOs?

As a result of the possible high impact of DDoS amplification attacks, organisations, organisations need to invest heavily in strategies to mitigate possible attacks. In addition to the investment costs, if an attack is successful, the business impact consists of 49% on operational expenses and nearly 40% indicates reputation or customer loss. On a detailed level, attacks with low impact and low duration result only in added operation costs, while high impact and long duration attack will also negatively affect revenues. On an organisational level, there are various risk involved when victimized of a DDoS attack. Firstly, the DDoS makes online services unavailable, which means that organisations are not able to continue their operations. This risk can result in significant revenue losses if the attack is not mitigated quickly. Second, due to the unavailable services, customers are not able to use those services. The unavailability influence customers negatively and thus lead to reputational harm. Thirdly, DDoS occasionally serves as a distraction for other attacks such as fraud and stealing of data. In addition, a DDoS attack can result in disruption or delay between the connection of different data sources, which impacts the data integrity. Lastly, DDoS can be used as a mean to extort organisations.

SQ3: What factors influence DDoS target selection according to literature?

The literature discusses various factors that could influence the number of attacks. These factors are categorised into external and internal factors. The organisation size is an important external factor that leads to increase DDoS attacks. Organisations that have more than 500 employees are more likely to experience a DDoS attack, incur higher attack costs and require more employees to mitigate the attack. The type of organisation and sector also affects the attack rate. For instance in online gaming DDoS is often used, as well as for the financial and telecom sector. One of the reasons why the telecom and financial sector are targeted often is due to the fact that organisation in these sectors provide various services online are innovating frequently on technical level. The presence of a capable defender also affects the number of attacks. A crime occurs when an offender comes into contact with a suitable target, and when no capable guardian is around to prevent the criminal from committing the crime.

In addition to the external factors, also various internal factors are identified, which relate to the impact of an attack. These factors are also assumed to influence the attacker, as attackers want to maximize their impact. Internally, the presence of experts is important. Due to the criticality of the response time, having dedicated and in-house expertise with business knowledge and are capable to countermeasure the attack decreases the number of successful attacks. Therefore, implementing an incident response team that is able to quickly response to an attack, does affect the target selection. This means that the security structure should also be decentralized. However, whether the security structure should be centralized or decentralize depends on various factors such as the type of business units or core security functions. Also, the incident response team should know what to do when the organisation is under attack; this needs to be formulated into a crisis plan. In addition, also working staff needs to be educated on the threats of DDoS in order to limit attacks. The manner in which organisations communicate internally, strongly affects on how is acted upon an attack, and thus also future attacks. Furthermore, DDoS application attacks abuse software vulnerabilities, these vulnerabilities have to be patched as quickly as possible. Lastly, organisations that spend too little on cyber security are of course susceptible for attacks. Therefore, many SMEs are being targeted due to their limited budget.

PART III: Data analysis

5. Target selection according to AmpPot

This section will provide insight in the factors of target selection according to the FSO attack data that was extracted from the AmpPot dataset (see section 5.1). This in turn will provide input for section 7 in which both the input from this section as the next section will be compared. Thus, provide the similarities and differences in the perspective of the experts and the findings in the AmpPot data. To do so, this section will start with the proportion of the selected financial attack data and how that relates to the total AmpPot data and total financial attack data. Furthermore, a descriptive analysis will be conducted to provide a high-level overview of the AmpPot data and a first glance into factors those are worthwhile to analyse. The descriptive research is followed by an explanatory analysis, which dives deeper into the results found in the descriptive analysis.

5.1 Representation of the identified FSOs

This section provides an overview of how well the mapped FSOs are representative for the total financial market as well, as how they are proportionated in the attack data. This is important as keywords provide the input for the analysed data. Therefore, the keywords should be robust in order to assemble a financial dataset that is representative for the whole financial market. In addition, in order to get a full understanding of the DDoS amplification landscape, it is important to know the proportion of attacks with a FSO as victim. Determining the proportion is the first step to understand the scale of victimization of financial services. This section will firstly provide the result from the sensitivity analysis, followed by an overview of the proportion of the financial data contrary to the remaining AmpPot data.

5.1.1 Sensitivity analysis

To perform the sensitivity analysis, this research uses an additional data set that originates from the USA Internal Revenue Service (IRS). This Foreign financial institution (FFI) dataset consists of 288128 entries that are related to financial institutions and is used for the Foreign Account Tax Compliance Act (FACTA). Contrary to the name of the list, this list also contains a set of the financial institutions in the USA. To understand how well the financial data represents the total financial market, the same search queries are performed on the dataset. The results are depicted in Figure 14 (left graph). The bar plot illustrate that approximately 47% of the list with financial institutions can be found using the keywords. Thus, slightly less than the half of the organisations can be mapped using these keywords. While this percentage is not low per se, it is important to understand how this number was formed. The main reason for this percentage has to do with the names financial institutions with non-financial names. The FFI data showed a significant amount of organisations that cannot be identified through their names solely, such as Ediana International S.A., Laertes Holdings or P health Sarl. Analysing the dataset that was not mapped by the keywords, almost all the organisations have non-financial names. While the keywords are only able to identify half of the financial institutions, it will be extremely time consuming a labour intensive to map individual financial institutions by hand. Therefore, this research will not focus on those organisations.

In order to understand how well the financial data represents the total financial market, a similar approach is used as for the FFI data. However, this part uses a MaxMind dataset that features a list of 428,226 organisations in 2015. The main reason for the use of the MaxMind data was to limit data asymmetry as a similar MaxMind database was also used during the matching of the targeted IPs to an organisation. The bar plot (right graph in Figure 14) shows that 4.5% of the all the total organisations can be mapped as a financial institution using the identified keywords. This is a small percentage, but it has to be noted that the data shows all the organisations worldwide. Of those financial organisations, 402 can be found in the attack data

and thus have been targeted according the AmpPot data. This is a 2.0% of all the found financial organisations. This result can be argued in two ways. First, not many FSOs are represented in the AmpPot data, and thus relatively few FSOs have been targeted compared to the other the non-financial gathered data. Second, an amount of FSOs have not been identified in the dataset by the keywords. However, it seems very unlikely that adding keywords that are not specific for an individual organisation could significantly improve the amount of FSOs. These issues will be addressed in 8.4.

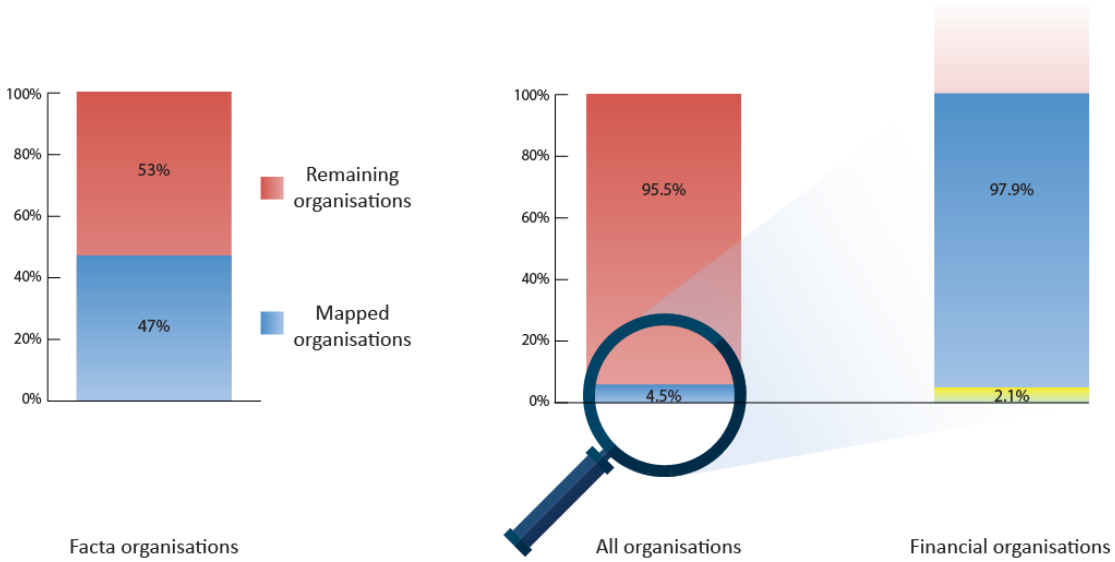

Figure 14: Bar plots mapped FSOs

5.1.2 Proportions of the FSO data

Table 4 shows the proportions of the various types of autonomous systems (AS) that have been classified in the AmpPot. The table shows the percentages for the total AmpPot data without the mapping of the FSOs as well as with the mapping of the FSOs. In the table it is visible that most of the types of AS are ISPs (~55%) and a large proportion of unknown AS (37%). The table also shows that most 8% of the AS's hosting providers. In addition, the data provides AS of the type education and government. A similar demographic can be observed with the FSOs. The table shows that only a small fraction of the dataset is considered FSO (0.28%). For more information of this issue, refer to the previous section and 8.4.

Table 4: Victim demographics

	Education	Government	Hosting	ISP	Other	FSO
AmpPot	0.20%	0.01%	8.28%	54.89%	36.61%	-
AmpPot incl. FSOs	0.20%	0.01%	8.28%	54.85%	36.465	0.19%

To dive deeper in the proportion of the FSOs, a general overview of the AmpPot data compared to the financial data will be provided. This section will provide the total amount of attacks, the amount of unique IPs, thus the total unique attacks and the approximate amount of unique organisations. The latter is important to understand how many companies have been targeted in a time span of 2 years see (see Table 5).

Table 5: Description financial AmpPot data

Type of cases	Total AmpPot data	Financial data	Non-financial data
Amount of attacks	5,721,432 (100%)	10,795 (100%)	5,710,637(100%)
Unique IPs attacked	1,114,787 (19.5%)	2,210 (20.5%)	1,112,591 (19.%)
Unique organisations	24,921	402	24,519

The total AmpPot data consist of 5,721,432 attacks, from which 1,114,787 are unique attacks. In addition, there are 24,921 unique organisations that have been targeted. Thus, a lot of DDoS attacks are targeted on the same IP addresses and same targets (see Table 5). The financial dataset that was extracted from the total AmpPot dataset is the key dataset for the analysis. The dataset consists of 10,795 IP addresses. That is 0.19% of the total AmpPot dataset, making it significantly smaller. The data consist of 2,210 unique IPs and 402 unique organisations. Proportionally this means that 0.016% of the total unique organisations are FSOs. The non-financial data was constructed by removing all the financial data from the total AmpPot data. While in percentage the difference of distribution between the non-financial dataset and the total data is none, this part is added for completeness. The dataset consists of 5,706,277 IPs from which there are 1,112,591 unique IPs and 2,491 unique organisations.

5.2 Descriptive analysis: an high level overview of the financial honeypot data

To find factors that influence target selection, one first has to understand how the data can provide for these answers. The purpose of this section is to provide an initial exploration that gives direction for an in-depth analysis into factors that could be used for target selection. To do so, this section will describe the relevant variables to use from the AmpPot data, and how these variables can function as target selection variables.

The AmpPot data consists of various variables that will not be used for this particular research as it also misses variables that need to be added to the dataset. Throughout the analysis, additional variables will be added to the dataset.

The list below, show the variables that will be used for this particular research.

1. **target_ip:** The IP address that has been targeted by a DDoS attack.
2. **date:** The date of the attack.
3. **service:** The protocol that was used to execute the attack.
4. **duration:** Attack duration.
5. **cc:** Short form of the country in which the IP address seems to reside.
6. **year:** The year of the attack.
7. **org:** The name of the organisation which has been assigned to the target_ip
8. **weekday:** The weekday on which the attack was launched.

5.2.1 Different attack variables

From this part on, a selection of attack variables will be explored and discussed. These variables are explored based on the target selection factors mentioned in the literature study (see section 4.4), as well as new interesting findings throughout the exploration. As AmpPot does not provide data on target selection factors, these variables are related to the number of attacks. While the number of attacks is not the same as target selection, the variables provide insight in how they influence the number of attacks, and thus how attackers can choose their target based on those variables. Important to note, these variables are by no means exhaustive lists of attack variables as the AmpPot data is within boundaries.

Attack types

The AmpPot data provides various protocols that were used by the attacker. As Rossow (2014) mentioned, there are attack techniques that are well-known for some protocols, such as DNS. For other attack protocols it is unclear whether these are vulnerable to similar or worse attacks. This section gives insight into the popularity of various protocols among attackers. Understanding the types of protocol gives insight into the ease of use or abuse rate of the various protocols and whether should be focus on a specific protocol.

In Table 6 the distributions of the various protocols is visualised. The AmpPot honeypots have gathered six protocols (DNS, NTP, CharGen (CHG), QOTD, SNMP, and SSDP). For FSOs, the most frequent used protocol is DNS, followed by NTP. CHG is less used for financial services, while SSDP is more used. SNMP is almost never used. The QOTD protocol was completely absent in the financial data. These results are similar to other studies (Krämer et al., 2015; Noroozian et al., 2016). The popularity of DNS and NTP is most likely due to the fact that they are open Internet services, and cannot be easily turned off to reduce the amount of abuse. Furthermore, services like DNS and NTP exist more often on the Internet than for instance QOTD. SNMP has one of the lowest BAF among the protocols researched by Rossow (2014), explaining the low usage of this protocol. In addition, the amount of attacks has increased by a factor of 11 from 981 in 2014 to 9,904 in 2015.

Table 6: Distribution attack protocols

	CHG	DNS	NTP	QOTD	SNMP	SSDP
Non-FSO	11.27%	41.27%	38.77%	0.02%	0.65%	8.02%
FSO	3.04%	50.68%	36.42%	0%	0.04%	9.82%

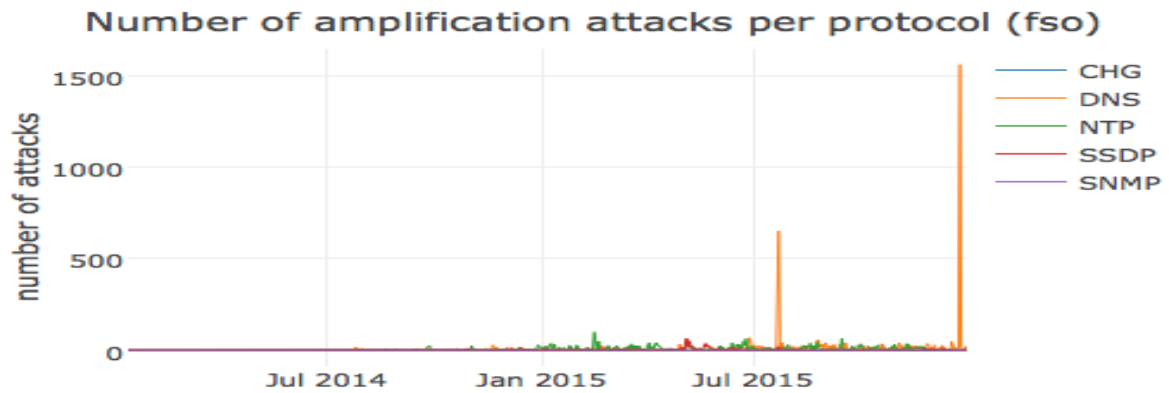

Figure 15: Number of attacks per protocol FSO data

Figure 15 shows the various attacks per protocol over time. Considering the most frequently attacked organisations by each protocol, most of the organisations were large FSOs that were listed on the Fortune500. For instance, the most attacked organisations for DNS were Barclays and AKBANK TAS. Diving deeper into the attacks on these organisations, it shows that these organisations were attacked on 23-7-2015 and 25-12-2015. While there was no clear reason for the attack on AKBANK TAS, there was for Barclays. Just before the 23rd, Barclays received a lot of media attention[1][2][3][4]. Other organisations that were frequently attacked were Wells Fargo & Company, Swedbank, Bank of America, and Itau Unibanco S.A. These organisations have in common that they are prominent and well known. This signals that prominent organisations

[1] https://www.scmagazineuk.com/exclusive-barclays-builds-out-security-team-with-second-europol-hire/article/537021/

[2] http://www.computerweekly.com/news/4500246707/DD4B-cyber-extortion-gang-targets-key-European-sectors

[3] http://www.abc.net.au/news/2015-05-21/us-britain-fine-top-banks-nearly-6-bn-for-forex-libor-abuses/6485510

[4] https://www.ft.com/content/a255cd2a-fef8-11e4-84b2-00144feabdc0

have some effect on the number of attacks on that particular organisation. To gain more insight into this finding, a closer look will be given in the next section.

Organisation size

The previous section showed that the most frequently attacked organisations per protocol were Fortune500 listed organisations. More comprehensively, taking a closer look at the top 10 most attacked organisations, the data demonstrates that most of the top attacked organisations are large organisations such as AKBANK TAS, Barclays, Itau Unibanco S.A., Swedbank, and Samba Financial Group. Aside from PayPal, all the Fortune500 listed organisations are banks (Table 7). The assumption is that being listed in the Fortune500 does influence the target selection due to the prominence of these organisations. In the table also FSOs are targeted, which are not known to be large organisations such as Oakleigh Capital and Capital Network Ltd. Therefore, how and to what extent the size of an organisations influence target selection remains unclear.

Based on these findings, the assumption is that the more prominent organisations were more frequently selected as target than other organisations. One way to analyse the prominence of the organisation is to measure their size. Various studies and cyber security companies have also mentioned the influence of organisation size, which have been discussed in section 4.4. The next section will provide more insight into the size factor of organisations. In order to do so, the size has to be defined properly in advance as it can be expressed by many factors. As AmpPot did not provide the organisation that was assigned the targeted IP, it naturally does not provide any indicators for the size of an organisation. Therefore, the data to measure the size has to be gathered first. For this research, size will be expressed by: number of owned IPs/domains per organisation, profits, revenues, market value, net income, total assets, and amount of employees.

Table 7: Top 10 attacked FSOs

#	Organisation	# Attacks
1	Cenozoic Investment Co.,ltd	1,590
2	AKBANK TAS	1,568
3	Barclays Capital	866
4	Itau Unibanco S.A.	782
5	Oakleigh Capital Ltd, Philippine	177
6	Vivo Trade L.P.	155
7	Swedbank AB	102
8	Samba Financial Group	96
9	PayPal	88
10	Bank of America	77

Type of country

Section 4.4 denotes that the context such as the country an organisation resides in can influence the target selection of DDoS attacks. This section explores the countries that have been targeted for the financial data. As the financial data on its own does not provide a clear view on the target selection, this section also compares the result of the financial data to the non-financial data. This comparison allows for a comprehensive view on how a country influence the number of attacks, and thus the target selection for FSOs compared to non-FSOs. Due to the large amount of countries present in the datasets, only the top 10 most targeted countries will be discussed.

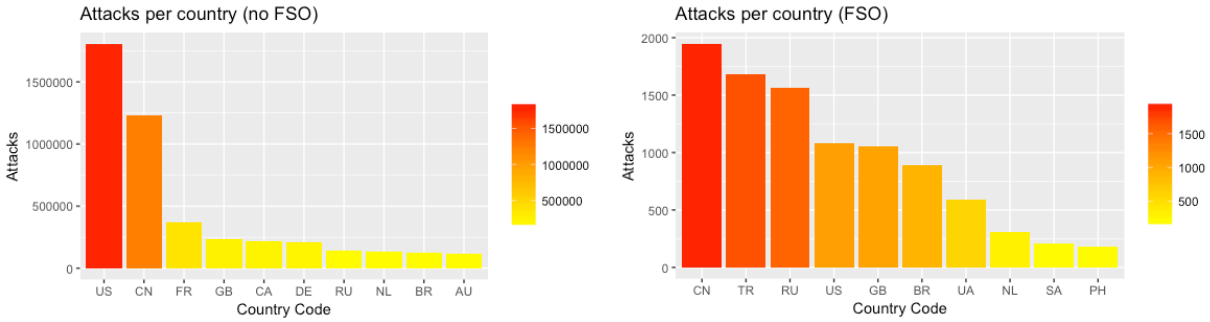

Figure 16: Total number of attacks per country non-FSO and FSO data

Given the bar plots, a significant different between the financial data and non-financial data can be observed. While the USA and China were most targeted for the non-financial data, the outcome is different from the financial dataset. The bar plot above (right graph in Figure 16) illustrates that the US is not among the top three most targeted countries for the financial organisations. Surprisingly Turkey (TR) holds the second place, followed by Russia. Pattern wise, a substantial difference between the two datasets is also visible. The non-financial data shows a more exponential pattern, while the financial data shows linear decay. The financial data demonstrates that the number of citizens does not affect the number of attacks of a country. However, the bar plots shows that most attacks occur in relatively developed countries.

To obtain a better understanding of the type of countries that were attacked, factors that explain the population, ICT development (see section 4.4.1), and economic status, such as the gross domestic product (GDP), Nominal GDP per Capita, Gross domestic product at purchasing power parity (GDP PPP) were gathered (see Table 8). This data has been gathered from the world databank and the ICTU database. The table shows that the top 3 countries (China, Turkey, and Russia) are not among the highest developed countries. These countries do not have a significantly high IDI or GDP such as the United States. Based on these findings, the conclusion is drawn that countries with an average IDI and are semi-developed are selected more frequently as target. A more in-depth analysis on these factors will be conducted in section 5.3.

Table 8: Country-level indicators top 10 countries FSO

Country level indicators					
Country	Population (m)	GDP ($)	Nominal GDP per Capita ($)	GDP PPP ($)	IDI
CN	1371.22	11,007,721	8,028	19,815,111	5.05
TR	78.67	717,880	9,126	1,574,018	5.58
RU	144.10	1,331,208	9,093	3,687,406	6.91
US	321.42	18,036,648	56,116	18,036,648	8.19
GB	65.13	2,858,003	43,876	2,722,455	8.75
BR	207.85	1,774,725	8,539	3,216,169	6.03
UA	45.15	90,615	2,115	340,172	5.23
NL	1,69	750,284	44,300	840	8.53
SA	3.15	646,002	20,482	1,688,633	7.05
PH	100.70	292,451	2,904	743,898	4.57

Weekday

Similar to the previous variable, also a comparison is made between the financial data and non-financial data for the variable weekday.

