Targeting financial organisations: a multi-sided perspective

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

R.T.M. Cheung
Faculty of Technology, Policy & Management
Delft University of Technology
Delft, the Netherlands
3 July 2017

Abstract

Currently, DDoS attacks have become inevitable for financial services and their threat keeps rising. Numerous researches have focused on the technical since the rise of DDoS amplification attacks. However, there is less understanding regarding their target selection on financial services. This research uses a mixed method approach to capture factors that influence cybercriminals in their selection of victims. Via data from amplification DDoS honeypots, various factors are identified and explanatory models are provided. In addition, financial cyber security experts are consulted to assess their perspective on target selection. The analysis demonstrates that certain countries have significantly higher or lower victims, which can partially be explained through country level factors such as the ICT development and Normal GDP Per capita. In addition, the ICT development influences the duration of the attack significantly. The findings also indicate that organizational size, as measured by market value, showed a limited effect on the number of attacks. Contrary, experts regarded the size as a highly influential factor. The analyses furthermore demonstrate that financial organisations incur significantly more attacks on Friday than on any other day. Moreover, the experts mention additional target selection factors such as, reputation, media attention, patching, having capable employees, and mitigation parties. Finally, this paper reflects on the implications of these findings for the financial sector and related sectors.

Keywords: Distributed denial of service (DDoS), booters, target selection, cybercrime, mixed method, quantitative analysis, qualitative analysis, financial services, AmpPot.

1. Introduction

The Internet has changed our lives in many ways. It has revolutionized our communication and is involved in almost every 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 [1]. 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 [2], [3]. 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 the rise of a new trend, namely, the rise of DDoS-as-a-service or booters [4]. 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. Nowadays almost everybody, regardless of the attackers' IT knowledge, can command a cyber-attack [5], [6]. Booters have made it irrelevant to have expert knowledge; even attackers with little knowledge, preparation, and resources can cause a high degree of damage. 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 [7]. 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 and duration of attacks, which pose as a greater threat to more resilient companies. As this research focuses mainly on amplification based DDoS attack, purely for the purpose of this research, booters will be used as a synonym to DDoS amplification attacks. It has to be kept in mind that outside this research, booters can be used for all sorts of DDoS techniques.

Contribution. There have already been various in-depth studies on the DDoS landscape as a whole. Numerous researches have focused on the technical side of amplification DDoS attacks. 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 [8], [9]. 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 [10]. Less research, however, has focused on the more socio-technical side of DDoS attacks such as the impact it has on the victims that DDoS amplification attacks target. Due to inabilities of catching attackers worldwide, there still remains a large knowledge gap in the motivations behind the specific DDoS attacks. Furthermore, researches 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 [11]–[13]. However, accurate and complete research that purely focuses on the implication using DDoS amplification techniques on financial organisations is limited. This research tries to fill the gap of the socio-technical side of DDoS amplification attacks for financial services.

This research aspires to provide insight into the specific target selection of DDoS amplification attacks from both the technical as the socio-technical perspective. For this research, target selection is defined as: *The attack choices by the cyber criminal regarding which institutions to attack*. The main objective is to identify factors that influence the target selection of DDoS amplification attacks in the

financial organisations realm. Therefore this research positions itself between the attacker and the victims with an aim to understand the motivation behind cyber victimization.

Paper outline. The paper is organized as follows. In Section 2, we define the methodology that will be used for the research. In section 3 more detail is given on the specific dataset that will be used. Section 4 discusses the current cybercrime landscape in the financial sector. Thereafter, this section sheds light onto the DDoS amplification attacks, how they are currently commoditising, and the target selection factors according to literature. Section 5 tackles the target selection according to the real world dataset. Likewise, section 6 elaborates on the target selection according to the experts. The following section brings the previous results together. Section 8 concludes this paper.

2. Methodology

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 [14]. A mixed method approach will lead to a more multi-dimensional approach that will improve the understanding of what influence target selection.

Quantitative research. The quantitative analysis uses the so-called AmpPot data, which will be discussed later in this paper, as input. The main dataset for this research will consist of a small part of the total AmpPot data, as mainly financial organisations will be the focus. 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 in-depth analysis on the results of the descriptive analysis. For the in-depth 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.

Qualitative research. The qualitative research comprises of data, gathered from various cyber security experts. To do so, the forthcoming results form the quantitative research will be used as input for the semi-constructed interviews. The interviews give a more detailed overview of the practical and social side of the cyber security realm according to the financial sector. A total of 9 experts in the financial sector were interviewed.

Comparing the results. After thorough analyses, both the results of the quantitative and qualitative data will be set side by side. Comparing both datasets will provide insights into how the perspective of the financial sector differs from real world data and how they are concurrent. Nonetheless, several limitations of the mixed method have to be taken into account. Firstly, 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 specifically focused on target selection of DDoS amplification attacks. In addition, issues regarding interpreting conflicting results will need to be taken into account as well.

3. AmpPot data

The fundamental data for this research is provided by the AmpPot data. 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 [15]. 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. Therefore, this research can be considered as a follow-up study. 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.

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

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 the financial service organisation (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. The second approach consisted of using various Internet sources such as Fortune500, Gartner and Forbes, to find additional keywords. 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-FSO 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, I 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.

4. The background

4.1 Cybercrime and financial organisations

The consequences of cybercrime in the introduction 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 [16], 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 organisations firms. Wilson [17] 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 financial organisations has not changed, the landscape in which this occurs has. Until the mid-1990s, the financial sector was relatively simple and reliable [18]. 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, financial organisations have opened up their technical infrastructures to more risks.

While there have been numerous researches and implementations to reduce the risks for financial organisations, the forecast is that cybercrime will only increase in the upcoming years [19], [20]. The increase in cybercrime is a real threat for financial organisations. The business continuity of these organisations is highly dependent on user-trust [21], and with the recent development to provide more services online (e.g. online banking and wireless transactions), new developments in the cyber security realm have to be followed up closely. Among the various sectors, financial organisations are among the top 3 sectors that are being attacked most often by cybercriminals [22].

The trend surrounding the increase of DDoS attacks are similar to all the trends relating to cybercrime for financial organisation. Financial services share the second place of being mostly targeted by cybercriminals in terms of DDoS. In 2014, financial organisations held the fifth place, and thus has moved up into a three-way tie for second place with government and hosting [22]. Among the demand for DDoS services, financial organisations score the highest with government and cloud/hosting providers as second and third place respectively. This concludes that financial organisations are still investing a lot in DDoS protection services.

4.2 DDoS amplification attacks

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 [23]. 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 [15]. According to Rossow [24], 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.

4.3 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 [15], [25]. This increase can be related to the overall increase of the usage of amplification attack methodology [15], [25]. 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.

Even though, building a powerful DDoS infrastructure is rather easy, Karami and Mccoy [6] 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 [26]. 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 [6] . 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 [27]. 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 [26]. 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.

4.4 Target selection factors

Studies have limited discussed factors that can influence the target selection of a DDoS attacks. This section provides insight into those factors. These factors fuel the focus of the upcoming quantitative and qualitative analyses.

Organisation size – 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 [28]–[30]. Tajalizadehkhoob et al. [31] 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. Not all studies agree that size has an effect on the amount of incidents. According to Torres [32] 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 [29].

Context of the organisation – The context of the organisation is related to the country in which the organisation resides. Krämer et al, [15] conclude that amplification DDoS attacks are a global problem, however most victims are located in the US or China. Also Noroozian et al. [33] observed differences between and within countries. They conclude that in a number of countries the victimization for ISPs is lower than for others. In addition, many reports show that well-developed countries do incur more DDoS attacks than others [4], [22], [29].

Technical innovativeness - 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 [34]. When FSO 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 [35], [36].

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 [37], [38]. 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 [39].

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 [15], [40]. These experts need to be capable to countermeasure the attack and In order to minimize financial and reputation losses [41] 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 [12], [42]. Not only on operational level, expertise is required, also cyber security expertise in organisation boards is necessary [43].