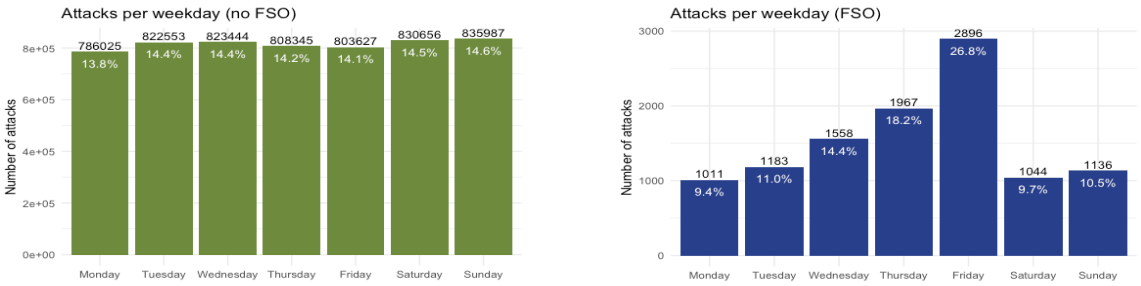

Figure 17: Distribution DDoS amplification attacks per weekday

Figure 17 shows a significant difference between financial and non-financial data. The bar plot on the left demonstrates a uniform distribution for non-financial organisations over the weekdays. The assumption is that for each given weekday, there is no different in the number of attacks based on a particular day of the week. One can assume that the non-financial data consist of a large number of gaming related DDoS attacks, which take the overhand of the distribution. As gamers do not discriminate between days to attack, there is no diversity in the number of attacks per day. On the contrary, a significant different distribution is observed from the financial organisations. This data clearly demonstrates that attacks on Fridays happen significantly more than each other weekday. There are almost twice as many attacks on Friday compared to other weekdays. An important observation is the fact that the least attacks happen during the weekdays. In addition, from Saturday to Thursday a linear increase in the number of attacks is visible, which indicates that as the week progresses, also more attacks happen, with the peak at Friday. A clear explanation of the attack distribution of the financial data is lacking. One can argue that attacks on Friday are due to less utilization as most of the staff will leave for the weekend, resulting in more attacks due to higher success rate for attackers. However, this assumption can also be argued for non-financial sectors. As information on whether the employee utilisation is different during the weekends for financial organisations is absent, no clear explanation can be given.

5.3 Explanatory analysis

The descriptive analysis showed that factors such as the type of protocol and weekday are influential factors for target selection. For other factors such as organizational size and the country where the company is manifested in, the actual effect remains unclear. This section will provide a more thorough analysis to obtain a more comprehensive understanding of the influence of the organisation size and the country on target selection and attack duration.

Preparing dataset for explanatory analysis

Since the AmpPot data does not provide country-level factors and organisation size indicators, these were added to the dataset. Due to limited accessibility to the size indicators, only data from the Fortune500 was used. The data was gathered from the Fortune500 website and data files that were made publicly available on the Internet. The size data was merged into one dataset and added to the AmpPot dataset. A summary of the data can be found in Appendix C (see Table 25). It has to be noted that in terms of size, the non-Fortune500 listed organisations were disregarded.

5.3.1 Explanatory analysis type of country

Section 5.2 argued that semi-developed countries are more selected as target. Based on this section, one can assume that the country or the context of the organisation correlates with the number of attacks. This correlation is adopted from Figure 16, which illustrates that a number of countries are disproportionally more attacked than others. This section will dive deeper into the analysis part, which looks at the country-level factors.

Finding patterns for country-level factors

Section 5.2 raised the assumption that there are various country-level factors that influence the number of attacks. Thus it remains the question *which and how country-level factors affect the target selection in terms of the number of attacks per organisation?* In order to answer this question a linear regression will be done to analyse if the added country-level factors (IDI, GDP, Nominal GDP Per Capita, GDP PPP, and the population) correlate with more attacks. The scatterplots (see Figure 18) visualises the number of attacks against each factor. To have a clearer visualisation, outliers were removed (see plot 2). Based on these scatterplots, a clustering pattern for the factors IDI, GDP PPP, and Nominal GDP Per Capita is observable. Taking a closer look at the plots of the Nominal GDP Per Capita, the points are clustered for low to average Nominal GDP Per Capita. For high GDPs there are not many of attacks. For the GDP PPP also clustering and a slight linearity is observable. However, there seems to be a large gap between high and low GDP PPP. As these three factors show patterns, they will be analysed more thoroughly using linear regression to determine whether there is a correlation between those two variables and the number of attacks. No patterns were found for the GDP and population size (see Figure 28 in Appendix E). Therefore, the GDP and the population size will be disregarded for further analysis.

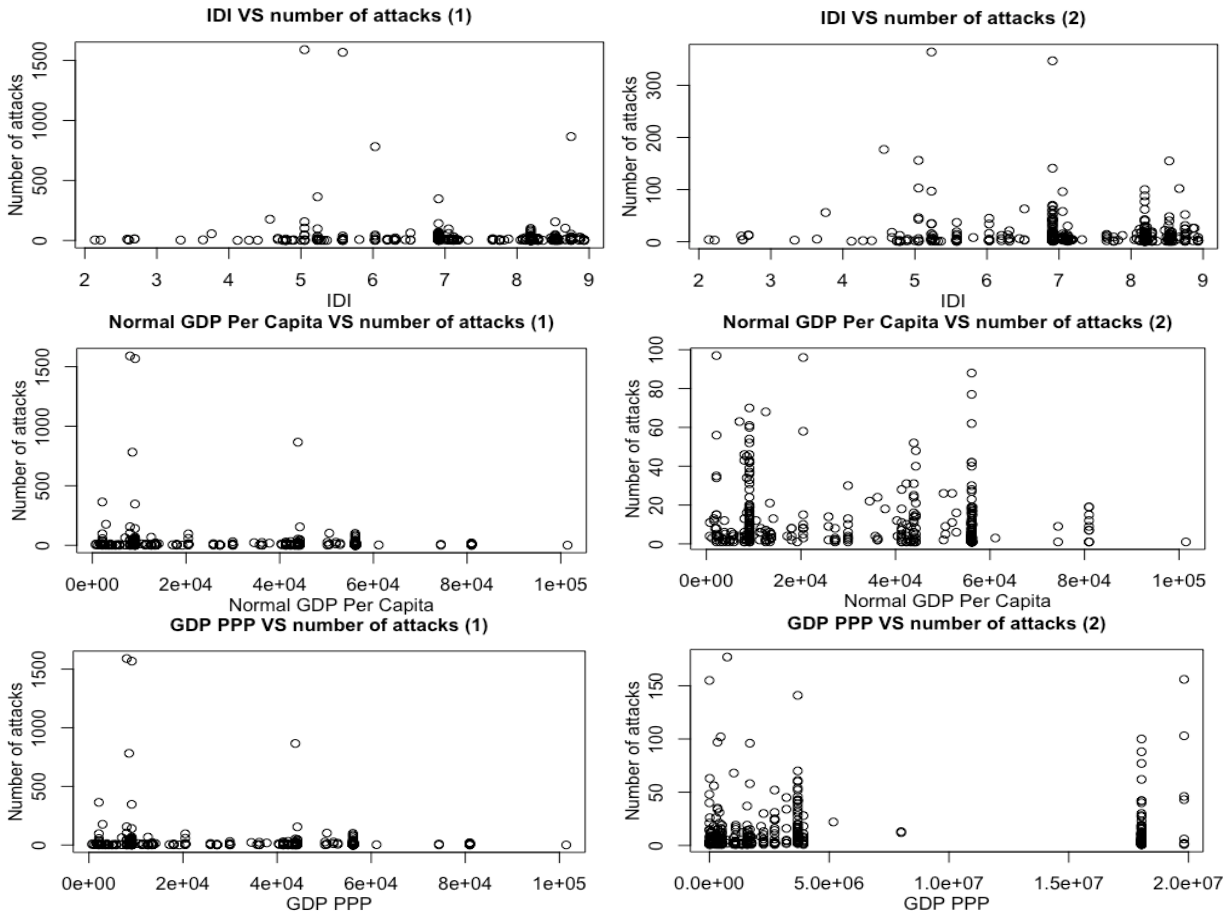

Figure 18: Scatter plots country-level factors

Linear regression country-level factors

In order to use linear regression, the independent variables needs to meet various assumptions. First of all, the relationship between the independent and the dependant (number of attacks) variables has to be linear. Looking back at the scatterplot, one can determine that there is indeed some sort of linearity between the independent and dependent variables. If the IDI, Nominal GDP Per Capita, or the GDP PPP increases, also the number of attacks increases. Second, the assumption of normality has to be met. In order to determine whether the data

meets the assumption of normality, a normality test was performed. The normality tests show that the factors do not meet the necessary assumptions. The results and explanation of the assumption test can be found in Appendix E.

To deal with the non-normal and heterogeneity of the data, there are a few mathematical transformations that can be applied. A frequently used transformation is the log function. However, in this case the generalized linear regression is used, as the log function did not normalize the independent variables. More specifically the negative binomial generalized linear regression is used.

Table 9: Negative binomial generalized regression country-level factors

	Dependent Variable:		
	Number of attacks		
	(1)	(2)	(3)
IDI (2014)		-0.329**	
		(0.053)	
Nominal GDP Per Capita (2014)			-0.00002***
			(0.00000)
Constant	3.280***	5.548***	3.928***
	(0.238)	(0.389)	(0.333)
Observations	406	404	397
Log Likelihood	-1,633.257	-1,607.337	-1,580.398
Theta	0.444*** (0.026)	0.475*** (0.029)	0.490*** (0.030)
Akaike Inf. Crit.	3,268.514	3,218.675	3,164.796
Note:			*p<0.1; **p<0.05; ***p<0.01

Table 9 shows a summary of the models used for the negative binomial generalized linear regression. $Model_1$ only includes the number of attacks. $Model_2$ adds the IDI as an additional factor, $model_3$ adds the Nominal GDP Per Capita, and $model_4$ adds both factors. The results show that individually the IDI and Nominal GDP Per Capita influence the number of attacks and thus the act as a target selection factor. $Model_2$ show that there is a significant effect of the IDI on the number of attacks (p-value is less than 0.01). Important to note is that this effect is negative. The effect can be interpreted as follows: while holding everything constant, if the IDI increases with 1 unit, the number of attacks decreases with e^(-0.3286) = 0.72. Due to the logarithmic scale of the variable, the e function is used. Thus, from this result the conclusion can be made that well-developed countries in terms of IDI are less frequently targeted than less ICT developed countries. One way of explaining this result is through the success rate of attacks. Organisations in well-developed countries are often well aware on cyber risks and cyber-attacks, thus making them less susceptible to successful attacks due to implemented mitigation strategies. In addition, if the success rate is low, then this demotivates attackers to launch an attack.

$Model_3$ can be interpreted in a similar fashion. Similar to the effect of the IDI does the Nominal GDP Per Capita influence the number of attacks negatively. If the Nominal GDP Per Capita changes by 1 unit (1$), the number of attacks decreases with approximately 1% (e^-2.434e-05=0.99). This finding shows that in if a country becomes more developed in terms of their Nominal GDP Per Capita, the number of attacks decreases. This finding fits the previous results and conclusions that organisations in well-developed countries are becoming less of a target. It seems that attackers do not focus their targets based on the overall economy of a country, or the purchasing power, but rather on the total economic wealth per citizen. Thus, it can be concluded that the countries with a high GDP (often large countries, due to their large amount of citizens) does not influence the target selection for FSOs. Rather, attackers look at the economy relatively to the amount of citizens. However, important to note is that the size of the effect is not large enough to make any strong claims.

Compared to the IDI, an increase in Nominal GDP Per Capita results in a more limited effect on the number of attacks. Both results illustrate a negative influence for the number of attacks. Worth mentioning is the fact that a change from 1 IDI is a relatively time consuming and involves large investments for the public and private sector (International Telecommunication Union (ITU), 2014). In general, the findings reveal that there are country-level factors that influence the number of attacks for FSOs, from which the IDI and the Nominal GDP Per Capita showed a statistical significant relation with the number of attacks. One way of explaining can be found using the bar plot in Figure 16. This bar plot shows that many semi-developing countries are being targeted frequently. This can be due to the fact that critical infrastructures in semi developing countries are still under a dominant ownership of the government. Researchers argue that the strict government intervention and regulation is not considered as a suitable option for cyber security by academia. A more privatized environment, which allows for cooperation, innovation, non-regulation, which is widely accepted by developed countries, is considered more appropriate for cyber security (Karabacak, Ozkan Yildirim, & Baykal, 2016). The factor GDP PPP showed no significant p-value and thus does not significantly influence the number of attacks. The table with the results of the generalized linear regression can be found in Appendix E (see Table 26). Due to the correlation between the IDI and Nominal GDP Per Capita they are not included in one model.

5.3.2 Explanatory analysis organisation size

The descriptive analysis shows that Fortune500 listed financial organisations are more attacked compared to non-Fortune500 listed organisations. The assumption is that more prominent financial organisations have a higher chance of being attacked. It was also made clear that the prominence of an organisation can be measured through size indicators. This section will dive deeper into those assumptions by analysing the influence of size indicators on the number of attacks.

Comparing Fortune500 VS non-Fortune500 organisations

To observe if there is a difference between the Fortune500 listed financial organisations and the non-Fortune financial organisations, a general analysis between the two groups will be conducted. To do so, the financial data was separated into Fortune500 listed organisations, and the non-Fortune500 organisations. To provide a visual representation of the difference between the two groups, strip plots were plotted (see Figure 19).

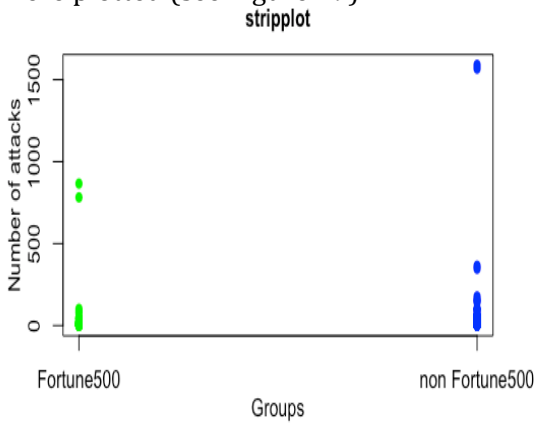

Figure 19: Strip plots Fortune500 VS non-Fortune500 against number of attacks

Figure 19 depicts the strip plot of the Fortune500 and non-Fortune500 groups against the number of attacks. At first glance, there seem to be no significant difference between the two groups as both show a similar pattern. In order to statistically proof there is a lack of difference; a student's t-test will be performed. The student's t-test provides a statistical proof of the differences between the dataset based on the means of both datasets. The results of the t-test

can be found in Table 10. The results demonstrate that the p-value of the t-test is 0.6126. Since this p-value is not significant (above the threshold of 0.05), the zero hypotheses can be rejected. Rejecting the hypothesis means that there is no significant difference between the Fortune dataset and the non-Fortune dataset. Thus, Fortune500 FSOs do not incur more DDoS attacks than non-Fortune500 FSOs.

Table 10: Student's t test number of attacks Fortune500 VS non-Fortune500

	t
T-value	0.50763
DF	129.25
P-value	0.6126
95% confidence interval:	
Lower	-23.00942
Upper	38.89150
Welch Two Sample t-test: Number of attacks (non-) Fortune500	

Finding patterns for the organisation size indicators

The previous analysis shows that Fortune500 organisations do not significantly differ in terms of numbers of attacks from non-Fortune500 organisations. As mentioned before, one of the possible explanations could be that also the non-Fortune500 organisations hold large organisations, which makes solely listed as a Fortune500 organisation not a good indicator for the organisation size. This section will provide a more thorough analysis of the size, using the size indicators mentioned in section 5.2.

To determine whether the number of owned IPs /domains per organisation can be used as size indicator, a scatterplot was conducted to see whether the IPs incur more attacks. The plot illustrated in Figure 20 shows that most of the financial organisations have little numbers of attacks per IP. Many IPs show similar results, which means that the owned IPs/domains does not show any influence on the number of attacks. The expectation is that FSOs do not have a lot of IPs/domains. For this reason, this variable would not be a good indicator for the size of the organisation.

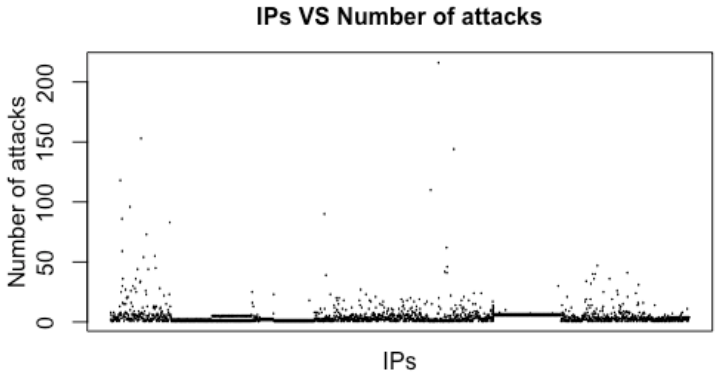

Figure 20: Scatterplot IPs VS Number of attacks

Similar scatterplots were plotted for the remaining indicator variables and the number of attacks to observe if there is a relation (see Figure 32 in Appendix E). The indicators profit, market value, and net income showed a clear pattern and will be analysed further. To understand the patterns more clearly, the scatterplots (see Figure 21) for the profits, market value, and net income have been plotted again without the outliers. In the plots it is evident that there are clustering patterns visible. Due to these patterns, it can be assumed that these indicators do influence the number of attacks. For the profits indicator, most organisations are

targeted if they have profits between $0 and $7,500 million, with most of the targeted organisations having a profit below $2,000 million. For market value, the same pattern is visible. Most organisations tend to be more attacked if they have a market value around 50,000 million. In terms of the net income, most organisations that have a net income below 5,000 are more targeted. The other three indicators (revenues, total assets, and number of employees) showed no pattern and will not be analysed further.

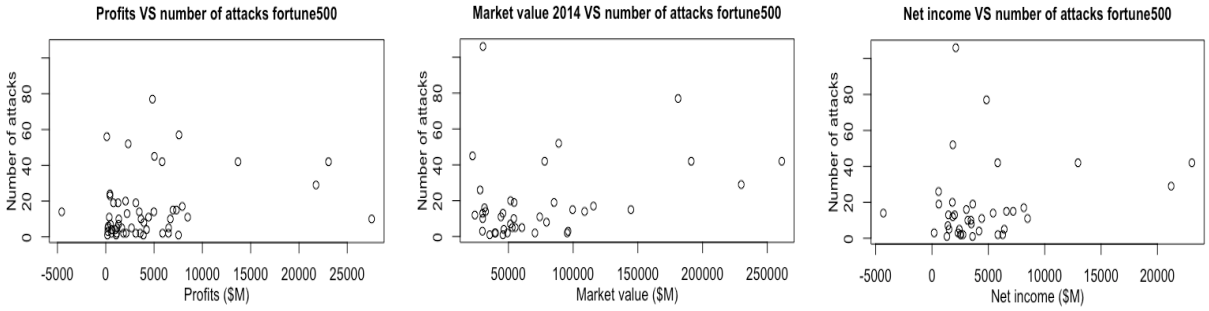

Figure 21: Scatterplots size indicators profits, market value and net income

Given these indicators, a more in-depth analysis will be done to understand the relation between these indicators and the number of attacks. In order to dive deeper into the patterns, the Fortune500 data is divided into two groups for each indicator (see table below). These groups are made according to the scatterplots where the clustered points are compared with the rest of the data points.

Table 11: Group classification

	Profits	Market value	Net income
Group1	< 5000	< 53000	< 50000
Group2	> 5000	> 53000	> 5000

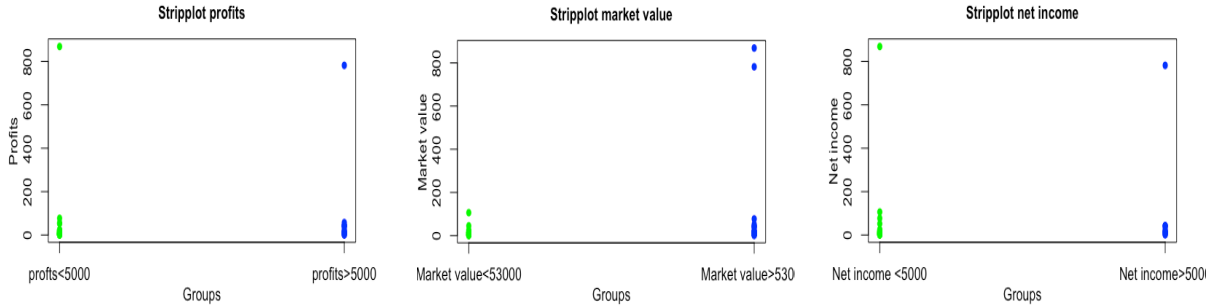

Figure 22: Organisation size indicators

To compare both the groups, strip plots and student's t-test were conducted. The strip plots above (see Figure 22), illustrates the differences the two groups have in terms of the number of attacks. These plots demonstrate that the profits indicator and the net income indicator do not have significant different patterns within their respective groups. For this reason, it is assumed that these indicators do not hold any substantial influence on the number of attacks. The market value, however, does show a substantial difference within its respective groups. Moreover, the student's t-test also showed a statistical significance (see Table 12). Hence, the two groups showed significant difference, which implies that there could be an underlying effect between the market value and the number of attacks.

Table 12: Student's t-test market value

	t
T-value	-1.5482
DF	21.46
P-value	0.1362
95% confidence interval:	
Lower	-184.73630
Upper	26.94539
Welch Two Sample t-test: Market value	

Linear Regression organisation size indicators

To understand the relationships between the market value and the number of attacks a linear regression analysis will be conducted. Similar to the country-level factors, the market value does not meet the assumptions for linear regression (see in in Appendix E). Again, to deal with the non-normal and heterogeneity of the data, the market value was transformed using the log transformation, but did not meet the assumption of linearity. Therefore, generalized linear regression was used again. Table 13 provides the results of the negative binomial generalized regression for the market value.

Table 13: Negative binomial generalized linear regression market value

	Dependent Variable:	
	Number of attacks	
	(1)	(2)
Market value (in $1000)		-0.002**
		(0.004)
Constant	3.745***	4.185***
	(0.186)	(0.413)
Observations	65	41
Log Likelihood	-291.971	-193.758
Theta	0.448*** (0.066)	0.417*** (0.076)
Akaike Inf. Crit.	585.942	391.516
Note:	*p<0.1; **p<0.05; ***p<0.01	

The table shows that there is a significant relation between the market value and the number of attacks of an organisation. If the market value increases with one unit ($1,000) then the number of attacks decreases with e^(-0.001894) = 0.99, which is a reduction of 1%. According to the analysis the market value is the only size indicator that influence the target selection of DDoS attacks, which begs the question whether size does indeed affect the number of attacks. In addition, while literature has shown that organisation size does matter for the attack rate, this result show that the size of the effect is not large enough to conclude that the size does influence the number of attacks. In the absence of more evidence, the assumption is that although size does affect the number of attacks statistically, there are secondary factors that are related to the size that could influence the target selection more directly. Chapter 6 will try to find factors that are more directly related to target selection with regard to the organisation size.

5.4 Conclusion AmpPot data analysis

SQ4: What are the proportions of FSOs in the AmpPot data?

The sensitivity analysis showed that almost half of the financial organisations could be found in the FFI database using the keywords. While this percentage seems low, one has to keep in mind

that all the remaining data were organisations that had individual names, which could not be mapped as financial solely based on their names. The literature states that FSOs are one of the main sectors that are being targets of DDoS attacks. However, after analysing and determining the FSOs in the AmpPot data, the proportion of the FSOs is relatively small. Only 10795 attacks are attacks on FSOs. This is 0.28% of the total dataset consists of FSOs. From the 1,114,787 unique IPs that were attacked, 2,210 (0.002%) are related to FSOs. In addition, the sensitivity analysis showed that 2.0% of the mapped FSOs are present in the attack data. Furthermore, the AmpPot data consists of 24,921 unique organisations, from which, 402 (0.016%) are financial. Thus, this shows that FSOs had relatively few attacks in the year 2014 and 2015. However, the data is based on individual attacks, and is not focused attacks on organisational level. Thus making it hard to compare, as also individual persons are present in the data. In addition, it is unclear how other sectors are proportioned to the total AmpPot data.

SQ5: Which factors are considered a threat according to the AmpPot data?

The financial dataset demonstrates that there are various factors that could be a threat for organisations. The descriptive analysis showed an interesting result regarding the day of the week. For FSOs there seems to be a significant increase in attacks on Fridays compared to the other weekdays. The amount of attacks was almost twice as much. Currently, there is no clear argument why this difference is that large. Moreover, this section provides various factors regarding organisation size, the context of the organisation, and the type of organisation, which are regarded important factors for target selection. This section reveals that among all the organisational factors, the market value is the only factor that influences the number of attacks, and thus relates to target selection. This effect, however, was extremely small. An increase of $1.000 would increase the amount of attacks with 1%. Therefore, no strong claims can be made based on this result. Thus, it remains the question whether size does actually influence the number of attacks. From this point on, the assumption is that other factors influence the target selection more directly than the size. On the other hand, the context of the organisation does influence the target selection. Country level factors such as the IDI and the Nominal GDP Per Capita show a stronger effect with the number of attacks. A specific argument for the IDI could be that in countries with lower IDIs the organisations are not technological advanced to incur DDoS attacks, while the more technological advanced countries are better at mitigation DDoS attacks, thus reducing the success rates of criminals. While the Nominal GDP Per Capita showed a more limited effect than the IDI, it can be argued that well-developed countries are aware of cyber risks and are also able to implement sophisticated, but expensive, mitigation techniques. However, this effect is also very limited thus no hard claims can be made as well.

SQ6: What are the characteristics of FSOs that are being attacked?

AmpPot does not provide any specific regarding the characteristics of the companies. Therefore based on the organisation names the characteristics have been determined. Organisations that have been attacked the most are the traditional banks such as Barclays and AKBANK TAS. In addition, many of those FSOs are listed in the Fortune500, which makes them prominent organisations and often large in size. However, as mentioned before, the size does not specifically correlate with the number of attacks. While most attacks are targeted at large organisations, there is no strong effect that the size does actually increase the number of attacks. Additional to the bank, also various investment groups are targeted frequently. Surprisingly, IT oriented FSOs are not well represented in the dataset. Only PayPal, which is the most known digital FSOs, is among the top organisations to be attacked. Furthermore, the most targeted FSOs do not particular reside in well-developed IT countries, but rather in semi-developed countries, such as China, Turkey, and Russia. These countries often are largely IT oriented but operate in a state owned environment, which is not suitable option for cyber security.

6. DDoS in the financial sector according to experts

To understand the importance of DDoS attacks in practice and the view of experts on this specific topic, various interviews were held. As qualitative data on the perspective of experts is hard to find, this section will be used in to compare the findings in section 7, as well as provide extended knowledge in this particular field. First, the interview set-up and the consulted experts will be discussed. Second, the factors that influence target selection according to literature will be provided. The third section describes the outcomes of the interviews. This part consists of the experts' general view of DDoS, the current development of the DDoS landscape, the financial sector versus other sectors, the attacker types, and the strategies used by FSOs to combat DDoS. Lastly, the factors that influence target selection according to the experts will be discussed.

6.1 Selection of respondents

For this research a mix of various experts were needed to give a complete overview of the thoughts of the sector on the target selection of DDoS attacks. As this research focuses on DDoS in the financial sector, solely respondents that are working, or have been working in the financial sector were consulted. In addition, these respondents had to have more than 5 years of experience in the cyber security or information security field with focus on DDoS attacks. Therefore, the respondents were selected based on their experience in the financial services sector and cyber security and considered experts. Furthermore, for a more diverse group, both respondents from big and small organisations have been contacted as well as, respondents that are more independent. These independent experts have not been directly involved in mitigation an attack, but have a more general knowledge on the DDoS landscape as a whole. Including independent respondents can lead to broader and new perspectives about the subject. These persons also tend to speak more freely. However, due to personal and client networks, experts from big and semi-big banks were mainly interviewed. These are also main targets of DDoS attacks and therefore a focus point in this research.

The respondents were contacted through various sources. First, the clients and personal network of EY employees were consulted. Second, the networks of the external supervisor were used. Thirdly, the professional and personal networks of academics from the Delft University of Technology were consulted in order to approach respondents with slightly different backgrounds. In the end, 9 respondents were gathered. The total number of respondents is the result of time constraints and the saturation point after the last two interviews. All the respondents have been contacted through e-mail. In addition, the experts have been consulted during face-to-face interviews or Skype, and e-mail communication afterwards. Due to the sensitivity of the data and the possibility of de-anonymization using cross-reference, all the data have been anonymised. Therefore, the names will not be mentioned in the research. Table 14 provides an overview of the respondents, their function and expertise level.

Table 14: Overview respondents, functions, and expertise

Code	Function	Expertise
[BA1]	Security officer manager	Banking
[BA2]	Information security manager	Banking
[BA3]	Security specialist	Banking
[BA4]	Security architect	Banking
[BA5]	Security specialist	Banking
[BA6]	Consultant	Banking
[IE1]	Consultant	Cyber software
[IE2]	Financial auditor	Financial services
[IE3]	Security specialist	Banking

6.2 Interviews structure

To understand the experts' view on the DDoS landscape, semi-structured interviews were held. The semi-structured approach gives the respondents the possibility to share their view more openly on the matter at hand, without steering them too much into one direction from the interviewer side.

The interview protocol has been designed to identify the current threat DDoS holds in the financial sector and the factors that could influence target selection of DDoS attacks that have been identified in section 4 and 5. The interview took approximately one hour. Prior to the interviews, the experts were notified on the subject of the interview, the goal of the interview, how the interview is related to the research, and provided with the main research questions. At the start of the actual interview, the general information about the interview was explained more elaborate. In addition, the interviews were asked if recording of the interview was allowed and validation of the answers happens through e-mail. Due to limitations of personal connections, the respondents were all experts who are currently working in the Netherlands, or have been working in the Netherlands. An overview of the general questions is provided in Table 15. The full interview protocol can be found in Appendix F.

Table 15: Interview protocol

Interview overview	
Concept	Questions
Introduction	• Introduction general background of research subject. • Explaining the goal of the interview. • Explaining the structure of the interview.
General questions	• What is your general viewpoint on DDoS attacks? • How often did you suffer from a DDoS attack in the last year? • What is your opinion about DDoS attack rates of other companies?
Specific questions	• Which mitigation strategies does your company use to defend against DDoS attacks, and how did they come into place? • What are according to you the types of cyber criminals that mainly try to attack your company? • What do you expect in regard the ease of use of launching a DDoS attacks? • What is your expectation on target selection of a cyber criminal?

6.3 Data analysis

In section 4.4, the various factors (see Table 3) that influence target selection have been described. For the qualitative analysis, the factors identified in the literature study will be used as a starting point.

6.3.1 Data structure

In order to analyse answer the research questions, the interviews need to be processed an analysed. As all interviews were conducted in person, they were firstly transcribed using notes and recordings during the interviews. Secondly, the gathered data was structured using a high level of coding, to assist in building theory around the provided answers. The first step in coding process was to highlight all the key elements that were related to DDoS and target selection of

DDoS of each interview. The second step consisted of finding differences and agreements among the interviews. In the last step, all the findings were combined in one of the themes (e.g. attacker types and mitigation strategies).

Based on the answers and coding, an assessment was done to understand the threat of DDoS and how target selection influence the threat. The first step in this assessment was to understand the current and future threats and developments of DDoS. Insight into the current and future threat landscape gives a broader perspective on the relevance of DDoS attacks for FSOs and thus also the factors influencing target selection. In the second step, the various attacker types were analysed. The attacker types are an important indicator of various target selection factors, as each attacker type has their own motives. The third step consisted of analysing the mitigation strategies of the FSOs to understand the current technical capabilities of defending against DDoS attacks. Insight in the current capabilities gives insight into the current and future threat DDoS has, and also is a factor that could influence target selection. The last step consisted analysing the factors for target selection. Based on these results, an overview of the current and future threat landscape of DDoS for FSOs can be determined. A visual representation of the themes discussed is given in Figure 23.

Figure 23: Overview interview themes

6.4 Experts' view on DDoS

6.4.1 General view on DDoS

[BA1, BA2, BA3, BA4, BA5, IE3] all discuss the importance DDoS has in the financial sector. According to them DDoS is still a big issue for FSOs as it has an impact on the continuity total organisation while for instance Malware and Phishing do not. Another reason is that DDoS mitigation is very costly and labour intensive. However, DDoS has become a commodity for most FSOs. It is, and has been part of the financial services sector for a significant amount of time. Hence, [BA2] adds "*the mitigation strategies financial organisations use, do not belong to the real security department, but are part of the operational department.*" This is in line with what [BA1] states: "*during an attack, banks have to kick-off some script and a select of operations to start the mitigation.*" In addition, not only have these mitigations been commodity, these mitigation strategies have turned out to be quite effective in practice [IE3]. FSOs are able to mitigate most attacks on their own and have to occasionally switch to an external mitigation party.

Similar to a software error DDoS leads to unavailability of services [BA4, BA5]. Therefore, DDoS is not part of the security department but part of the business continuity management department, even tough there is still as security component involved [BA3]. However, the difference between a software issue and DDoS attacks, is that you can often handle software errors internally, while DDoS attacks are always an external threat [BA4, BA5]. Hence, DDoS is

still seen as a big issue for FSOs. In addition, experts see that DDoS attacks are on the rise again [BA4, BA5, BA6, IE1, IE3], not only in terms of the amount, but also in terms of the power of the attacks. The experts expect the rise of the DDoS will increase even further due to the growth of Internet of Things (IoT) for both the amount as the intensity. As one [BA3] said: "Due to IoT, *the growth of DDoS shall increase both in terms of frequency and intensity. Through IoT devices, it is relatively easy to disrupt the data traffic with only 10.000 devices".* As this falls outside the scope of the research, it will not be looked into more detail.

However, according to [IE1], DDoS is the least important cyber-attack nowadays. [IE1] explained: "*due to the ease of access of DDoS, it is relatively easy to launch such an attack. Therefore, a lot of attackers are unsophisticated who do not have the intention of severely harming the financial organisation. A much bigger cyber threat is the issue of fraud schemes. Which can be used in combination with a DDoS attack, where the DDoS is used as distraction for the actual attack (e.g. stealing data, fraud). For financial services organisations the damages of fraud schemes are much higher than for DDoS".* The lower threat of DDoS can be explained by the fact that companies are currently much more protected against DDoS attacks. [IE1] Further explains:" *criminals need to have high-tech tools to seriously damage an organisation. While there is a continuous increase in DDoS attacks in the last couple of years, the average intensity of these attacks for financial organisations have not increased*". This shows that there are conflicting opinions about the threat of DDoS. While all banks consider DDoS as a severe threat, some individual experts do not.

6.4.2 Development of DDoS landscape

Despite the effectiveness of current mitigation strategies in the financial sector, DDoS will remain a significant problem for the future. The DDoS landscape is continuously changing according to all experts. This problem is stressed by [IE3]: "*recent media has shown that an old-fashioned volume attack can still have a significant impact*". In addition [BA6] has argued that: "*within 5 years there will be attacks with a power of 1,000-2,000 Gb/s. There will be a slight hick-up due to technical reasons, however this will be temporary"*. This quote shows that DDoS will stay a threat in the future, and could possibly become a bigger problem than it currently is. One of the most important reasons for the development of large DDoS is IoT. Experts note that due to the increase of IoT devices, it will spark the development of DDoS to a next level. These IoT devices often do not have adequate security measures, and the manufactures are not incentivised to focus on the security issues of these devices, thus leaving them vulnerable for infections [BA1, BA2, BA3, BA4, BA5, IE2]. Hence, according to [IE2] creating awareness for consumers to focus on security is an important aspect that can help in combatting DDoS attack. More importantly, manufactures should be incentivised to implement security in all their devices. As a consumer, whether the devices is susceptible for participating in DDoS attacks is not relevant. Therefore, governments should focus on legislation to enforce secure IoT devices.

The increasing threat is not only observed by the financial sector, but also by many other sectors. [IE3] said: *"the telecom sector observes an increase in the power of DDoS. They are worried about the slope of this growth, as a very large attack can impact the whole society"*. As the DDoS landscape is rapidly changing intelligence capacity is needed to detect new forms of DDoS in the threat landscape [BA2, BA4, B5, IE3]. According to [IE] a consequence of the changing landscape the specialist shift to the intelligence side.

Another development of DDoS is that fact that there are relatively few third parties that offer mitigation. While the current mitigation parties possess the necessary capacity to mitigate current DDoS attacks, it begs the question what will happen if there is too much data going all at once to a mitigation party. This can occur when multiple organisations that are supplied by the same mitigation party are being targeted. In such situations, the mitigation party should choose between their clients. [BA4] and [BA5] state that it is important to think about the next steps

that need to be taken in order to cope with the increasing threat of DDoS in the future. They state that if plan A were to have in-house mitigation, plan B would be external mitigation. Plan C should therefore be to discuss exclude certain areas or continents in times of attacks. Plan D would be to block traffic of certain access providers. Thus, implementing these plans would lead to mitigate on four different levels: internal, external, dynamic flows, network flows.

According to [IE3] another important way of combatting DDoS is to make spoofing more difficult. This can be done on ISP level. However, this would mean that ISP's should work together, which is not always possible. Cooperation would make it difficult to launch a DDoS attack anonymously. Additionally, disrupting the business model of leads to less booter websites, which would drastically reduce the amount of DDoS attacks. Also, forensic research is needed to find attacker types that are not focused on financial benefits. According to [IE3] forensic research would definitely help in catching attackers as stated in the following quote: *"forensic research would help in searching for attackers".* However, forensic research is not the core business of FSO and the tools to monitor threats are not always adequate, making forensic research more difficult [IE1].

6.4.3 Financial sector versus other sectors

The respondents of the large FSOs mentioned that they see DDoS attacks on a daily basis. Traditionally, the financial sector and the telecom sector are in the Netherlands the top sectors that are being targeted by DDoS attacks, or any other cyber-attack for that matter. The telecom sector is close to the network and thus has to deal with a lot of DDoS traffic. The telecom sector sees an increase in the power of DDoS attacks. Also for FSOs there is a continuous flow of DDoS attacks. Luckily, currently the banks claim to be able to mitigate most attacks [BA1, BA2, BA3, BA4, BA5, BA6]. As [BA1] said: "*Almost every time, from the time an attack started we are usually back online within 30-60 minutes".*

Financial services have traditionally always been a prominent target of cyber-attacks, but a shift of cyber-attack to other sectors can be observed. Nowadays, criminals are attacking all companies that possess some sort of data. Based on scientific research, in particular medium-sided organisations are expected to be an increasingly targeted in the upcoming years [BA6]. Nevertheless, as financial services are also capturing a lot of data, these organisations are still a priority of cyber criminals. Between the types of FSOs, there is no significant distinction. For example, there is no difference between a private bank, with a lot of wealthy customers, and a cooperative bank that have customers in all the social layers [IE1].

From a DDoS perspective, the literature and various reports shows that financial services are among the top sectors for DDoS attacks (Arbor Networks, 2015b; Nagurney, 2015; Pierrakis & Collins, 2013; Wueest, 2014). However, various experts note that the financial sector is not one of the most important sectors. [BA3] states: *"it is important to understand what one can achieve with a DDoS attack. For a financial organisation, a criminal is able to get money, since banks hold a lot of money."* In addition, FSOs are often known institutions, so to DDoS them would lead to a high impact. Yet, the financial services are not the most important sector compared to other sectors. For example, if a successful attack occurs in the energy sector the impact could be nation-wide. The education sector is another sector that is becoming an increasingly important target [IE3]. It appears that DDoS is an easy way for students to bail out of exams. Hence an increase in DDoS attacks during exam periods. Yet, the financial sector remains an important target for criminals. Hence, the financial sector has good inter-sectorial cooperation to combat cybercrime. It happens that criminals move from one bank to another bank, even geographically. To combat cybercrime, information sharing between the FSOs is a standard. For the financial sector, cooperation in so-called ISACs (information sharing analysis communities) is common practice. [IE3] said: "*The financial sector has also decided that that there is no competition on security, which makes information sharing possible".* With the previous quote, it

shows that FSOs take cyber security very seriously and understand the importance of working together to defend against attacks. Information sharing, reduces the uncertainty associated with cyber security investments and can as well result in reducing the tendency to underinvest in cyber security activities (L. A. Gordon, Loeb, Lucyshyn, & Zhou, 2015). While these ISACs are common among all vital sectors in the Netherlands, there is a difference in the maturity of each ISAC. [BA3, BA4, BA5, IE3] mention that both the telecom sector and the financial sector have a much higher maturity level than many other vital sectors. They also state that between the ISACs there is not much communication. "*There have been made small steps in direction to cooperation between ISACs, so they assume that this will be improved in the future*" [BA3]. This shows that in the future large DDoS can be mitigated inter-sectorial. This development could be extremely important when DDoS become so large that they influence various sectors such as the infrastructure of telecom providers and FSOs. On the other side, there is insufficient cooperation between governmental organisations and the private sector, for instance between the FSOs, telecom sector and the police. For example, even though it is mandatory to send a report to the police when a large DDoS attack happened, this does not lead to finding the attackers [BA1, BA3].

As FSOs have been an important target for criminals for many years, it shows that they have also been able to combat the cybercrime. The financial sector has passed the stage in which FSOs would go bankrupt due to DDoS attacks. The financial sector has also passed the stage that becoming victim of a DDoS attack which leads to a full day would costs millions. However, as services like online banking belong to the primary services, the impact of a DDoS attack is still high [IE3].

6.4.4 Attacker types

To understand the target selection of DDoS attackers, one has to understand what drives and motivates attackers to launch an attack [BA1, BA3]. In section 3.4 a quick grasp has been given on the possible motivations based on literature. This part will provide added information on the attacker types and their underlying motivation, based on the experts' view. For DDoS there are only a small amount of types of criminals, which were determined using logic and common sense [BA1, BA2, E1]. It is however, hard to determine what types criminals there actually are in the field due to the low catching percentage. This makes it difficult to sketch a profile of the actual types of criminals and their motives.