Communication structure – Security has been and viewed as a nuisance for the business, but this can be changed with better communication and alignment [44]. The manner in which information security is communicated can strongly influence how it is influenced and whether and how it is acted upon [45]. 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 [40], [46].

Shared responsibilities- Many security responsibilities cannot be performed by single person or a dedicated security person [40]. Having shared responsibilities is therefore necessary and have proven to be quite satisfactory in practice [47]. Having shared responsibilities can result in better communication and cyber governance.

Speed of updating, patching – Patching is an important factor that can limit the amount of live botnets, and thus also limits the amount of DDoS attacks [48], [49]. 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 [50], 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 [51].

(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 [52]. Bougaardt & Kyobe [41] 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. 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[44], [52].

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 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. Somani et al. [36] 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 [45], [53].

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 [48], [54]. 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 [40].

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.

5. Target selection according to AmpPot

This section will provide insight in the factors of target selection according to financial organisation attack data that was extracted from the AmpPot dataset. 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 a sensitivity analysis to validate the financial dataset. 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 Sensitivity analysis

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.

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 1. 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 (see Figure 1) 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.

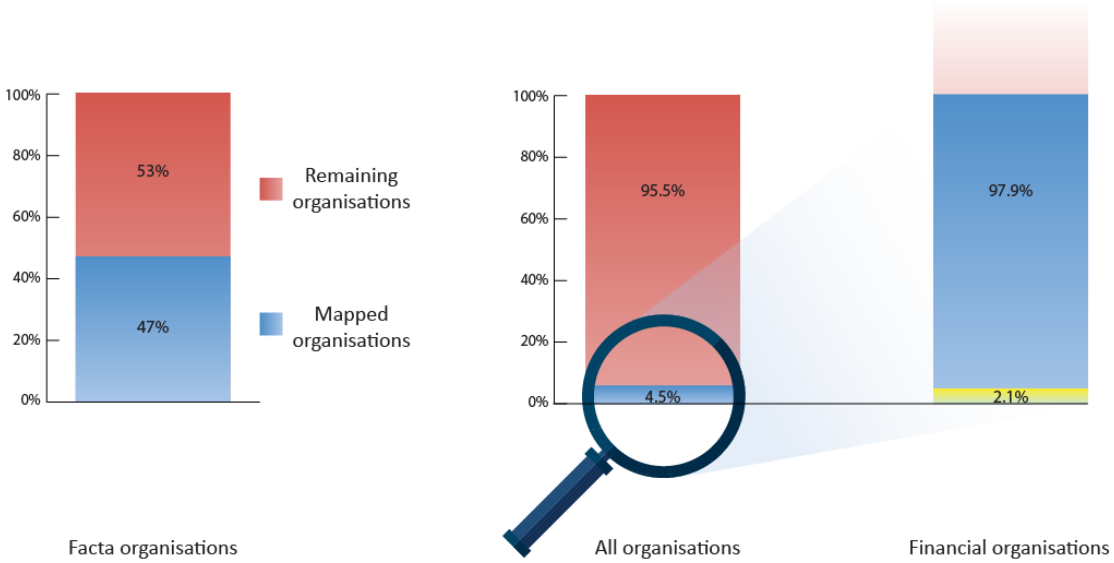

Figure 1: Bar plots mapped financial organisations

5.2 Descriptive analysis

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 attack ratio 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. Understanding the types of protocol gives insight into the ease of use or abuse rate of the various protocols and whether there should be a focus on a specific protocol. The data shows that 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. Important to note is that the difference between DNS and NTP use is much bigger compared to the non-financial data, implying that DNS is especially popular among attackers on financial institutions. According to Krämer et al [15], DNS stands out as most other protocols can be filtered due to the fact that they have little benign use on the Internet (CharGen, QOTD and SSDP).