To understand a possible motivation, FSOs use various scenarios and compare the attack with the possible attacker types to trace back the motive. However, it is often impossible to understand actual motive based on only the attack [BA3]. To somewhat understand a possible motive, attacks are analysed to figure out the possible attacker type. It is possible to estimate the kind of attacker due to the patterns of an attack. The distinction of attackers is based on the patterns the criminal used to get into the system. An attack often results in so-called traces (breadcrumbs) that can be analysed [IE1]. The more professional criminal organisations often have a more specific goal (getting specific data) and this can be seen when analysing the data, while scriptkiddies often have no clue what to do when they got in. What happened before an attack is of importance? Did the attacker perform proper reconnaissance or did they just do some random things? If the attack had a high level of sophistication or used a Zero Day exploit (vulnerability is unknown to the market and the outside world), it is most likely that a government ordered the attack. These Zero Days can cost up to 1,500,000 (Zerodium, n.d.), hence are too expensive for various criminals [IE1]. The most frequently attacker types that were mentioned by the respondents are:

Scriptkiddies

Scriptkiddies are the most mentioned attacker type of during the interviews. According to the experts, these types of criminal are below the age of 30 with no specific goal in gaining any

serious assets from the targeted organisations [IE1]. These types of attackers are not the most technical persons and thus use relatively easy techniques or tools such as booter websites. On of the frequently mentioned motivation for scriptkiddies is the status that is gained from launching a successful DDoS attack. They focus on building their online resume among Internet (hacker) communities. These communities provide a sense of invincibility and status. The bigger the company that have been successfully targeted, the higher the status. While attacks originating form script kiddies are taken serious by organisations, they often hold no significant threat that would harm them. "One of the *biggest threat for FSOs is scriptkiddies in terms of the amount of attacks. However, for smaller organisations these impose no threat"* [BA2].

Another motivation for them might be solely the possibility to attack, with no obvious reason. This motivation will be discussed in more detail in the next section. Another possible motivation is the fun of targeting organisations. These two motivations can all be related to the low costs of launching DDoS attacks. Experts argue that due to the low costs, there is not much motivation needed to launch an attack [BA4], [BA5]. Next to the low costs, another reason might be the change of getting caught. As most of the attackers have not been caught, getting caught is close to zero. This can also motivate scriptkiddies to launch an attack. The motivation of script kiddies can be separated into three parts: (1) what are the costs? (2) What do I get from it and (3) what are the risks? If the risk of getting caught is almost zero, it is just a small step to actually launch an attack [BA4, BA5]. Increasing the change of getting caught would according to experts [BA1, BA3, BA4, BA5, IE3] significant decrease the current amount of DDoS attacks targeting FSOs. However, not all experts are convinced scriptkiddies target organisations just for fun. [BA6] argues that there are at most some that target institutions. Most of the scriptkiddies will be more active in the gaming industry.

Traditional cyber criminals

Even though most of the cyber criminals are script kiddies, approximately 9 out of 10, a small percentage is imposing a severe threat. These more serious criminal organisations often have more resources to harm the company or gain a financial advantage (e.g. stealing valuable data). These criminal organisations are often also active on the dark web, by providing hacking on demand [IE1]. DDoS attacks that are related to gaining financial profit is currently limited to only DDoS extortion. Another possibility might be to use DDoS as distraction. However, in the case of DDoS extortion, large FSOs have only seen this once. In the case of DDoS as a distraction, this has not happened yet [BA1, BA4, BA5]. Experts note that in order to gain a financial profit, it is more effective to use other cyber-attacks such as Malware, Phishing, or crypto lockers [BA3, IE2]. These attacks also have less impact and thus are harder to detect by organisations.

Activist / hacktivist

Next to the traditional cyber criminals and scriptkiddies there is also a small part that act according to an ideological belief [IE1]. Experts see these hacktivists as the most significant threat to FSOs. These actors are the ones that possess the technical knowledge as the resources to launch a DDoS attack with impact. [BA3] argues that these actors impose the most threat to large organisations that are often in the media. "*Hacktivists are the most significant threat to banks. A large bank will be a suitable target for hacktivists because these banks often do risky investments*"[BA3]. In addition, large organisations also have the investment portfolio to invest in riskier businesses. As long as the hacktivist can connect your organisation to something that they dislike (risky investments, redundancies), then the incentive to attack your organisation is present.

Others

In addition, to the three types of actors above, there are some noteworthy types that have also been mentioned.

Nation state – There is a possibility that state actors also target various organisations. One of the motives might be because of the shares a government hold shares and thus have a high interest in a number of companies or to distort the financial system [BA1, BA2, BA3, IE1, IE3]
Competitors – competitors might launch DDoS attacks in order to influence the stock price for a hostile takeover, or to affect the reputation of a competitor BA1, BA2, BA4, BA4, IE1].

An overview of all the attacker types mentioned during the interviews is given below

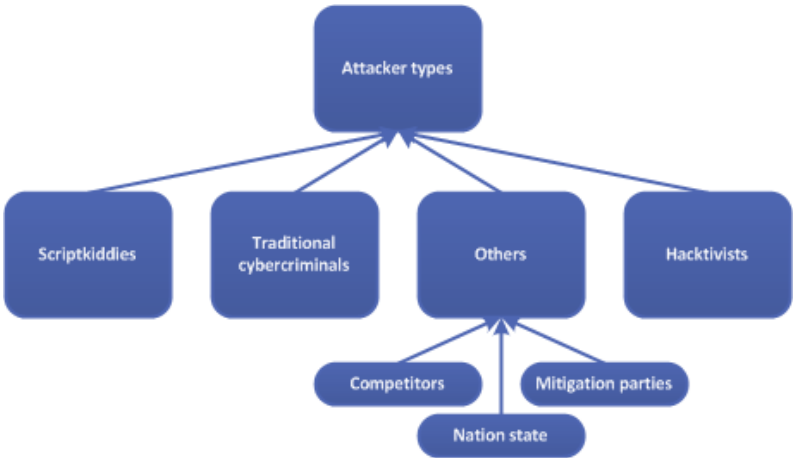

Figure 24: Overview attacker types

DDoS mitigation parties – As mitigation parties profiting from DDoS attacks, a more unorthodox thinking is that mitigation parties launch attacks in order to show the significance of having a mitigation party. This discussion also happened with the antivirus providers. While this is possible in practice, this motivation has never been proven, similar to the motivation of competitors and nation states [BA4, BA5].

While the motivation might be interesting from a scientific perspective, for FSOs the motivation is not important. As it is relatively easy to launch an attack, there could be 1000 of motivations. It is not worthwhile to focus on a couple of specific motivations and remove them. In addition, finding the motivation is not the core business of FSOs and thus they are not willing to really look into it [BA3, BA4, BA5].

6.4.5 Strategies tackling DDoS

To mitigate a DDoS attack, FSOs use both internal as well as external mitigation strategies, which are operational 24/7. The external mitigation is done through a mitigation party that provides defence services in DDoS attacks and ensures that the organisation will remain operation during an attack. In that sense, an external mitigation party can be seen as insurance in terms of large DDoS attacks that are outside the infrastructural capacity of the organisation. If an organisation detects a DDoS attack, and the attack is deemed (too) large, the company redirects (automatically or manually) the traffic to the mitigation party. In order to redirect the traffic to the mitigation party, the technique of spoofing is used. The mitigation party in turns scrubs the traffic and sends all legitimate traffic back to the organisation [BA1, BA3, BA4, BA5, BA6, IE3]. Currently, these procedures are relatively standard. Despite this strategy, customers will notice for a short time that the servers are not responding. Especially when the client base is large, there are bound to be a number of customers that have suffered from the consequences from the attack [BA1, BA3, BA4, BA5]. Internal mitigation is done using the organisations' own infrastructure and is focused on small attacks, application attacks and/or HTTPS attacks. These are necessary, since third parties are not allowed to look into the traffic of their clients. *"In the Netherlands there are regulations regarding the 7th layer of the OSI model due to privacy reasons"*

[IE3]. Hence, external parties are able to mitigate application attacks. This means that redirecting these attacks would result in encrypted data. According to [BA3], the main reason a structure using internal and external mitigation is the costs. It is far too costly to scale up the bandwidth of the company. In addition, for the FSOs that have been interviewed, they already have a disproportional large bandwidth that is able to handle five times the peak load. For FSOs that have not been interviewed, no conclusion can be made.

Acquiring and implementing of DDoS mitigation tools and strategies is not sufficient for effectiveness. An essential part is to test the mitigation. Testing in this case means regularly simulating a DDoS attack scenario on a level that internal and external mitigation is needed. Even though [BA4, BA5] emphasizes the importance of simulated testing, not all organisations adopt this methodology. These organisations only switch to the mitigation and back. The essential parts of detecting and anticipating on DDoS are not included. Since protection can never be guaranteed, a great emphasis on detection and reaction should be placed. This should increase the chance that an organisation detects a security breach and know the to taken actions (Schneier, 2011). In addition, DDoS waste various resources (e.g., processing time, space etc.) on paths that lead to targeted machine. Hence, the goal of DDoS dense is to detect them as soon as possible and to stop them as near as possible to their source (Jin & Yeung, 2004; Zargar et al., 2013).

While almost all banks and payment service providers (PSP) use this mitigation structure in the Netherlands, there are still various organisations that do not have a strategy to mitigate DDoS attacks. One important reason is the risk of being targeted by criminals [BA2, IE2]. For these organisations the threat of DDoS is not significant as for instance Ransomware or Malware. These organisations often do not provide online services or these services are not part of their core business. Thus, the impact of a DDoS will be limited as core activities can still be continued. Taking these factors into account, the costs of DDoS mitigation do not outweigh the benefits [BA2]. For them having mitigation tools will be important due to digitalisation of their services in the future. They assume that by that time, the mitigation tools have been developed sufficiently and are less costly.

These strategies have all been established due to the high possibility of being targeted. For many of the FSOs, these strategies were implemented after a large DDoS attack or during the process of implementing the strategy [BA3, BA4, BA5]. The first DDoS attacks resulted in a significant downtime before they were successfully mitigated. After these attacks, the FSOs have decided that such a long down-time due to DDoS was could not happen in the future. Thus, implementing internal and external mitigation. "*Until now, these mitigation strategies have been successful, as there has not been a long downtime due to DDoS anymore"*[BA6]. This quote shows that all FSOs are capable of defending against current DDoS attacks and do so successfully. Additionally, all FSOs have successfully been able to mitigate the smaller attacks internally as well [BA2, BA4, BA5, IE2].

While the amount of stopped DDoS attacks is increasing, and the amount of successful attacks is not significantly increasing, some argue the success of these strategies nevertheless. According to [IE1] it is not clear whether these strategies are really successful in a sense that the more sophisticated DDoS attacks can still severely harm an organisation. Organisations currently take DDoS more seriously and spend an increasing amount of time on cyber security, especially in the current times where reputation is important.

6.5 Target selection factors for FSOs

This section will provide the factors that influence target selection according to the respondents. During the interviews many factors have been mentioned. These factors can be

categorised as the characteristics a FSO has that will incentivise a specific attacker to launch a DDoS attack.

6.5.1 Randomly (target selection without pre-selection)

During the interviews, various experts discussed the fact that not always a clear factor was at hand to attack an organisation. This was also due to the fact that it still very unclear why FSOs are targeted outside the obvious motivations (extortion, online statement). This part will describe the factors that are related to the characteristics of organisations.

Intrinsic motivation

One of the most mentioned factors regarding target selection of DDoS can be summarised as the intrinsic motivation that an attacker holds, or as hackers would call it, "for the lolz" [IE2]. Which means for fun. To get a better understanding of this factor, one has to understand the meaning of intrinsic motivation. According to Deci & Ryan (2000) Intrinsic motivation is defined as: "*doing of an activity for its inherent satisfaction rather than for some separable consequence".* When intrinsically motivated, a person is moved to act for the fun or challenge entailed rather than because of external products, pressures, or rewards. According to [BA4] and [BA5], the intrinsic value of fun is possible due to the ease of access to DDoS-as-a-service as well as the ease of building a powerful infrastructure. As previously mentioned these attacks are originating from scriptkiddies that have no specific target or have a specific business case.

[BA6] does not share the same opinion as [BA4] and [BA5]. According to [BA6], an attack happens based on a specific business case (financial benefit, personal resentment, status, competition, diplomacy) rather than just for fun. "*There should be a specific motivation to attack an institution. This could be: money, personal resentment, social status, competition or diplomacy. Based on these factors a criminal would attack*". The attacker should always know who the target is, and how the chance of getting caught can be limited.

6.5.2 Target selection with pre-selection

While according to [IE1] randomly selected targets play a significant role in the DDoS attack landscape, also attacks based on pre-selection can be thought of. Some of the experts argue that some criminals carefully select their target based on various factors of FSOs. This section will provide the mostly mentioned factors, that experts deemed as important for target selection on FSOs specifically.

Organisation size

The size of a FSO is a common factor of an organisation to be targeted. According to [BA2, BA3, IE1, IE3]. The larger the bank, the more often you get attacked. One of the biggest motivations for attackers is to show-off their capability, according to Arbor Networks (2015a), showing of their attack capabilities was the number one motivation for cyber criminals. Logically, large FSOs are best to show that in terms on how well their DDoS attack is designed and what their impact is. The larger the attack on a big company, the more attention it gets. Size can be expressed by many factors such as net profit, total assets, total payments, number of clients etc. (Moorsel, 2016). As DDoS impacts the services provided by the FSOs, the number of clients is an important factor in terms of size of a FSO, and was therefore also frequently mentioned as a factor. The differences in attack frequency were also confirmed in terms of the amount of attacks a certain FSO got. The larger the FSOs, the more frequent they were attacked (daily basis) while the smaller FSOs had a significantly lower attack rate [BA4, BA5]. *"Large FSOs experience DDoS attacks everyday. However, due to the mitigation strategies, large FSOs are not affect by the attacks"* [BA4].

Reputation

Another factor that was often mentioned is the reputation of the organisation. In this regard, having a bad reputation or brought to bad daylight by for instance the media, plays an important role in being seen as a target for attackers [BA1, BA2, IE1, IE3]. According to [IE3] a bank often does not hold a good reputation, certainly in the present days due to lots of automation in this sector, which leads to a higher dismissal rate. During a period of dismissal, organisations take into account that there is a slight increased risk of more DDoS attacks, either by former employees, or hacktivist [BA4, BA5, IE3]. One of the factors that influence the reputation is the investment portfolio or corporate social responsibility. "*Corporate social responsibility is an factor that is of great importance for target selection. This factor will definitely influence target selection"*[BA2]. A clear example can be given by organisations that cooperating various arms manufacturers or regimes that do not align with the ideological beliefs of the attacker [BA3]. For banks this is an eminent problem, as most banks invest in certain projects, and thus have to be careful in selecting the project. According to [BA3] banks should focus on the levels on which they are able to change the risks of being targeted. The previously mentioned size is a difficult factor to alter. Therefore, focussing on the reputation is more important to decrease the risks of being targeted. Various experts share this opinion [BA4, BA5, IE1, IE2] and believe that for instance the investment portfolio should be managed also in terms of risk management, in practice this does not happen.

Media attention

Closely related to reputation is the media attention a FSO gets. From the respondents, it can be concluded that the media plays an important role in the target selection of DDoS attacks, it is among the top mentioned factors [BA3, BA4, BA5, IE1, IE2]. If a FSO has been visualized negatively in the media, they are bound to be attacker more often according to the experts [BA3, BA4, BA5, IE2, IE3]. Some even argue that during high media attention, the amount of DDoS attacks rises. *"What is often seen in practice is that if a company has a lot of exposure in the media, the amount of cyber-attacks also increases. So there is definitely a correlation between the media exposure and the amount of attacks a company has to endure"* [IE1]. In addition, various experts have discussed that it does not matter whether the media attention is negative or positive [IE1, IE2, BA2]. The sole thing that counts was if the FSO was mentioned in the media frequently during a period. According to these experts, FSOs are targeted based on their exposure due to the fact that attackers are looking for just a target, rather than a specific target. Therefore, the attacker will unwittingly think of the frequently exposed FSOs and used that as a target. Additionally, after successfully mitigated a DDoS attack, bragging about the success of mitigating also leads to extra attention for attackers. As previously mentioned, a motivation of criminals launch a DDoS attack, is to become part of a cyber community and to gain a high status. Showing off how 'good' you are at defending against DDoS, incentivise cyber criminals in targeting you as a company. However, not all experts share the same opinion [BA1]. According to some there have not been an increase in DDoS attacks during a period of increased media attention.

Patching/updates

According to [BA4, BA5], application DDoS attacks are one of the most troublesome attacks there are. With a relatively cheap and small attack it is possible to have a high impact. In addition, these attacks blend into the regular data flows and are thus hard to detect. Therefore, criminals are eager to find various exploits within the infrastructure of FSOs. Scanning the system is relatively easy as one can just perform an automated scan and wait for it to find an exploit. Naturally, finding an exploit does not happen on a regular basis. However, exploits are being sold on the black market. Most of the vulnerabilities are known, in a number of cases it happens that these are unknown, the Zero days. Patching and updates are thus an important factor to take into account when thinking of target selection of DDoS attacks [BA1. BA6, IE1, IE2]. Therefore, it is important to update and patch software swiftly. For large FSOs the rule is to patch instantly if possible, if the criticality is high. If within the security operation centre

(SOC) an exploit is detected, there are contingency procedures to patch the exploit [BA1]. However, [IE2] argues that this is not often the case. " *A company takes on average 60 days before a patch is actually implemented. Companies are not often eager to implement the patch instantly as there is a lot of uncertainty about the effect on the total system".* The statement by [IE2] shows that there are conflicting arguments about how organisation should and actually do their updates and patching.

Third parties

Organisations often make use of third party software, making them dependent on those third party software providers. This factor is almost similar to the patching factor. All companies use software of third parties. Software companies are obliged to mention their threats and data leakages. Publicly mentioning the vulnerabilities in your software gives free game to cyber criminals [IE1]. In addition software suppliers are not always completely focused on the security of their software, while they claim to be. They focus more on the user friendliness and the costs of the product, which not always go well together with security [IE2]. In addition to third party software, almost all FSOs have an external mitigation party to mitigate large volume DDoS attacks, having a capable guardian that protects the company can be a factor that influence the target selection. If an organisation does not have mitigation tools or strategy then it easy for criminals to launch a successful DDoS attack [IE2].

Internal expertise

While the external factors are leading to the most attacks, these factors are often outside the scope of a company and therefore cannot be helped. To combat DDoS attacks, there should be measures on both technical and socio-technical level. While DDoS is a technical attack, the human aspect plays an important role. To detect and mitigate a DDoS, experts are needed. These experts should also be able to prevent DDoS attacks, and detect new DDoS threats. They should understand the total landscape and the new measures to tackle the new threats. Thus, in-house experts who are continuously scanning the threat landscape for new threats should be part of an organisation [IE2]. This is an important aspect, as successful attacks can lead to more future attacks if the organisation was not capable in mitigation the attack. Therefore, attackers will think that to indulge the most impact, a vulnerable organisation should be targeted [IE1].

Location/country

[BA3] states that the biggest threat for FSOs are the hacktivist and the scriptkiddies. Therefore, smaller banks are of less interest for cybercriminals. This aspect can also be related to the specific country the FSO operates. If a country has a lot of online services, they are more susceptible for getting attacked. This is due to the fact that certain countries are technological advanced. Attacks that are successful in countries with large and fast digital economies will also be successful in other countries. Another factor that is related to a country is the GDP; some experts argue that the GDP of the home country of the FSO plays a part in the DDoS attacks. This can be explained as countries with high GDP often also have a high IDI and thus are susceptible for more attacked.

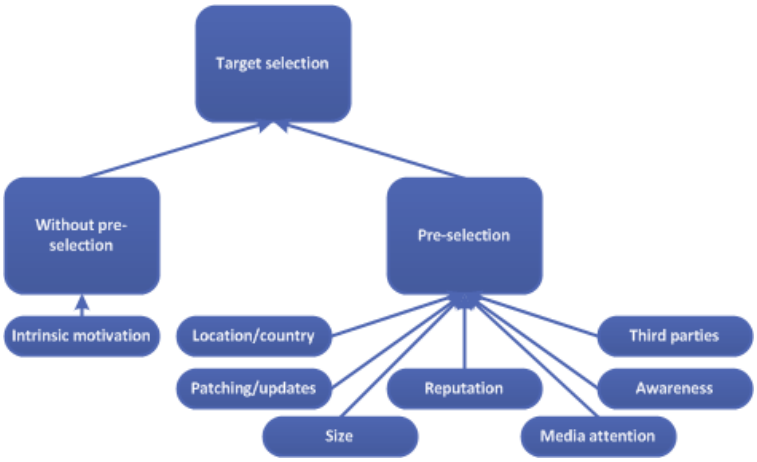

Figure 25: Overview target selection factors according to experts

An overview of the factors and by whom they are mentioned is given below (see Table 16). The "X" stands for a factor that influence target selection according to the expert, while an "-" stands for a factor that does not influence target selection according to the expert.

Table 16: Target selection factors according to experts

	Codes								
Factors	**BA1**	**BA2**	**BA3**	**BA4**	**BA5**	**BA6**	**IE1**	**IE2**	**IE3**
3rd party		X					X	X	
Affinity							X		
Bragging							X		X
Internal expertise							-	X	
Intrinsic		X		X	X	-			
Location		X	X						
Media	-		X	X	X		X	X	
Patching	X			X	X	X	X	X	
Reputation	X	X	X	X	X	X	X	X	X
Size	X	X	X	X	X				X
Strategy		X						X	
Client type			-				-		

6.6 Conclusion interview analysis

While the previous section focuses on the factors that influence target selection according to the AmpPot data, this section discusses target selection in the perspective of various experts. These insights are necessary for the next section where both lessons learned from the previous and this section will be brought together. Three sub-questions were devised to understand the target selection from a field perspective:

SQ7: How has the threat of DDoS amplification attacks affected victims in FSOs?