Organisation size. Exploring the data showed that per protocol the most frequently attacked organisations are Fortune500 listed organisations. Going into more detail, 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. The data clearly shows that the most frequently attacked organisations are banks. Aside from PayPal, all the Fortune500 listed organisations are banks, with a large non-Fortune500 bank (AKBANK TAS) as well. 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 researches and cyber security companies have also

mentioned the influence of organisation size (see 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.

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. The data shows a similar result (see Figure 2). While the USA and China were most targeted for the non-financial data, the outcome is different from the financial dataset. The data demonstrate 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 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.

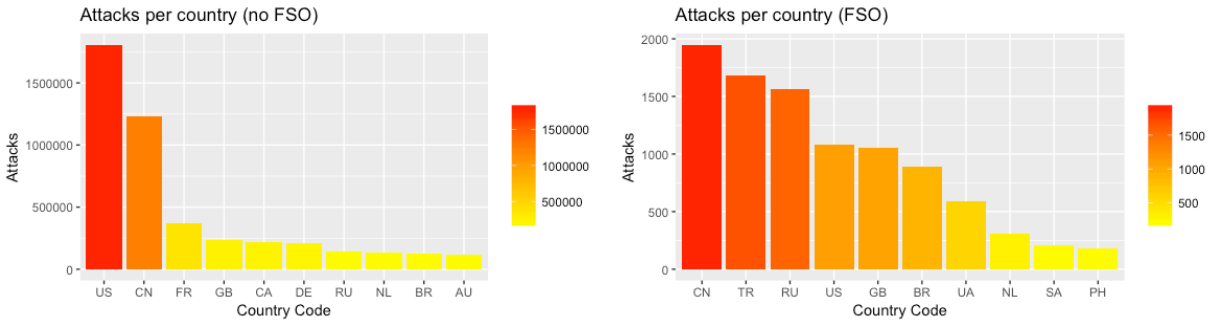

Figure 2: Total number of attacks per country no FSO and FSO data

To obtain a better understanding of the type of top countries that were attacked, factors that explain the ICT development and economic status were gathered. To consider the influence of each country, country-level factors such as the gross domestic product (GDP), normal GDP per Capita, Gross domestic product at purchasing power parity (GDP PPP), and the ICT development index (IDI) are added to the dataset. 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.

Weekday. The financial organisation attack data demonstrates a substantial different distribution of the attacks per weekday. Figure 3 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. 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 currently information on whether the employee utilisation is different during the weekends for financial organisations, no clear explanation can be given.

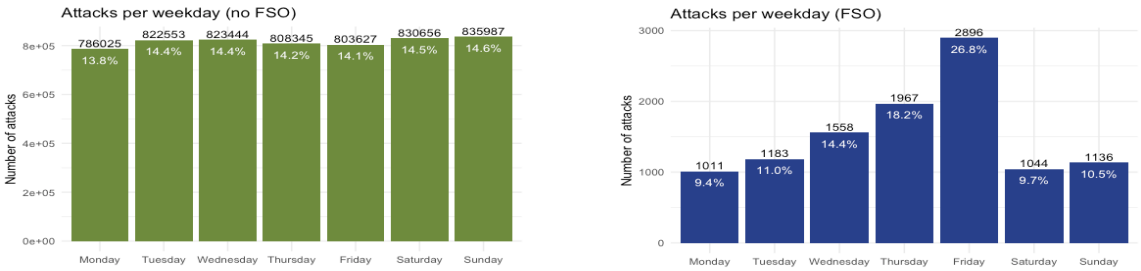

Figure 3: Distribution DDoS amplification attacks per weekday

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 the company is manifested in, the 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 the attack duration.

Explanatory analysis type of country

The previous section 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 2, 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.

Table 1 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.

Table 1: 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

$Model_3$ 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 [55]. 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 2. 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 [56]. The factor GDP PPP showed no significant p-value and thus does not significantly influence the number of attacks. Due to the correlation between the IDI and Nominal GDP Per Capita are not included in one model.

Explanatory analysis organisation size

The descriptive analysis shows that Fortune500 listed financial organisations are more often being attacked compared to non-Fortune500 listed organisations, from which the assumption was drawn 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 compare both subsets of the data, t-tests were performed to observe if there is a significant difference between both the groups. Based on the results, no significant difference was observed in terms of their number of attacks (see Table 2).