DDoS remains a big issue for FSOs, as the impact of an attack can lead to long downtime and thus harm the organisation. However, in today's society, DDoS has become a commodity threat for most FSOs. Most attacks do not lead to any significant downtime and DDoS has moved from the security department to the business continuity departments. For attackers DDoS has also become a commodity leading to disproportional costs, as the attacks can easily launch an attack with little resources. On the defender side, DDoS mitigation is costly and labour intensive. Furthermore, experts expect that the threat of DDoS will increase in the upcoming future. They

state that the current DDoS attacks are a small compared to future attacks in terms of the amount and power. Current mitigation techniques will fall short if the rise of DDoS will increase at its current pace. Threat Intelligence capacity is needed to analyse the changes in the DDoS landscape leading to specialist shift to the intelligence side instead of the mitigation side. However, not all agree on the fact that DDoS is a significant issue for FSOs. While the impact may be high, most attacks are unsophisticated and easy to mitigate with occasionally large attacks that can be mitigated using external parties. In addition, while there is a continuous increase in DDoS attacks in the last couple of years, the average intensity of these attacks for FSOs have not increased.

SQ8: What are the current practices to defend against DDoS attacks?

To defend against DDoS most FSOs use the same structure. This structure comprises of both internal and external mitigation techniques. External is necessary for large volume attacks, which exceed the bandwidth of the organisation. In addition, purchasing the service from an external party is far more cost efficient than having internal mitigation for large volume DDoS attacks. Furthermore, FSOs already have more bandwidth than necessary and large DDoS attacks are very limited. Internal is necessary to cope with application and HTTPS attacks as external parties are not allowed to see detailed information in the 7th layer of the OSI model. Currently these techniques are standard due to the daily DDoS attacks large FSOs have to deal with. Since the large attacks on various banks in 2012, most of the FSOs have implemented this structure to prevent future downtime. An important aspect in effectively mitigation is to also test on various scenarios, which includes DDoS detection and anticipating on attacks. These scenarios focus mainly on the type of attack and the intensity and mitigating, understanding the motivation of the attacker falls outside the scope of the FSOs. In addition, finding the attacker is a big issue for the police force. For future attacks, only internal and external mitigation strategies are not sufficient. To cope with the future threats, FSOs should include dynamic flow mitigation and network flow mitigation. In addition, to deal with the spoofing issue, ISPs should cooperate more closely to complicate spoofing in the future. Furthermore, forensic research is key to catch the attackers, thus cooperation with the police force is necessary. However, these strategies require cooperation with other sectors and are still a far way from being operational.

SQ9: What factors do attackers focus on in selecting a suitable target according to experts?

Based on the interviews, the factors of target selection can be separated into randomly selected targets and pre-selected targets. Most important in this regard, is what the specific motivation is of the attacker. As mentioned by various experts, the motivation is the underlying cause on how an attacker chooses their target. However, as of now, it is very unclear what the frequent attack motivations are due to the inability to catch attackers.

For randomly selection, the intrinsic motivation plays a significant role. In this regard, the aspect of fun is a factor that influences attackers to target an organisation. This factor is possible due to the ease of access that DDoS-as-a-Service provides. However, some experts note that an attack on a FSO have to have a certain business case. They do not believe in the fact that FSOs are attacked based on fun. For FSOs the factors that are for pre-selection are more important as they can influence these factors. While there can be argued for many factors, the ones that have been mentioned most frequent have been discussed in this section. 1) The size of the organisation is an important factor as a successful attack on a large firm can increase status of a criminal. 2) The reputation of an organisation is extremely important for hacktivist. A bad reputation or bad investment can lead to a significant increase in DDoS attacks as punishment for bad social corporate responsibility or a wave of dismissal. 3) The media can spark the thought of a criminal to launch an attack. Solely bad media attention does not lead to more attacks per se. Some experts indicate that also positive media attention can lead to an increase in attack. 4) If an organisation is not able to sufficiently patch/update their systems, criminals

can use these exploits to launch an attack. Application attacks use these kinds of exploits and can harm more damage than an old-fashioned volume attack. Additionally, application attacks are hard to detect as they blend in the normal data flow. 5) Having a capable guardian can reduce the amount of downtime can decrease the amount of attacks. Therefore, most FSOs also use third parties to mitigate large volume attacks. There is also a risk in having a third parties, for instance when using an operation system. These parties are often obliged to let certain errors in their systems know to the public. Criminals can make use of these publicly known errors (similar to the patching/update problem). 6) The employees are still the primary vulnerability for a company. Having capable employees is a definite must to successful mitigate a DDoS attack. 7) The location/country can influence DDoS attacks, as attacks in technological developed countries are most likely successful in les technical developed countries.

7. Comparison quantitative and qualitative analysis

In this section, the results of the quantitative and qualitative analysis presented in the previous sections are contrasted. Since both analyses provide different oriented perspectives, this section provides insight into how both analyses complement each other. Firstly, an overview of the consistencies and inconsistencies between the quantitative and qualitative analysis is presented, followed by a discussion of the comparison. Secondly, both analyses are put next to each other to give insight into the domains the analyses could complement each other. Finally, the conclusion of this section will be drawn through answering the sub-questions of research question four. what are the similarities between the two sources? What are the differences between the two sources? How can the previous findings be complemented to each other?

7.1 Consistencies and inconsistencies

Table 17 and Table 18 give an overview of the consistencies and the inconsistencies from the quantitative and qualitative analysis.

Table 17: Consistencies of quantitative and qualitative analysis

Consistencies			
Domain	Quantitative analysis	Qualitative analysis	Limitations
Location/country	The AmpPot data shows that the location of the FSO matters. As IDI and the Nominal GDP Per Capita does influence target selection.	The experts mentioned that the GDP influence target selection, as these countries often have a higher IDI.	Only experts were interviewed in the Netherlands. They did not have insights into cross-country effects.
Organisation size	The linear regression reveals that the Market value is an important indicator for the number of attacks.	The experts mentioned that the large banks are more prone to be targeted, and are more targeted than the smaller banks.	The experts did not mention the attack rate of organisations that were not banks.
Recognised organisation	Recognized organisations seem to be targeted more frequently than others.	According to the experts are well-known companies attacked more frequently than unknown.	

Table 18: Inconsistencies of quantitative and qualitative analysis

Inconsistencies			
Domain	Quantitative analysis	Qualitative analysis	Limitations
Location/Country	The AmpPot data showed that an increase in the country-level factors, reduces the number of attacks	According to the experts does a high IDI and GDP leads to more DDoS attacks,	
Organisation size	Size is only weakly affecting the number of	The experts mentioned that size	Size could only be measured for

	attacks. Therefore, the correlation between size and target selection can be questioned.	increases the target selection.	Fortune500 data, as size indicators were not available for non-Fortune500 listed organisations.
Type of organisation	The quantitative data shows that mostly banks and investment groups are being targeted.	While banks are also in the top lists of targeted, the experts mentioned that all sorts of organisations that have online services are being targeted.	Interview mainly focused on the banking sector

7.1.1 Location/country

Both the AmpPot data and the experts agree on the fact that the location of the target is of influence for the number of attacks. The data shows that there is a statistical significant correlation between the IDI and the Nominal GDP Per Capita on the number of attacks. The experts agree on the fact that country-level factors play an important role for target selection. According to the expert leads a higher GDP and IDI lead to more risk of being targeted, due to more technological advancement and more exposure on the Internet. The quantitative analysis, however, showed a different result. The statistical analysis showed that an increase in IDI and Normal GDP Per Capita reduces the amount of attacks, and thus influence the attacker negatively.

7.1.2 Type of organisation

The AmpPot data revealed that most attacked FSOs are banks. From the experts' perspective, they mentioned that banks are historically being targeted frequently by cyber-attacks. However, there is a shift visible that also other organisations, in the financial and in other sectors are being attacked more frequently. This shift is not visible in the AmpPot data. One possible explanation is that the data is out-dated (2014-2015), which means that only recently (last 2 years) also other FSOs are being targeted, such as insurance companies.

7.1.3 Organisation size

The data analysis as well as the interviews showed that size of an organisation is an important factor that influences the target selection. According to the AmpPot data, is especially the market value is correlated with the number of attacks. The respondents mentioned that especially large banks with many clients are getting attacked more often than smaller sized banks. However, the AmpPot data also revealed that although the there is an effect between the market value and the number of attacks, this effect was very limited. In addition, the other factors such as number of employees, revenue, net income, assets, and profits did not have an influence on the number of attacks. Therefore, it is not clear whether the size of influences the target selection or that there are other variables that are related to the size that influence the number of attacks.

7.1.4 Recognized organisation

As most of the top 10 frequently targeted FSOs are listed in the Forutune500, these organisations are well known. From this can be concluded that most recognized companies are attacked more often. Also the experts mentioned that a well-known organisation is attacked

more frequently, as they indulge more media attention when a DDoS attack was successfully performed on the organisation.

7.2 Complementariness

As the AmpPot data do not provide organizational data, these data were gathered from the interviews. In addition, the AmpPot revealed various interesting insights, which were not mentioned during the interviews or the other way around. Therefore, this section will provide an overview of the factors that complement each other. Factors mentioned during the qualitative analysis such as intrinsic motivation, internal expertise, third parties, patching/updates, client type, could not be gathered from the AmpPot data. It can be stated that these factors are complementary to the AmpPot data. However, these factors operate on a level, which could not be analysed with the AmpPot data. Therefore, no additional comparison can be made based on these the results of the qualitative and quantitative data.

7.2.1 Quantitative analysis

The quantitative analysis showed that the number of attacks per weekday differs relatively to the total dataset. Especially on Friday the attacks were extremely high compared to the other weekdays. Although this is a factor that cannot be influenced by any organisation, the organisations can change their internal mitigation strategies to be more alert on Fridays. However, the experts did not mention that the weekday was an influential factor for target selection. When asked about the weekday as a targeting factor, some mention that they did not see a big difference between each of the weekday. They did mention that utilization is different during the weekends, however, as most strategies can be automatically deployed, this should not matter. This difference can possible be explained through the fact that mainly experts in a well-developed country were interviewed, while the AmpPot data consist of FSOs around the world, with a large representation of FSOs in semi-developed countries. Due to lack of knowledge, it remains unclear how the weekday influence the target selection. Furthermore, the dataset showed that DNS is still the most frequently used protocol for an attack on FSOs. DNS is the overall favourite, however, the difference between DNS and NTP is smaller for non-FSOs. Although the experts have mentioned that it is not important where the attack is coming from, and which protocol is used. A total overview of the factors that can add to the other analysis is show in Table 19.

7.2.2 Qualitative analysis

An important factor that can be related to the AmpPot data is the media attention and reputation. The AmpPot data showed that large banks are being attacked more often. However, only a weak correlation between the size and the organisation was found. The media attention and reputation are important indicators that are related to the target selection and size. As the experts have mentioned reputation, more specifically, a bad reputation lead to more attacks. This could be combined with the size of an organisation as large and well-known organisations get more media attention. Smaller organisations are less interesting, and thus, are less mentioned in the media. In the quantitative analysis this subject has already been briefly touched upon, when trying to understand why Barclays was among the top attacked organisation using the DNS protocol. During that period Barclays was frequently mentioned in various cyber security related articles. In addition, if a large organisation is involved in shady investments, they are more easily brought into a bad daylight by the media and thus more easily implanted in the minds of criminals as a possible target. Smaller organisations often do not have the investment portfolio to invest in those kinds of projects, and if they do, they are also less interesting for the media. Furthermore, large organisations often have a large client database, and employees, which increases the chance of getting attacked as only a slight motivation can trigger a person to attack the organisation. However, the generalized linear regression showed

that there was not statistical significant correlation between the amount of employees and the number of attacks.

Table 19: Complementary factors quantitative and qualitative analysis

Complementary factors	
Quantitative analysis:	**Qualitative analysis:**
Organisation size	Internal expertise
Protocols	Intrinsic motivation
Weekday	Organisation size
	Third parties
	Patching/updates
	Media attention
	Reputation

7.3 Conclusion of comparison analysis

SQ10: What are the similarities between the AmpPot data and the opinion of experts?

Both sources have a couple of similarities when it comes to the factors that influence target selection. According to both analyses, the country where the FSO is located influences the target selection. The experts are located in a well-developed country with a relatively high GDP and IDI. Countries that have a high GDP and IDI are more prone to being targeted as these countries use more online resources. Furthermore, both analyses reveal that the organisation size influence the number of attacks. According to both datasets, the victims are usually the large banks. Closely related to size, is the name branding of the FSOs. Well-known organisations are often more targeted, as they are also well known by the cybercriminals.

SQ11: What are the differences the AmpPot data and the opinion of experts?

The comparison analysis showed three significant differences. The first difference relates to the type of country the organisations resides in. While both analyses mention that this is a factor that influence target selection, they both argue the opposite way. According to AmpPot does an increase in the IDI and Normal GDP per Capita result in fewer attacks, while the experts argue that this is the opposite is the case. However, both agree that this is an influential factor. The second difference is related to the size of the organisation. As mentioned above, both analyses showed that the size influence the target selection of DDoS. The experts' mentioned that the size is a big factor and thus holds lots of influential power, while the AmpPot data only showed a weak effect between the size of the organisation and the number of attacks. The last difference is the type of FSO that are being attacked. The AmpPot data shows that mostly large banks and investment groups are being targeted. While the experts also mentioned that mostly large banks are targeted, the investment groups were not mentioned. The experts did not mention that other FSOs are also attacked frequently.

SQ12: How can the previous findings be complemented to each other?

Both the data showed various factors that fall outside the scope of the other analysis. For the qualitative analyse the factors: internal expertise, intrinsic motivation, third parties, patching/updates, organisation size, media attention, and reputation can complement the qualitative dataset. However, the first four are difficult to relate to the AmpPot data as these factors operate on a different level than the AmpPot data. While the last three factors also operate on a different level, these factors can be related to the AmpPot data due to the

organisation name, which is related to the target IP address. Factors identified from the quantitative analysis such as the organisation size, protocols and the weekdays can in their turn complement the quantitative dataset. The organisation size is directly relatable to the interviews. The protocols can add to the fact that experts are not keen on finding out where the attack is coming from. However, this insight can provide information about the possible intensity of the attack. The weekday can indicate what the probability of an attack. As the probability of an attack on Friday is higher than the other days, it is possible to allocate more resources to the Fridays if necessary.

Part IV: Conclusion

8. Conclusion

DDoS attacks are one of the most frequently used cyber-attacks worldwide and impose a significant threat to all types of victims. The growth of DDoS attacks has not gone unnoticed in the scientific world as well as the business world. The commoditization of these attacks has played a primary role in the increase of DDoS attacks. These applications have made it possible to provide DDoS services at low costs, which made it possible for everyone with an Internet connection and little basic knowledge to launch an attack. While the technical side of DDoS has been researched a multitude of times, the more socio-technical side is still a relatively untouched field. Studies have focused extensively on how DDoS works and how they can be mitigated. However, this research tried to provide more insight into the socio-technical side of DDoS based on organisational factors for the financial sector. In order to do so, this research has used DDoS honeypot data parallel to qualitative data gathered from DDoS experts in the financial world. This approach allows for a comprehensive view of factors that influence the target selection, which brings the world a step closer to the possible motivations of attackers. To reach these goals, four research questions, and their associated sub-questions were constructed. This section will provide answers to the four research questions, which subsequently answers the main question of this research. Furthermore, this section will provide the contribution, limitations of the research, recommendations for FSOs, and future research suggestions.

8.1 Answering the research questions

RQ1: Based on what factors do attackers choose their financial target, and how do these attacks influence FSOs according to literature?

FSOs are organisations have historically been frequently attacked by organisations. So based on what factors do attackers select their targets within the financial sector? The literature provides a limited list of target selection factors. One of the most frequently mentioned is the size of the organisations. Organisations that have more than 500 employees are more likely to experience a DDoS attack. The second factor is the type of organisations. Thus, in which sector the organisation operates or if the organisation holds a lot of money. The third factor relates to the country in which the organisation resides. The fourth factor is the technical innovativeness of an organisation. Lastly, the presence of a capable defender also influence target selection according to the literature. In order to provide a better understanding, this research also added factors that are related to the impact. These have been added due to the assumption that attackers want to have an as high impact as possible, and thus focus also on these factors. These factors are: Presence of experts, communication structure, shared responsibilities, speed of updating, internal knowledge of DDoS, centralized security, budget on cyber security, crisis plan, and the presence of a security task force.

RQ2: Which factors influence target selection via booters according to the AmpPot data, and how can these factors be traced back to the FSOs?

At first glance, the data reveals that factors regarding organization size, the context of the organisation, and the type of organisation are important factors that influence the target selection of attackers. Taking a closer look at the organization size, there is a relation between the market value and the number of attacks on FSOs. However, this relation is too small to make any hard claims. Other size related factors such as: number of employees, revenue, profit, net income, and total assets did not show any sign of relation with the number of attacks. This begs the question whether organisation size does indeed influence the target selection. Furthermore, the country in which the FSO resides shows a clear relation with the number of attacks. One of the country-level factors that showed a significant was the IDI. From this it can be concluded that the higher the IDI, the less likely an organisation will be chosen as a target. Compared to

organisation in less high IDI. This seems intuitive, as countries that are developed less in terms of the ICT, are also less capable of mitigation attacks and thus seen as a more vulnerable target by attackers. Another country-level factor was the Nominal GDP Per Capita. This factor showed a significant relation with the number of attacks. Countries with high Nominal GDP Per Capita incurred less attacks. Thus it can be argued that attackers do not focus on the well-developed countries. The type of organisation also showed an effect on the number of attacks. The dataset shows that most large banks that are listed on the Fortune500 are being targeted. In addition to banks, also many investment organisations are being targeted. However, upon analysis this statistically, no significance was found. Lastly, a major factor is the weekday. The analysis showed that FSOs are almost twice as much attacked on Fridays compared to other days. The data also showed, that as the week progresses (from Saturday to Friday) the attacks increasing linearly. However, due to the absence of additional day, it remains unclear why attackers are more prone to attack a FSO on a Friday. Combined, it can be concluded that mostly large banks and investment organisations that are residing in semi-developed countries (China, Turkey, Russia) with lots of IT development and where the critical infrastructure such as the financial sector is largely regulated by the government. However, as the size was weakly related to the number of attacks, it remains unclear whether size actually does influence the number of attacks, or that there are secondary factors related to the size that influence the number of attacks.

RQ3: Which factors influence target selection of DDoS amplification attacks according to experts in FSOs, and how have they coped with those factors?

During the quantitative analysis, seven factors were identified that could influence the target selection. The factors are as follows: organisation size, reputation, media attention, patching and updating, the presence of a guardian, capable employees, and location/country the organisation is located. An important factor according to the experts is the organisation size. If the organisation is large, they are more susceptible for getting attacked. The experts mentions that an attack on a large size organisation would result in more status, which implies that gaining status is an important motivation for using DDoS attacks. Another important factor is the reputation of the FSO. A bad reputation or bad investment can lead to a significant increase in DDoS attacks as punishment for bad social corporate responsibility or a wave of dismissal. These attacks are mostly inflicted by hacktivist. As the media influences the reputation, also media attention could increase the number of attacks. Interestingly, some experts noted that the media attentions one gets does not have to be bad publicity. Also positive media attention can lead to an increase in attack. In addition to those factors, various experts argue that FSOs are targeted randomly. Other experts argue that a DDoS attack always involves any intrinsic motivation. The experts show contrasting results regarding this factor. While the factors could influence target selection, they have not affect the FSOs in terms of strategy. For the FSOs, the why question is not important, but rather how to mitigate the attack. In this regard the FSOs uses more or less similar strategies. This strategy comprises of an internal and external DDoS mitigation capabilities. For their external DDoS mitigation capabilities, FSOs uses third parties that are able to handle large volume of attacks that exceed the bandwidth of the FSO (a capable guardian). When the FSO is targeted by a large DDoS attack, the traffic is spoofed to the external party, which scrubs the traffic and sends the clean traffic back to the FSO. Internally, the FSO uses in-house capabilities for smaller attacks, and attacks on the application layer. However, due to the increasing threat of DDoS experts highlight that new strategies are needed. FSOs should include dynamic flow and network mitigation. Furthermore, cooperation among various sectors is needed, such as cooperation with the police to improve forensic research or close cooperation between ISPs to tackle the spoofing issue of attackers. While these are possible factors that could influence target selection, the experts emphasize that the underlying motivation is a key aspect. Especially showing of the capabilities, and ideological believes have been mentioned as widely used motivations by the experts. Contrary to the literature motivations as financial gains and extortion were not seen much in practice by the experts.

However, currently there is less known about attack motivations due to the low chance of catching attackers. According to the FSOs there should be more focus in catching attackers.

RQ4: What are the similarities and differences between the target selection factors according to the AmpPot data and the opinion of experts?

Contrasting the results of both the quantitative and qualitative analysis showed more similarities than differences. This implies that experts do have a realistic view on the DDoS landscape as it is. Both analyses advocate that the location the FSO resides is important. According to the experts interview, especially well-developed countries with high IDIs are more prone to DDoS attacks. However, the AmpPot data showed a different result, where the IDI and Normal GDP reduce the number of attacks. However, both see the location of the organisation as an important factor for target selection. Furthermore, both analyses mention the organisation size as an important factor that influence target selection. Section 7 also revealed two differences. The first difference is the fact that organisation size is extremely important according to the experts. However, the quantitative analysis only showed a weak relation between the size and the number of attacks. The second difference is the type of organisation that is being targeted. The experts argued that mostly large banks are being targeted, but did not mention investment groups.

To give a more comprehensive view, the analyses are complementary on three factors. Firstly, the organisation size, which was mentioned in both analyses, showed that size was extremely important according to the experts. However, the quantitative analysis was more reserved in this regard. An assumption based on the analyses is that media attention and reputation is more important than organisation size. The media attention and reputation are closely related to the size, as large FSOs are better known globally. Secondly, the results of the protocols in the quantitative analysis can be related to the number of attacks and the intensity of the attack, making it an important indicator for the experts. For instance, if an attack uses a SNMP or SSDP protocol, it can be expected that the intensity is lower than when DNS or NTP is used. Thirdly, the weekday can also improve the predictability of an attack, as the quantitative analysis showed that the number of attacks on Friday is significantly higher than on other days.

8.2 Answering the main question

Concluding, based on the literature study, quantitative and qualitative analyses, the main question can be answered.

Which factors influence target selection of financial services organisations suffering from DDoS amplification attacks?

The quantitative analysis resulted in a set of factors that show statistical significance to the number of attacks as well as the duration of the attacks. Moreover, forthcoming the qualitative analysis, additional factors were identified as factors that impose an influence on the target selection of DDoS attacks. The factors that have been identified are represented in Table 20 and Table 21.

Table 20: Target selection factors quantitative analysis

Quantitative analysis	
Factor	**Description**
Country/location	An increase in IDI and Nominal GDP Per Capita leads to an increase in the number of attacks. IDI showed a stronger effect than the Nominal GDP Per Capita.

Organisation size	The market value showed a significant effect on the number of attacks. However, the effect was very limited, thus no strong can be made based on these findings.
Type of organisation	The type of organisation influences the number of attacks. Mainly large banks and investment groups are prone to DDoS amplification attacks.
Weekday	The numbers of attacks on Fridays are significantly higher than for other weekdays. The weekends and Mondays have fewer attacks.

Table 21: Target selection factors qualitative analysis

Qualitative analysis	
Factor	**Description**
Organisation size	Large banks are more targeted than smaller banks.
Reputation	FSOs with bad reputation are more prone to being attacked by hacktivists, however this is also related to the size and fame of the FSOs.
Media attention	The more FSOs are mentioned in the media, the bigger the chance of getting attacked. It does not matter whether the publicity is bad or good. However, bad media attention would trigger hacktivist rather than good publicity.
Patching/updating speed	DDoS application attacks make use of errors in the systems. Timely updating and patching can significantly reduce the number of abuses and thus also the number of attacks.
Capable guardian	All the banks use a third party that is capable in mitigation large DDoS attacks. This has ensured that banks are currently capable in defending against DDoS attacks.
Capable employees	The employees are still one of the biggest threats for organisations. Having in-house experts is a necessity to defend against DDoS attacks.
Location/country	Countries that do not use many online services, and are not well developed seem to be less interesting for attackers.

The AmpPot data showed that among the countries there is a convincing diversity in attacks per country. On a more detailed level, there are certain country-level factors that influence the target selection of DDoS. Firstly, There seem to be a significant relation between the IDI and the number of attacks. With most attacks targeting semi-developed countries. Secondly, the Nominal GDP Per Capita showed a significant relation with the number of attacks. However, this effect is very limited. Furthermore, These factors were also mentioned during the interviews. The experts mentioned that the number of citizens, the size of the country, and the technical innovativeness influence the target selection. Hence, these factors do indeed influence target selection. However, the experts argue that this effect is significantly different than was found in the AmpPot analysis.

For organisations, there are some contradictory results regarding their size. Various size indicators have been researched from which the market value had the most significant influence. However, contrary to what experts believe, the size indicators showed a limited effect on the number of attacks. This begs the question if the organisation size does indeed relate target selection, or if there are secondary factors in place. One of the possible explanations is that the size does not effect the target selection on its own, but is inherently related to the media attention it receives. In addition, banks as various investment groups are targeted more frequently than other financial organisations. This is an interesting finding, as this implies that having technical oriented organisation does not mean that the number of attacks also increases.

A more surprising factor is the day of the week. While for DDoS in general there is a more linear pattern regarding the number of attacks per day, financial are attacked significantly more often on Fridays. Putting this into perspective on the regular workweek, employees leave for their homes on Friday, which limits the utilization of number of employees to defend against an attack. Cybercriminals tend to response to this aspect, as the chance of success is higher on Fridays. However, this argument can also be argued for other sectors. In addition, the experts did not see such a different in distribution.

In addition to the previous factors, the experts discussed various other factors. As slightly touch upon in the beginning of this section, the media attention could be an influence factors as well. However, not all experts agree on this factor. The rationale is that financial organisations that are more often in the news are more known (among cybercriminals). This makes them more susceptible for attacks. Yet, some experts are not convinced that this factor does indeed raise the number of attacks. What the experts do agree on is the fact that the reputation increases the number of attacks. A bad reputation leads to more attacks.

DDoS is a highly technical attack that abuses various systems. Similar to the abuse of the protocols, DDoS could thus abuse internal organisation systems. Therefore, the experts agree that the doing patching/updates reduces the target selection. However, often an attack can already be seen in advance, as organisation are able to spot sniffing in their network.

Furthermore, organisations should have capable employees in order to mitigate and defend against DDoS attacks. Earlier attacks on the Dutch banks have shown that having employees that know how to act during an attack can reduce the number of future attacks. In addition to having capable employees, it is well suggested that having a mitigation party that is specialized in scrubbing traffic results in significantly less successful attacks and future attacks. However, this has to be studied in more depth as this research did not focus on the relation between success rate and future attacks.

8.3 Contributions

While the list provided in table 20 and 21 looks inherently similar to the one provided by the literature, there are some notable differences. Firstly, the weekday is a significant factor, which the attacker based their attacks on. Most attacks occur on Fridays; while this is not the case for the remaining DDoS attack data. The weekday can thus be added to the list of target selection factors for FSOs. Secondly, the size of the organisations was the most mentioned factor to influence the target selection. However, this research showed that there was only a little effect of the size on the number of attacks. This effect was significantly small, that not claims can be made based on these results. Therefore, it begs the question whether the organisation size does indeed influence the target selection. This research assumes that media attention combined to the size of organisation is a better indicator for target selection than size solely. Thirdly, similar to the literature, does the country affects the target selection. However, this research showed the opposite effect for some of the country-level factors. While most researchers showed an increase in attacks, if one of the factors also increased, this cannot be said for FSOs. For them, a lower IDI or Nominal GDP Per Capita would imply a higher chance of getting attacked by a criminal. In addition, this research showed that attackers also focus on various internal factors, which are more related to impact, such as having a capable guardian, employees and/or speed of patching & updates.

In addition to the above stated contributions, this research also adds secondary contributions. First and foremost, methodology used for this research to map the financial institutions can be used by other researches. While it shows that only 47% of the total financial organisations can be mapped, it could find the fast majority which names are related to financial organisations. Secondly, the script used to match the targeted IP to an organisation can be used for other types

of research and matching. Thirdly, the descriptive analysis provides a general overview of the financial DDoS landscape according to AmpPot. Lastly, an overview on how experts view the current and future DDoS landscape and how that compares to global DDoS attacks.

8.4 Research limitations

The research was initiated considering the boundaries defined by limitations. The datasets that were used for comparing were not perfectly complementary. The AmpPot data is mainly focused on DDoS amplification attacks, while the qualitative data addresses DDoS in general. In such, the datasets did not match perfectly in terms of their DDoS techniques i.e. their attack protocols as well as the use of various botnets. The time line of both datasets was not concurrent. The experts discussed DDoS based on their experience, which varied among the experts. However, they focused mainly on DDoS attacks since 2012, with major emphasizes on the last two years. The AmpPot data only gathered data from 2014 until 2015. The trends and attack cases regarding DDoS attacks for the last couple years (2016-2017) could not be analysed using the quantitative analyses. Another limitation is the fact that various organisational variables needed to be added to the AmpPot data. As data was not always available, the variables had to be added by hand. One specific limitation was the extracting of the financial data. Limitations were also encountered during the extraction of the financial data. The keywords necessary for obtaining the financial data were based on laborious searches. In this regard, the financial data was limited more frequented keywords, while there could be more financial organisations. In addition to this, as only 47% could be mapped, the results could be biased due to missing cases in the financial dataset. For instance, missing of a large amount of smaller FSOs. The size of an organisation also needed to be added to the AmpPot data. Due to time limits and availability of the data, only size indicators of listed Fortune500 organisations could be gathered and added. This has limited the regression analysis of the size to only those FSOs that are in the Fortune500. The last limitation is the focus of the two data sources. The financial AmpPot data consisted of all types of financial services, while the qualitative analysis consisted of data that was mainly deducted from the banking sector. In addition, the AmpPot data consisted data of FSOs around the world, while the qualitative data was gathered from mainly Dutch organisations. This has implications for the recommendations based on the qualitative data, as they are mainly focused for the Dutch financial sector.

8.5 Recommendations

8.5.1 Recommendation to financial organisations

This research has some useful insights regarding the target selection of DDoS (amplification) attacks on financial institutions. While a number of factors are outside the scope of some financial organisations, a few recommendations that could significantly reduce the DDoS attacks are:

- Due to the differences in target selection between countries, it is important to work internationally to share knowledge in order to educate less developed organisations/countries.
- Even though size was not an influential factor for target selection, large organisations should be focussing on the factors that trigger criminals to target them. These organisations have the financial means to do research on this particular topic, which helps tackling the DDoS issue as such.
- FSOs should focus more on the motivations of the attacks. It is important to know the motivations behind an attack as this will help to understand why the FSO is being targeted. As the motivation cannot be observed from solely the attack, FSOs should have already probable scenarios in place to exclude unlikely motivations.

- The financial institutions should allot as such attention to the origins of the attack as to mitigating the damages caused by attacks.
- FSOs should be more alert on DDoS attacks on Fridays, due to the higher risk of getting attacked. However, as no clear argument can be given for this development it still has to be studied, how this relate to an organisation.

8.5.2 Overall recommendation

DDoS does not limit itself to organisational boundaries. To contain the current and increasing threat of DDoS, actions should not be limited to solely financial services. For this reason, also recommendations to authorities and other sectors will be given.

- It is important that attackers are caught and prosecuted. This would result in better understanding the attack motivations and thus how to understand target selection. This asks for a close cooperation between organisations and law enforcement institutions.
- As DDoS are increasing in power, inter-sectorial cooperation should be stimulated. An example could be collaboration between ISPs and financial institutions to be able to exclude between traffic from different countries or continents, or tackle the issue of spoofing.
- Sharing knowledge both within and between sectors is encouraged. Organisations should share information about the reasons behind the attack, from which IP the attack is coming from, and the bandwidth.

8.5.3 Suggestions further research

Based on the results and the limitations of this research, the following research subjects for future research are suggested:

- This research can be a starting point to dive deeper into the differences between the financial data and compare the results with other sectors (e.g. the telecom sector). This can provide insight into the fact as to how FSOs are attacked differently compared to other sectors, and to what extent.
- A more thorough analysis on the factors that influence target selection. For instance, the size as to whether DDoS attacks are currently moving to smaller financial organisations, or if the influence of media attention affects the number of attacks.
- Target selection can also be addressed in the perspective of attack duration. A similar research that focuses on target selection relatively to attack duration could be a follow-up study of this research.

In addition, based on the expert interviews there are also various future research suggestions:

- As the banks are capable in defending against DDoS it is interesting to research whether successful mitigating DDoS would also result in less follow-up attacks. Thus whether there is recurrence based on the success of an attack.
- There is still a big gap in terms of knowledge on the motivation of attacks. In that sense it is also important how attackers can be found and brought to justice.
- As the bandwidth of DDoS is increasing, it is important for various sectors to work together in defending against DDoS. An important research field would be to focus on the inter-sectorial relationships in targeting DDoS.

References

Akamai. (2014). *Akamai's [state of the internet]/security*.

Alieyan, K., Kadhum, M. M., Anbar, M., Rehman, S. U., & Alajmi, N. K. A. (2016). An Overview of DDoS attacks based on DNS, 276–280. http://doi.org/10.1109/ICTC.2016.7763485

Alvarez, C. S. (n.d.). Amplified DDoS Attacks: The current Biggest Threat Against the Internet. Retrieved October 26, 2016, from https://www.icann.org/news/blog/amplified-ddos-attacks-the-current-biggest-threat-against-the-internet

Anderson, R., Barton, C., & Böhme, R. (2012). Measuring the Cost of Cybercrime. *WEIS*.

Andriesse, D., Rossow, C., Stone-Gross, B., Plohmann, D., & Bos, H. (2013). Highly resilient peer-to-peer botnets are here: An analysis of Gameover Zeus. *Proceedings of the 2013 8th International Conference on Malicious and Unwanted Software: "The Americas", MALWARE 2013*, 116–123.

Arbor Networks. (2015a). The Risk vs. Cost of Enterprise DDoS Protection, 10.

Arbor Networks. (2015b). *World Wide Infrastrucure Security Report 2015* (Vol. XI).

Arbor Networks. (2016). *Worldwide Infrastructure Security Report 2016* (Vol. XII).

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). 2020 cybercrime economic costs: No measure no solution. *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, 701–710.

Bakshi, A., & Yogesh, B. (2010). Securing cloud from DDOS attacks using intrusion detection system in virtual machine. *2nd International Conference on Communication Software and Networks, ICCSN 2010*, (fig 1), 260–264. http://doi.org/10.1109/ICCSN.2010.56

Berg, J. Van Den, Zoggel, J. Van, Snels, M., Leeuwen, M. Van, Boeke, S., Koppen, L. Van De, … Bos, T. De. (2014). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. *NATO STO/IST-122 Symposium in Tallin*, (c), 1–10.

Böttger, T., Braun, L., Gasser, O., Von Eye, F., Reiser, H., & Carle, G. (2015). DoS amplification attacks - protocol-agnostic detection of service abuse in amplifier networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9053*(March 2013), 205–218. http://doi.org/10.1007/978-3-319-17172-2_14

Bougaardt, G., & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. *The Electronic Journal Information Systems Evaluation*, *14*(2), 167–178.

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law and Criminology*, *97*(2), 379–476. http://doi.org/0091-4169/07/9702-0379

Briney, A., & Prince, F. (2002). Does Size Matter ?, (September).

Broadhurst, R., & Choo, K. R. (2009). Cybercrime and on-line safety in cyberspace. *International Handbook of Criminology*, (March), 153–165.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731.

Chromik, J. J., Santanna, J. J., Sperotto, A., & Pras, A. (2015). Booter websites characterization: Towards a list of threats. *Brazilian Symposium on Computer Networks and Distributed Systems (SBRC)*, (i).

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach A ROUTINE ACTIVITY APPROACH*. *Source: American Sociological Review American Sociological Review*, *44*(44), 588–608.

Czyz, J., Kallitsis, M., Gharaibeh, M., Papadopoulos, C., Bailey, M., & Karir, M. (2014). Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks. *Imc*, 435–448. http://doi.org/10.1145/2663716.2663717

Deci, E. L., & Ryan, R. M. (2000). Commentaries on "The 'What' and 'Why' of Goal Pursuits:

Human Needs and the Self-Determination of Behavior." *Psychological Inquiry*, *11*(4), 269–318. http://doi.org/10.1207/S15327965PLI1104_02
EY. (2014). Achieving resilience in the cyber ecosystem Rise of the cyber ecosystem. *Insights on Governance, Risk and Compliance*, (December).
Geyres, S., & Orozco, M. (2016). *Think banking cybersecurity is just a technology issue?*
Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519.
Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. http://doi.org/10.1007/s11416-006-0015-z
Groot, M. De. (2015). Unveiling Weaknesses of Booters.
Hall, M. J., David Hansen, D., & Jones, K. (2015). Cross-domain situational awareness and collaborative working for cyber security. *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015*.
Holl, P. (2015). Exploring DDoS Defense mechanisms, (March), 1–10.
Hoque, N., Bhattacharyya, D., & Kalita, J. (2015). Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys & Tutorials*, *PP*(99), 1–1.
Imperva. (2016). Global DDoS Threat Landscape. *Global DDoS Threat Landscape Q1 2016*. Retrieved from https://www.incapsula.com/ddos-report/ddos-report-q1-2016.html
International Telecommunication Union (ITU). (2014). *Measuring the information society report: 2014*. *Organizacija znanja* (Vol. 8). http://doi.org/10.3359/oz0303157
Jin, S., & Yeung, D. D. S. (2004). A covariance analysis model for DDoS attack detection. *Communications, 2004 IEEE International …*, *4*(c), 1882–1886 Vol.4. http://doi.org/10.1109/ICC.2004.1312847
Johnson Onwuegbuzie AJ, R. B. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*, *Vol. 33 No*(7), 14–26.
Kambourakis, G., Moschos, T., Geneiatakis, D., & Gritzalis, S. (2008). Detecting DNS amplification attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5141 LNCS*(October 2002), 185–196. http://doi.org/10.1007/978-3-540-89173-4_16
Karabacak, B., Ozkan Yildirim, S., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Computer Law and Security Review*, *32*(3), 526–539. http://doi.org/10.1016/j.clsr.2016.02.005
Karami, M. (2016). *Understanding and undermining the business of DDoS booter services*.
Karami, M., & Mccoy, D. (2013). Understanding the Emerging Threat of DDoS-As-a-Service. *LEET '13 Usenix*, 2–5.
Karami, M., Park, Y., & McCoy, D. (2015). Stress testing the Booters: Understanding and undermining the business of DDoS services. *Arxiv*, 1033–1043.
Kark, K., Dines, R. a., Balaouras, S., & Coit, L. (2010). Security Organization 2.0: Building A Robust Security Organization, 18. Retrieved from http://eval.symantec.com/mktginfo/enterprise/articles/b-article_security_organization_20_building_a_robust_security_organization.en-us.pdf
Kaspersky Lab. (2015). *Denial of Service: How Businesses Evaluate the Threat of DDoS Attacks*.
Kelley, D. (2016). *Insights from the 2016 IBM X-Force Threat Intelligence Report*.
Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers and Security*, *28*(7), 509–520.
Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., & Rossow, C. (2015). AmpPot: Monitoring and defending against amplification DDos attacks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9404*, 615–636.
Krebs, B. (2016). Are the Days of "Booter" Services Numbered? Retrieved October 10, 2016, from https://krebsonsecurity.com/2016/10/are-the-days-of-booter-services-numbered/
Krupp, J., Backes, M., & Rossow, C. (2016). Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks, (i), 1426–1437.

Kuhrer, M., Hupperich, T., Rossow, C., & Holz, T. (2014). Hell of a Handshake : Abusing TCP for Reflective Amplification DDoS Attacks. *USENIX Workshop on Offensive Technologies (WOOT)*, 1–6.

Kührer, M., Hupperich, T., Rossow, C., & Holz, T. (2014). Exit from Hell ? Reducing the Impact of Amplification DDoS Attacks. *23rd USENIX Security Symposium, USENIX Sec 2014*, 111–125.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*(0), 58–74. Retrieved from http://www.sciencedirect.com/science/article/pii/S016740481400087X

Mason, J. (2006). Mixing methods in a qualitatively driven way. *Qualitative Research*, *6*(1), 9–25.

Matthews, T. (2014). Incapsula Survey: What DDoS Attacks Really Cost Businesses. Retrieved from http://lp.incapsula.com/rs/804-TEY-921/images/DDoS Report Q2 2015.pdf

Moorsel, D. van. (2016). Target selection regarding financial malware attacks within the Single Euro Payments Area. Retrieved from http://repository.tudelft.nl/islandora/object/uuid:c1c0e0e0-7fe2-469d-a010-325f1942f89b/datastream/OBJ/download

Morgan, S. (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Retrieved October 26, 2016, from http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#29621cb03bb0

Nagurney, A. (2015). A multiproduct network economic model of cybercrime in financial services. *Service Science*, *7*(1), 70–81.

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber …*, *5*(1), 773–793.

Noroozian, A., Korczy??ski, M., Ga??an, C. H., Makita, D., Yoshioka, K., & Vaneeten, M. (2016). Who gets the boot? Analyzing victimization by DDoS-as-a-service. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 9854 LNCS, pp. 368–389). http://doi.org/10.1007/978-3-319-45719-2_17

Parsons, K., Mccormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security : Individual , Culture and Security Environment. *Science And Technology*, (DSTO-TR-2484), 45.

Pescatore, J. (2014). DDoS Attacks Advancing and Enduring : A SANS Survey. *SANS AInstitute InfoSec Reading Room*.

Petee, T. (2010). Defining "Cyber-Crime": Issues in Determining the Nature and Scope of Computer-Related Offenses. *Future …*, 6–11. Retrieved from http://futuresworkinggroup.cos.ucf.edu/docs/Volume 5/PeteeV5.pdf

Pierrakis, Y., & Collins, L. (2013). Banking on Availabilty, (April), 1–43.

Pras, A., Santanna, J. J., Steinberger, J., & Speretto, A. (2016). DDoS 3.0-How terrorists bring down the Internet. *International GI/ITG Conference on Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance*, 1–4.

Preyadharsini, R., & Deepa, K. (2016). Duplicate Record Detection Using Progressive Sorted Neighborhood Method. *Avinashilingam*, (February).

PWC. (2014). *Economic crime: A threat to business globally*.

Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank ' s finances. *International Journal of Current Research and Academic Review*, *2*(2), 173–178.

Rescorla, E. (2003). Security Holes... Who Cares? *Proceedings of the 12th USENIX Security Symposium*, 75–90.

Rescorla, E. (2005). Is finding security holes a good idea? *IEEE Security and Privacy*, *3*(1), 14–19. http://doi.org/10.1109/MSP.2005.17

Rossow, C. (2014). Amplification Hell: Revisiting Network Protocols for DDoS Abuse. *Proceedings 2014 Network and Distributed System Security Symposium*, (February), 23–26.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer Security Incident Response Team Development and Evolution. *IEEE Security & Privacy*, *12*(5), 16–26. http://doi.org/10.1109/MSP.2014.89

Santanna, J. J., Durban, R., Sperotto, A., & Pras, A. (2015). Inside booters: An analysis on

operational databases. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 432–440.
Santanna, J. J., Van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015). Booters - An analysis of DDoS-as-a-service attacks. In *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015* (pp. 243–251). http://doi.org/10.1109/INM.2015.7140298
Schneier. (2011). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.
Shadows, D. (2016). Ransomware and Other Cyber Extortion :, (July), 1–20.
Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2016). Service resizing for quick DDoS mitigation in cloud computing environment. *Annales Des Telecommunications/Annals of Telecommunications*, 1–16. http://doi.org/10.1007/s12243-016-0552-5
Tajalizadehkhoob, S., Asghari, H., Gañán, C., & Eeten, M. van. (2014). Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware. *Workshop on the Economics of Information Security (WEIS)*, 1–26.
Thomas, D., & Loader, B. (2000). Introduction: Cybercrime: law enforcement, security and surveillance in the information age. In *Cybercrime: law enforcement, security and surveillance in the information age*. London: Routledge.
Torres, A. (2014). Incident Response : How to Fight Back. *Sans Institute*, (August), 28.
Turner, R. (2014). *Tackling the DDoS Threat to Banking in 2014*.
Verschuur, E. (2012). strategic feasibility of NFC mobile payments in the Netherlands? How the individual strategies of stakeholders affect the NFC mobile payment ecosystem as a whole. Retrieved from http://repository.tudelft.nl/view/ir/uuid:cc178b20-6489-48d1-a58a-5ae5bb890516/
Wilson. (2013). Every minute of every day, a bank is under cyber attack. Retrieved November 3, 2016, from http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10359563/Every-minute-of-every-day-a-bank-is-under-cyber-attack.html
Wilson, M., & Hash, J. (2003). (2003). Building an Information Architecture Checklist. *Organization*, *2*(2), 1–70. http://doi.org/10.1109/IEMBS.2010.5627684
Wueest, C. (2014). The continued rise of DDoS attacks, 1–31.
Yar, M. (2005). The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407–427.
Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y., & Tang, F. (2012). Discriminating DDoS attacks from flash crowds using flow correlation coefficient. *IEEE Transactions on Parallel and Distributed Systems*, *23*(6), 1073–1080. http://doi.org/10.1109/TPDS.2011.262
Zargar, S. T., Joshi, J., Tipper, D., & Member, S. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS), *15*(4), 2046–2069.
Zerodium. (n.d.). ZERODIUM Payout Ranges. Retrieved April 2, 2017, from https://www.zerodium.com/program.html
Zimmermann, H. (1980). OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, *28*(4), 425–432.

Appendix A Keywords

In the table below, the keywords used to map the financial organisations from the AmpPot data are shown. Various different sources were used to identify relevant keywords: firstly, personal conversations with employees from the accounting firm EY were used. These conversations helped identified the universal keywords, which are often used in names of financial institution (see Table 22). In addition to the universal keywords, a set of keywords was identified using the quote500 and global500 compiled by Fortune. Thirdly the website of the research institute Gartner was used to add missing financial keywords to the search list Table 23. These sources provided a list of financial institutions, which were also added to the data.

Table 22: Keywords (Universal)

Universal	
Acquisition	(Invest)ment
Asset	Loan
Assicurazione/ Assicurazioni	Money
Assurance	Mortgage
Balance	Pagamento
Banc	Pay
Banca	Pension
Banco	Price
Bank	Pricing
Banque	Property/properties
Belasting	Real estate
Bitcoin	Savings
Bonds	Securities
Broker	Seguro
Capital	Stock
Cash	Tax
Credit	Trade
Currency	Transaction
Debit	Transfer
Divestures	Trust
Equity/Equities	Valores (eng. Securities)
Exchange	Vastgoed
Fee	Versicherung
Finance	Verzekering
Financial	Visa
Finanz	Wallet
Funds	Wealth
Hedge funds	Yield
Impuesto (eng. Tax)	銀行 (bank in chinese trad.)
Insurance	银行 (bank in chinese simp.)

Table 23: Keywords (organisations)

Financial institutions	
ABN AMRO Bank	Jones Financial
Achmea	Jones Lang LaSalle
Aegon	JPMorgan Chase
Affiliated Managers Group	Kemper
Aflac	KeyCorp
Agricultural Bank of China	KKR
AIA Group	Knights of Columbus
AIG	Legg Mason
Alleghany	Liberty Mutual Insurance Group
Allianz	Lincoln National
Allstate	Lloyds Banking Group
Ally Financial	Loews corporation
American Express	LPL Financial Holdings
American Family Insurance Group	M&T Bank Corp.
American Financial Group	Manulife Financial
American National Insurance	Mapfre Group
Ameriprise Financial	Mapfre vera cruz seguradora
Amica Mutual Insurance	Markel
AmTrust Financial Services	Marsh & McLennan
Aretec Group	Massachusetts Mutual Life Insurance
Arthur J. Gallagher	MasterCard
Assicurazioni Generali	Medical Mutual of Ohio
Assurant	Meiji Yasuda Life Insurance
Australia & New Zealand Banking Group	Mercury General
Auto-Owners Insurance	MetLife
Aviva	Mitsubishi UFJ Financial Group
AXA	Mizuho Financial Group
Banco Bilbao Vizcaya Argentaria	Morgan Stanley
Banco Bradesco	MS&AD Insurance Group Holdings
Banco do Brasil	Munich Re Group
Banco Santander	Mutual of America Life Insurance
Bank of America Corp.	Mutual of Omaha Insurance
Bank of China	National Australia Bank
Bank of Communications	National General Holdings
Bank of New York Mellon Corp.	Nationstar Mortgage Holdings
Bank of Nova Scotia	Nationwide
Barclays	Navient
BB&T Corp.	New China Life Insurance
Berkshire Hathaway	New York Community Bancorp
BGC Partners	New York Life Insurance
BlackRock	Nippon Life Insurance

Blackstone Group	Northern Trust
BNP Paribas	Northwestern Mutual
Boston Properties	Old Mutual
Capital One Financial	Old Republic International
Carlyle Group	Omnilife de Mexico
Cathay Life Insurance	OneMain Holdings
CBRE Group	Pacific Life
Charles Schwab	PayPal
China Construction Bank	Paysafecard
China Everbright Group	Penn Mutual Life Insurance
China Life Insurance	People's Insurance Co. of China
China Merchants Bank	Ping An Insurance
China Minsheng Banking	PNC Financial Services Group
China Pacific Insurance (Group)	Popular
China Poly Group	Poste Italiane
China Vanke	Power Corp. of Canada
Cincinnati Financial	Principal Financial
CIT Group	Progressive
CITIC Group	Prologis
Citigroup	Prudential
Citizens Financial Group	Prudential Financial
CME Group	Rabobank Group
CNO Financial Group	Raymond James Financial
CNP Assurances	Realogy Holdings
Comerica	Regions Financial
Commonwealth Bank of Australia	Reinsurance Group of America
Country Financial	Royal Bank of Canada
Crédit Agricole	Royal Bank of Scotland Group
Credit Suisse Group	Samsung Life Insurance
CUNA Mutual Group	Sberbank
Dai-ichi Life Insurance	Securian Financial Group
Dalian Wanda Group	Selective Insurance Group
Depository Trust	Sentry Insurance Group
Deutsche Bank	Shanghai Pudong Development Bank
Discover Financial Services	Simon Property Group
DZ Bank	Société Générale
Edward D. Jones and Company	Sompo Japan Nipponkoa Holdings
Equity Residential	StanCorp Financial Group
Erie Insurance Group	Standard Chartered
Evergrande Real Estate Group	State Bank of India
EXOR Group	State Farm Insurance Cos.
Fannie Mae	State Street Corp.
Farmers Insurance Exchange	Stewart Information Services

Fidelity National Financial	Stifel Financial
Fifth Third Bancorp	Sumitomo Life Insurance
First American Financial	Sumitomo Mitsui Financial Group
First Republic Bank	SunTrust Banks
FM Global	Swiss Life
Franklin Resources	Swiss Re
Freddie Mac	Symetra Financial
General Growth Properties	T. Rowe Price
Genworth Financial	Talanx
Goldman Sachs Group	TD Ameritrade Holding
Greenland Holding Group	Thrivent Financial for Lutherans
Groupe BPCE	TIAA
Guardian Life Ins. Co. of America	Tokio Marine Holdings
H&R Block	Torchmark
Hanover Insurance Group	Toronto-Dominion Bank
Hanwha	Travelers Cos.
Hartford Financial Services Group	U.S. Bancorp
HCP	UBS Group
Hedefonline Investmnet Ltd.	UniCredit Group
Hospitality Properties Trust	Unipol Group
Host Hotels & Resorts	Unum Group
HSBC Holdings	USAA
Huntington Bancshares	Ventas
Icahn Enterprises	Vornado Realty Trust
Industrial & Commercial Bank of China	Voya Financial
Industrial Bank	VTB Bank
ING Group	W.R. Berkley
Intercontinental Exchange	Wells Fargo
Intesa Sanpaolo	Welltower
INTL FCStone	Western & Southern Financial Group
Itaú Unibanco Holding	Westpac Banking
J.P. Morgan Chase	Zions Bancorp.
Japan Post Holdings	Zurich Insurance Group

Appendix B AmpPot Data

The victim data used for this research was gathered via a set of amplifier honeypots called APPOTs (Krämer et al., 2015). This dataset will be mainly used for the quantitative analyses part. AmpPot mimics services having amplification attack vectors by listening on UDP ports that are likely to be abused. More specifically, AmpPot supports all protocols that are said to be vulnerable: QOTD, CharGen, DNS, NTP, Net- BIOS, SNMP, and SSDP, MSSQL, and SIP (5060/5061) (Krämer et al., 2015). AmpPot provides data about 5.721.432 IP addresses, captured over the two years (2014-2015) via amplifier-honeypots or AmpPots. This data was gathered and research by Kramer et al (Krämer et al., 2015). Kramer et al. focused their research on exploring attackers preparing and launching amplification DDoS attacks in the wild. This research has focused on the target selection of the data in general.

On a first glance there seems to be enough financial data that can be extracted from the dataset. From the total dataset, 17,781 IP addresses can be linked to FSO, each having 19 variables. This seems sufficient for the analysing. However, it has to be kept in mind that this is only 0.31% of the total dataset.

To extract the financial IP organisation addresses, various keywords have been used. These keywords were collected from three different sources. Firstly, the accountancy firm EY was consulted. Keywords extracted from the website and with personal communication were used. Secondly, FSOs that were ranked in the Quote500 and Global500 by Fortune were also used as keywords. These FSOs were found using the filter of Fortune, which is able to filter by sector ("*financials"*) and industry ("*financial data services"*). Lastly, the website of Gartner was consulted to search for keywords that have not been used. These keywords were found using *the filter by industry* ("*Banking and investment services*") of the Gartner website. Some of the keywords that were used: *bank(ing), wealth, insurance, capital JPMorgan Chase, transaction, credit, visa, debit*. A full list of all the keywords is presented in the previous appendix (see Appendix A). In addition, a handful of the keywords were translated to different languages (English, Spanish, Italian, Portuguese, Dutch, German, and French). However, an issue occurs for the languages that not use western letters (e.g. Arabic and Chinese). Therefore, various keywords have also been used for different languages, such as the Chinese word for bank. It is expected that most of these keywords have an English counterpart, which reduces the chance of missing out.

The variables that are being used in the dataset are:

1. **target_ip:** The IP address that has been targeted by a DDoS attack.
2. **date:** The date of the attack.
3. **sensor_id:** The name of the honeypot that monitored the attack traffic.
4. **service:** The protocol that was used to execute the attack.
5. **start_time:** The start time of the attack.
6. **stop_time:** The stop time of the attack.
7. **duration:** Attack duration.
8. **pyasn_as:** The autonomous system number identifying which AS is routing traffic for the attacked IP.
9. **pyasn_as_bgp_size:** The total number of IP addresses that the AS routes.
10. **cc:** Short form of the country in which the IP address seems to reside.
11. **as_type:** The type of the Autonomous system (Could be ISP, Hosting, EDU, etc.).
12. **tg_op:** A string identifier to ASes that are known to be Broadband ISPs.
13. **caida_type:** A type identifier for ASes based on different source (CAIDA).
14. **dc:** The number of second level domains that have been observed to map to the attacked IP address in DNS traffic.
15. **subs:** The number of subscribers for those ASes that are known to be Broadband ISPs.

16. **as_ipsize_seen:** The total number of IP addresses of the AS that have been observed to be used in DNS traffic.
17. **as_domainsize_seen:** The total number of second level domains that have been observed to be routed to IPs of the AS in DNS traffic.
18. **year:** The year of the attack.
19. **udp_port_list:** The ports that attack packets have been sent to.

Appendix C Samples dataset

Table 24: Sample AmpPot data

target_ip	date	sensor_id	service	start_time	stop_time	duration	pyasn_as	pyasn_as_bgp_size	cc	as_type	tg_op	caida_type	dc	subs	as_ipsize_seen	as_domainsize_seen	year	udp_port_list	org
162.123.87.66	2014-10-18	sensor004	dns	2014-10-18T06:48:26+09:00	2014-10-18T06:48:53+09:00	27.0	11857.0	75008.0	US			Enterprise	0		449.0	656.0	2014	[2171,37069,53555, 56844]	Aegon USA
162.123.19.220	2015-07-13	sensor001	ntp	2015-07-13T21:42:31+09:00	2015-07-13T22:42:41+09:00	3610.0	11857.0	75008.0	US			Enterprise	37		449.0	656.0	2015	[888]	Aegon USA
198.39.106.38	2015-11-25	sensor004	ssdp	2015-11-25T22:17:50+09:00	2015-11-25T22:47:45+09:00	1795.0	11857.0	75008.0	GB			Enterprise	32		449.0	656.0	2015	[13402]	Aegon Edc Limited
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Table 25: Sample Fortune500 data

Company	Revenues	Revenues_change	Profits	Profit_change	Mvalue2014	Mvalue2015	Mvalue_change	Net_Income	Total_Assets	Employees	Price	PE_ratio	Dividend_yield
American Express	35999	0.03	5885	0.1	95396.9	79617.9	-0.17	5839	156993	54000	78.1	14.1	1.3
Banco Bradesco	55628	0.09	6505	0.13	60410.5	43225.9	-0.28	6413	388423	95520	9.3	6.1	5.8
Citigroup	90646	-0.03	7313	-0.47	144627.3	156359.8	0.08	7202	1842530	241000	51.5	23.4	0.1
...	...	...	...	...	...	...	...	...	...	...	...	...	...

Appendix D Data preparation

In this section the code for assigning the organisations to the target_ip is explained. In order to assign the organisations, the data analysis toolkit Pandas was used. This toolkit is based on the programming language Python and is specifically design to analyse large datasets.

```
# import relevant libraries
import dateutil.parser as dp
import datetime
import GeoIP
import os
import pandas as pd

# path of the database
_ORG_MAPPING_DATABASE_PATH = "/Users/ryan/GeoIp_data/db.geoiporg"


def closest_matching_orgdb(date):
  """ Returns Closest Matching ASNDB for a specific day looking forward in time"""
  s  =  os.path.join(_ORG_MAPPING_DATABASE_PATH,  'GeoIPOrg_%4d%02d%02d.dat'  %  (date.year,
date.month, date.day))
  if os.path.isfile(s):
    return s
  else:
    d = date + datetime.timedelta(days=1
    while d <= datetime.date.today():
      s  =  os.path.join(_ORG_MAPPING_DATABASE_PATH,  'GeoIPOrg_%4d%02d%02d.dat'  %  (d.year,
d.month, d.day))
      if os.path.isfile(s):
        return s
      d += datetime.timedelta(days=1
  return None

def lookup_org(orgdb, ip):
  """ This will look up the organization name for you and remove some special characters if
there are any"""
  ip_str = str(ip)
  org = orgdb.org_by_addr(ip_str)
  if org is None:
    org = "None"
  if '|' in org:
    org = org.replace('|', '')
  return org

def lookup_org_per_entry(row):
  date = dp.parse(row['date']).date()
  ip = row['target_ip']
  matching_orgdb = closest_matching_orgdb(date)
  db = GeoIP.open(matching_orgdb, GeoIP.GEOIP_MEMORY_CACHE)
  org = lookup_org(db, ip)
  print(date)
  return org

data    =    pd.read_csv("/Users/ryan/Desktop/small_data_with_ports.csv",    low_memory=False,
sep='|')
data["org"] = data.apply(lookup_org_per_entry, axis=1)

# write new data to text file.
data.to_csv(ROOT_DIR + "/" + "DDoS_DatebasedOrg_db.txt", sep='|')
```

Extract organisations from the AmpPot dataset:

```
# import relevant libraries
import pandas as pd
import os
pd.set_option('display.max_rows', None)

def create_dir(directory):
  if not os.path.exists(directory):
```

```
    os.makedirs(directory)

ROOT_DIR = "./DDoS_data/fin_data"
create_dir(ROOT_DIR)

# keywords in the dataframe
word = "bank"
# keywords that needs to omitted
nword = "cash"
write = False

# Read the big file into a pandas
data = pd.read_csv("./DDoS_data/DDoS_datebasedOrg_db.txt", delimiter="|")

# Extract the lines
organisations = data.loc[data["org"].str.contains(word, case=False)]
organisations = organisations.loc[~organisations["org"].str.contains(nword, case=False)]
```

Appendix E Data analysis

This section will provide an overview of the additional graphs and tables for the AmpPot data analysis. In appendix E-1 the graphs for the descriptive analysis are provided. In appendix E-2 the additional tables and graphs for the statistical analysis will be discussed.

Appendix E-1 Descriptive analysis

The graphs below depict the total overview of the attacked countries for the financial data. This graph illustrates that more linear decay of the number of attacks per country compared the non-financial data. In that graph the top countries are significantly more often attacked than the remaining countries.

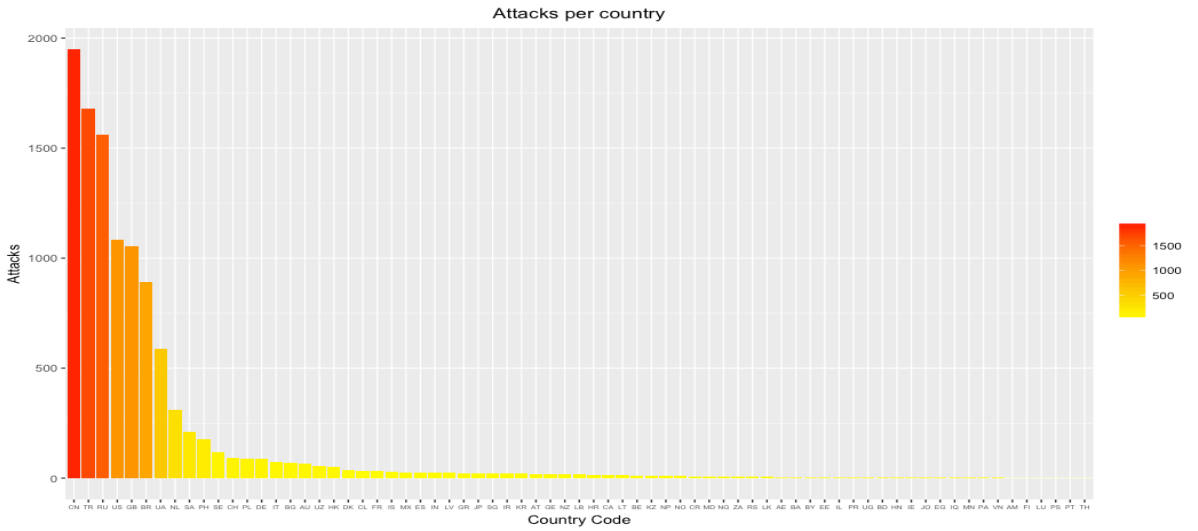

Figure 26: Total number of attacks per country FSO data

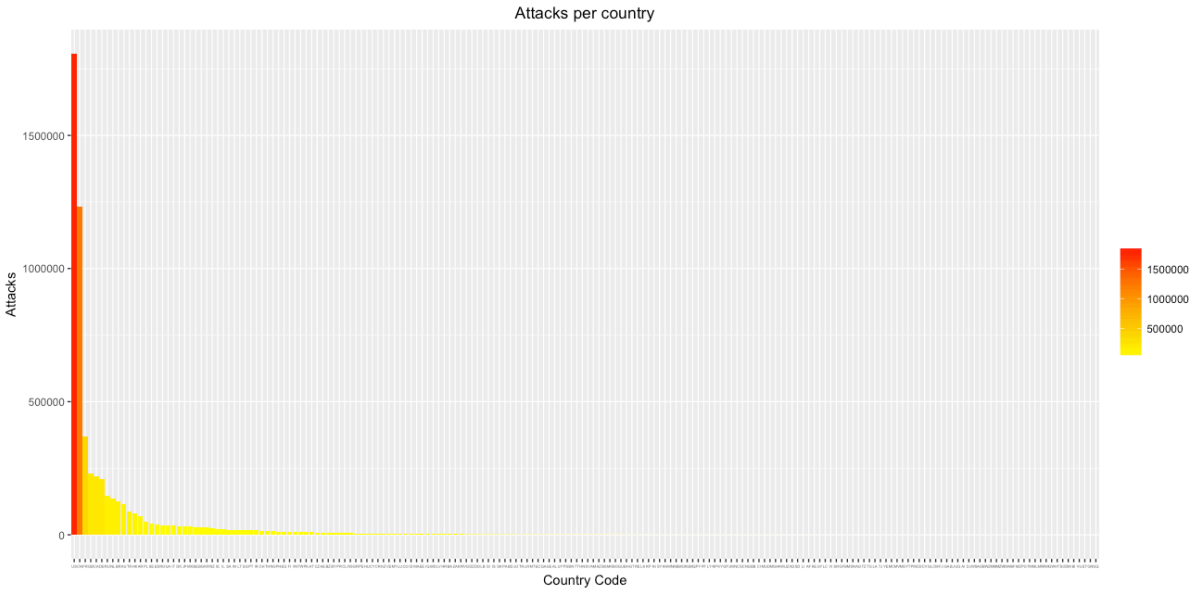

Figure 27: Total number of attacks per country non-FSO data

Appendix E-2 Statistical analysis

The scatterplots in Figure 28 show that there is not relation between the GDP and the number of attacks, as well as the population and the number of attacks. The right graphs are zoomed in

versions of the left graph for a more detailed visualisation. The graphs show no significant pattern, thus can be disregarded for further analysis

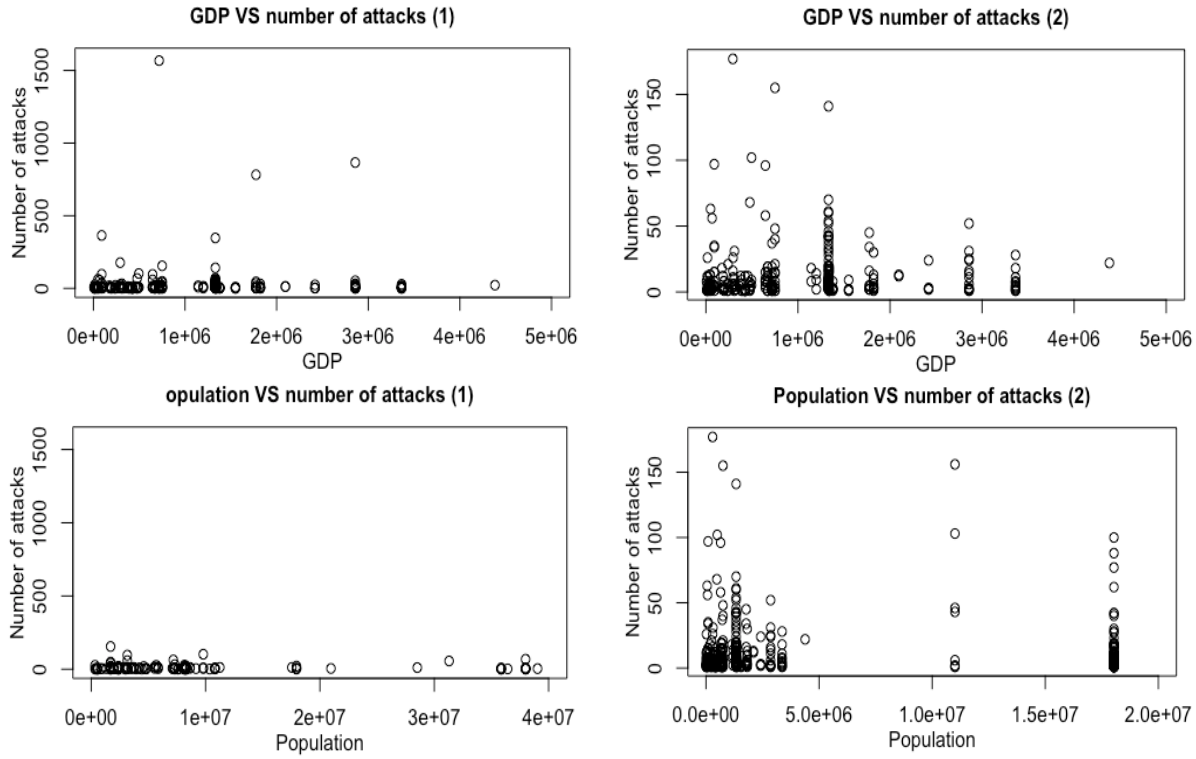

Figure 28: Scatterplots GDP & population against number of attacks

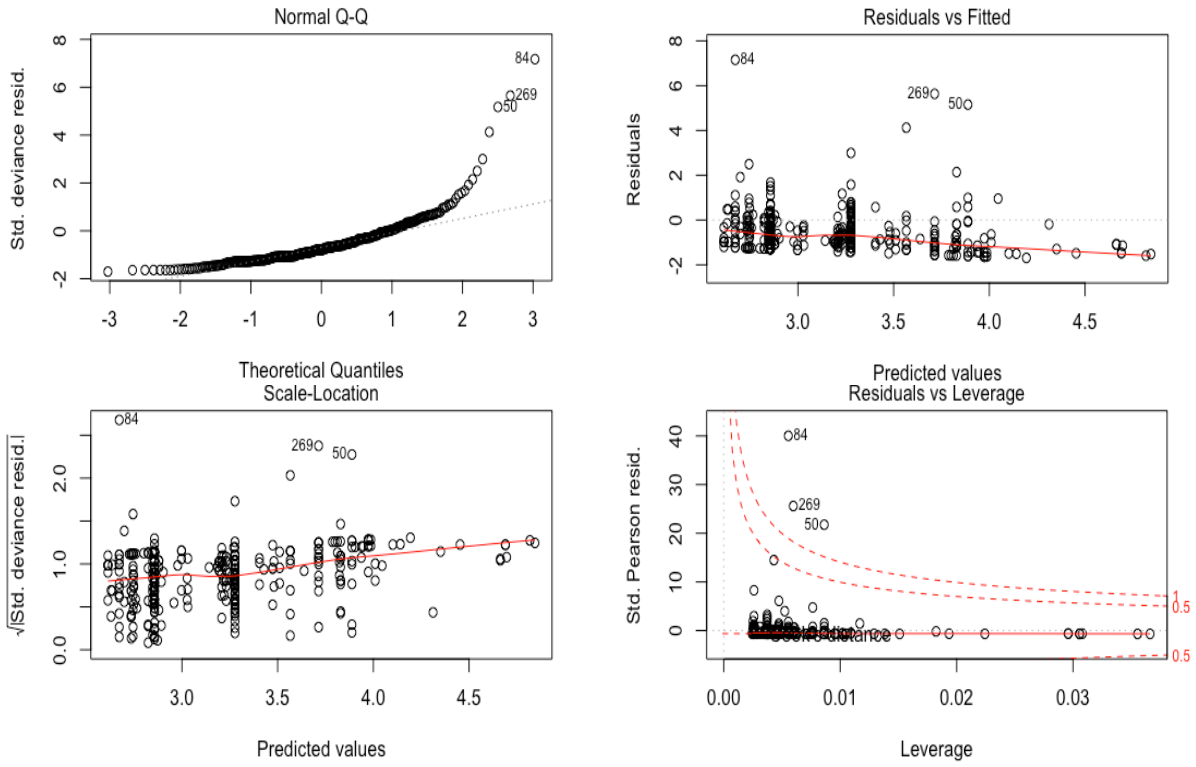

Figure 29: Graphs to check for assumptions linear regression IDI

The normal Q-Q graph shows whether the data is normally distributed. The data is normal distributed if the points are on a straight line. From the graph it can be seen that the data points deviating from the straight line, which implies that the data is not normally distributed.

The Residuals vs. Fitted graph and the scale-location graph provide insight into the reasonability of the linear relationship, the quality of the variance in the error terms and the outliers. With both graphs the homoscedasticity can be tested. For homoscedasticity to occur, both graphs should show no pattern. However, when analysing the graphs, a clear pattern is visible. Taking a closer look at the residual vs fitted graph, the residuals are not distributed randomly around the zero (dotted) line. In addition, the variance of the error terms are not equel. Thus, the assumption of homoscedasticity are not met.

Lastly, the residuals vs. leverage graph provides insight into the influence of the dependent variable (number of attacks). Each value is removed in the next model, and the influence of that point is compared to the previous model with the removed value. If the value is very influential, the point will have a higher leverage value. The function of this graph is to remove points that have a leverage value that are too high, as these points are outliers and will result in outlying effects on the model. However, these points are interesting to analyse as these provide insights into the factors that an organisations holds that have been attacked frequently.

The plot in Figure 30 show similar results as the plots from the IDI, mentioned in the main text. The normal Q-Q plot demonstrates that the data is not normally distributed, as the dots are not on a straight line. The Residuals vs. Fitted and the scale-location graphs illustrate a clustering pattern on the data points. For this reason, the assumption of homoscedasticity is not met. Moreover, the residuals vs leverage graph show two outliers. In order to analyse the data, generalized linear regression needs to be used.

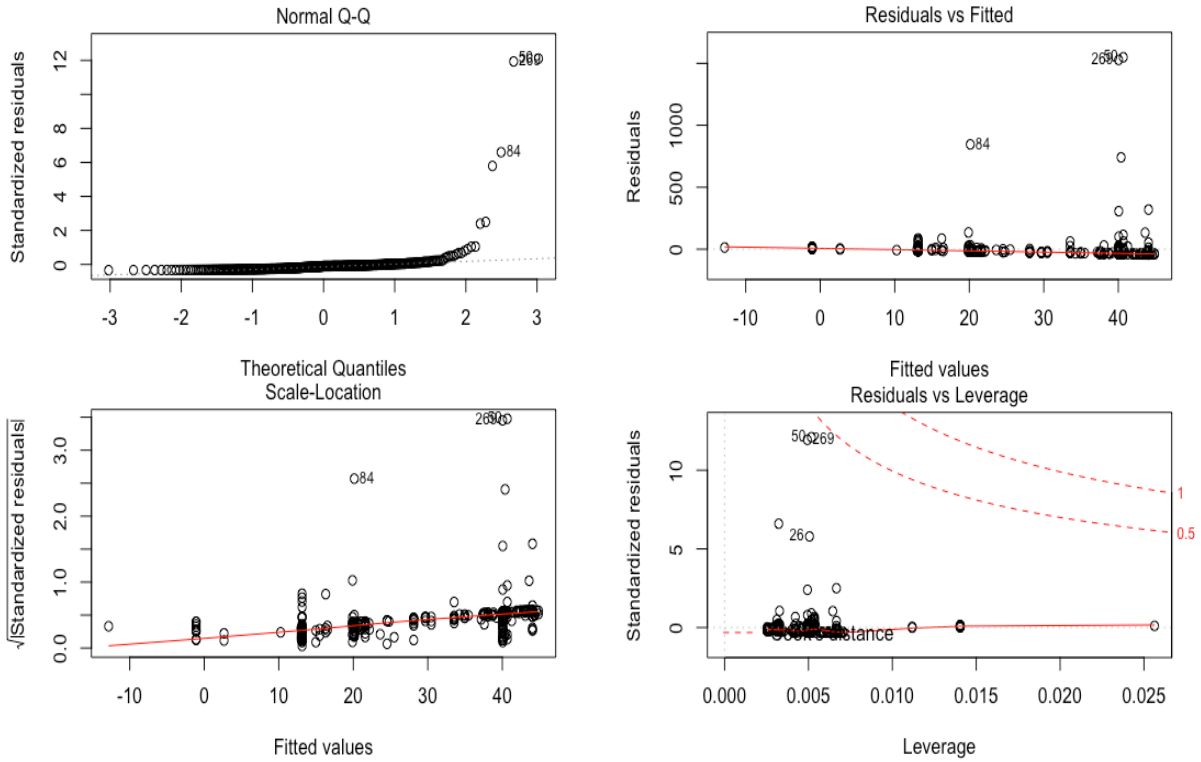

Figure 30: Graphs to check for assumptions linear regression Nominal GDP Per Capita

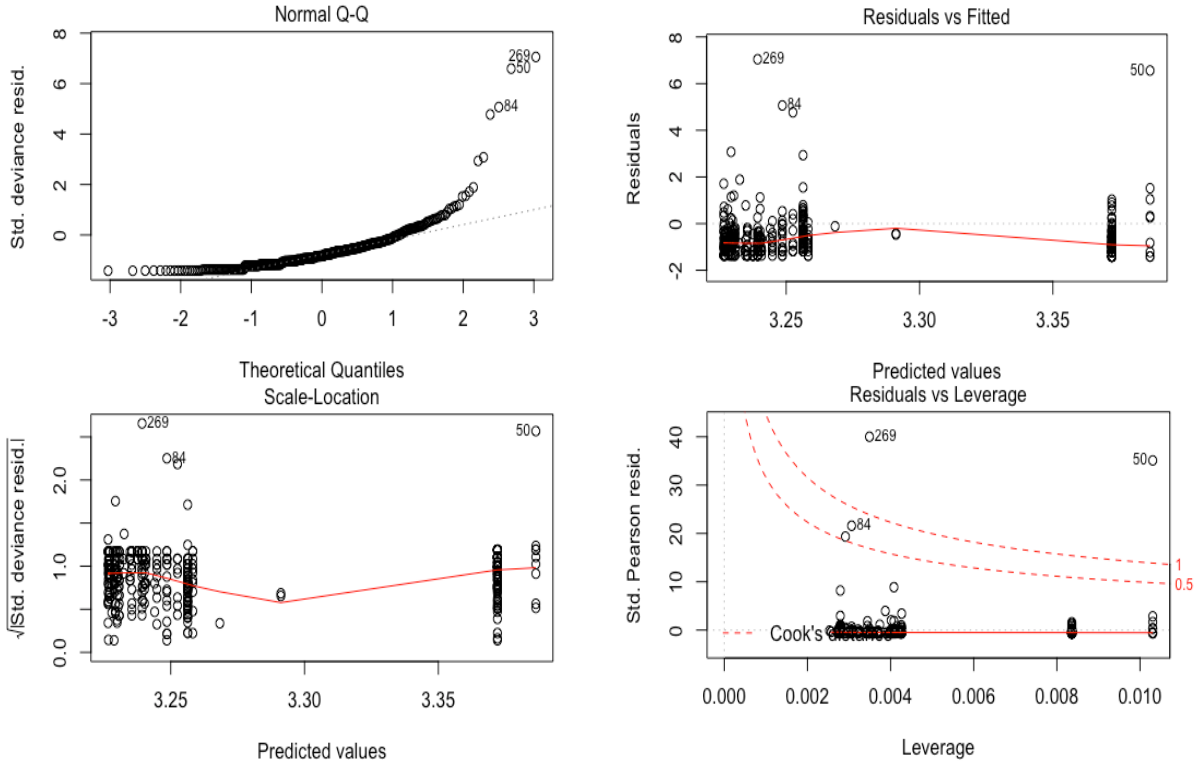

Figure 31: Graphs to check for assumptions linear regression GDP PPP

This table below shows the results of the negative binomial generalized regression for the country-level factor GDP PPP. Since the p-value is not significant (0.42) it can be concluded that there is no significant effect of the GDP PPP on the number of attacks

Table 26: Negative binomial generalized regression GDP PPP

	Dependent Variable:	
	Number of attacks	
	(1)	(2)
GDP PPP (2014)		0.000
		(0.000)
Constant	3.280***	3.227***
	(0.238)	(0.310)
Observations	406	406
Log Likelihood	-1,633.257	-1,632.922
Theta	0.444*** (0.026)	0.444*** (0.026)
Akaike Inf. Crit.	3,268.514	3,269.844
Note:		*p<0.1; **p<0.05; ***p<0.01

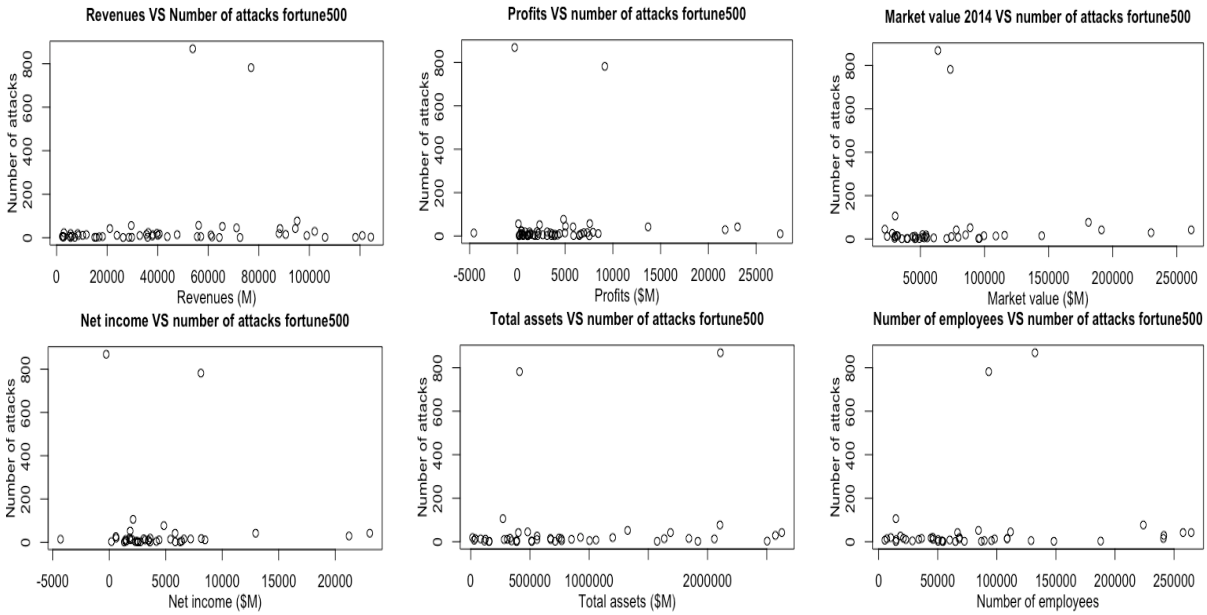

Figure 32: Scatterplots size indicators

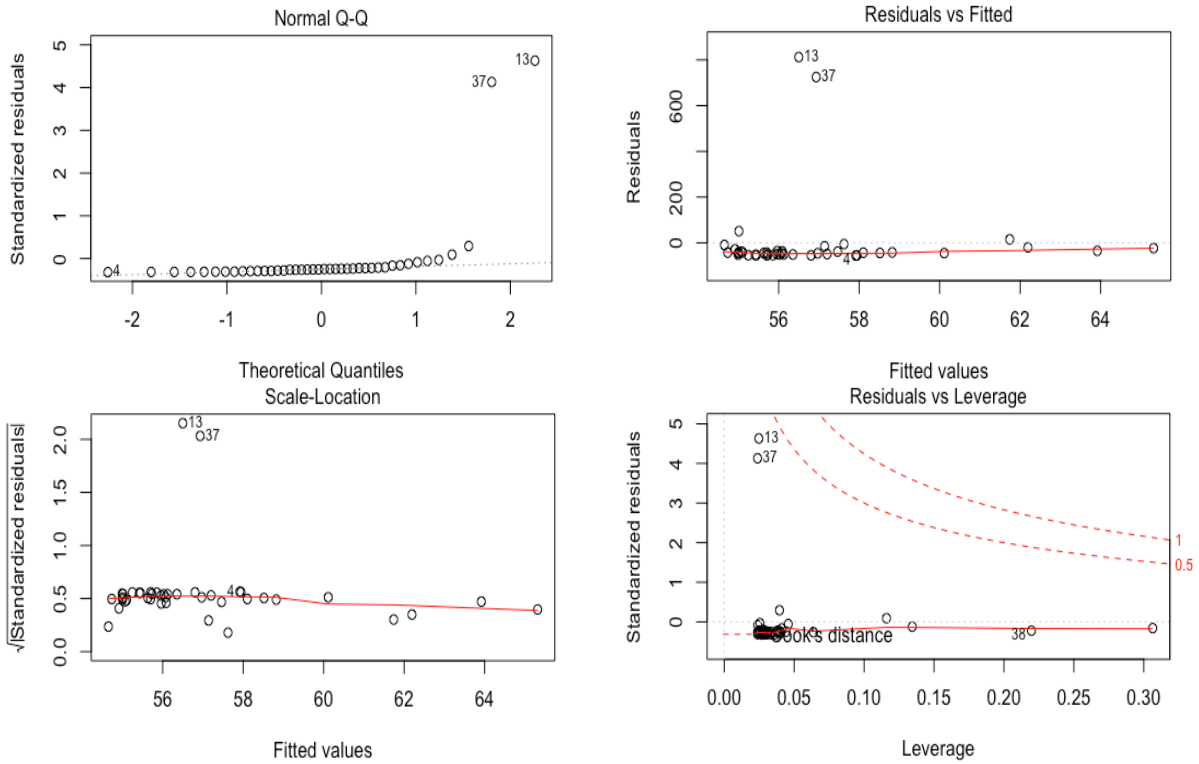

Figure 33: Graphs to check for assumptions linear regression market value

Appendix F Interview

In this section the interview protocol is explained. The interview was conducted in order to gather the qualitative data from experts in the field of cyber security for FSOs. The interview took approximately 1 hour and was semi-constructed to respect the flow of the conversation.

Before interview:

- Introducing myself and my master thesis
- Explaining set-up of the interview
    - Anonymisation of the data if necessary
    - Validation of the answers
    - Permission to record the conversation

Start of the conversation

- General background on the subject of my research
- Explaining the aim of the interview

Start of interview

General questions

1. What is your general viewpoint on DDoS attacks?
2. How often did you suffer from a DDoS attack in the last year?
    a. What part of the company was mostly attacked and why do you think this part?
    b. Do you have a sense of the impact of such an attack?
3. What is your opinion about DDoS attack rates of other companies? Are you aware of being attacked more often than other FSOs or sectors?

Specific questions:

4. Which mitigation strategies does your company use to defend against DDoS attacks, and how did they come into place?
    a. Do you consider those strategies successful? Why/why not?
    b. In case no strategies are being used, what are the reasons for this decision?
    c. Do you think that those strategies are being observed by cyber criminals to launch an attack?
5. What are according to you the types of cyber criminals that mainly try to attack your company?
    a. Can you explain how this information was gathered?
6. What do you expect in regard the ease of use of launching a DDoS attacks
    a. Are you aware of booters?
    b. Plans to change strategy when you knew about booters?
7. What is your expectation on target selection of a cyber criminal?
    a. Based on what (internal/external) factors do cyber criminals focus when they are planning an attack? Or is an attack being executed randomly without taking any factors into account?
    b. What is according to you the importance of external factors that increase the change of being attacked (patches, updates, dependency on clients, dependency on third parties)

End of the interview:

- Are there additional comments?
- Thanking respondent for time.