Table 2: Student's t-test duration 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

Influence organisation size indicators on number of attacks

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. To determine whether the size indicators influence the number of attacks, scatterplots were conducted. These scatterplots showed only patterns for the profits, market value, and net income. In order to dive deeper into the patterns, a student t-test was performed to test if these indicators hold a significant difference. The data was divided into two groups for each indicator. These groups are made according to the scatterplots where the clustered points are compared with the rest of the data points. After conducting a student t-test only the market value showed a significant difference, within its groups. To consider the effect of the market value on the number of attacks a generalized linear regression analysis was conducted. A summary of the analysis is presented in Table 3. 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, this effect is not large enough to make any strong claims.

Table 3: Negative binomial generalized 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	

6. DDoS in the financial sector according to experts

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. Due to the sensitivity of the data, all the data have been anonymised. Table 4 in the appendix provides an overview of the respondents and their role, function and expertise level.

6.1 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 financial organisations are targeted outside the obvious motivations (extortion, online statement). This part will describe the factors that are related to the characteristics of organisations.

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 [57] 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.

6.2 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 financial organisation.

Organisation size. The size of a financial organisation 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, Logically, large financial organisations 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. [58]. As DDoS impacts the services provided by the financial organisation, the number of clients is an important factor in terms of size of a financial organisation, 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 financial organisation got. The larger the financial organisation, the more frequent they were attacked (daily basis) while the smaller financial organisation had a significantly lower attack rate [BA4, BA5]. *"Large financial organisations experience DDoS attacks everyday. However, due to the mitigation strategies, large financial organisations are not affect by the attacks"* [BA4].

Reputation. Having a bad reputation 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. One of the factors that influence the reputation is the investment portfolio or corporate social responsibility, such as cooperating with arms manufacturers. "*Corporate social responsibility is an factor that is of great importance for target selection. This factor will definitely influence target selection"*[BA2]. 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. The media attention is among the top mentioned factors by the respondents [BA3, BA4, BA5, IE1, IE2]. If a financial organisation 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 financial organisation was mentioned in the media frequently during a period. According to these experts, financial organisations 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 organisation 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. 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 a financial organisation. 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 financial organisation 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 financial organisations 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.

7. Comparing the results

In this section, the results of the quantitative and qualitative analysis presented in the previous sections are contrasted. Since the AmpPot data is more technically oriented and the interviews are more socio-technically oriented, this section provides insight into how both analyses complement each other.

7.1 (In) consistencies

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.

Type of organisation. The AmpPot data revealed that most attacked financial organisations 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 financial organisations are being targeted, such as insurance companies.

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 interviewees mentioned that especially large banks are getting attacked more often than smaller sized banks. However, the 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.

Recognized organisation. As most of the top 10 frequently targeted financial organisations 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.

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, 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. 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.

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 data 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.

8. Conclusion & discussion

8.1 Implication

The main objective of this research was to identify factors that influence the target selection of financial organisations. Section 5 has identified various factors according to the AmpPot data. Among them the IDI and market value showed the most significant effect. The organisation size also showed an effect, though limited. In addition, the qualitative analysis in section 6 showed various factors, similar to the AmpPot data. Also new factors such as media attention were added to the list. Though, due to the difference in scope of both analyses, comparing the results was inherent of discrepancy. Section 7 revealed how the results were concurrent, and could complement one another. Thus, the conclusion is that the research objective is fulfilled.

What do these findings mean for the consequences of financial institutions and the threat landscape as a whole? There are some actions that financial organisations have to take into account when defending against target selection. Firstly, 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. Secondly, 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. Thirdly, 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. Fourthly, banking institutions should allot as such attention to the origins of the attack as to mitigating the damages caused by attacks. Lastly, 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.

While actions regarding financial organisations are important, the DDoS landscape is expanding to an extreme extent. To contain the current and increasing threat of DDoS, actions should not be limited to solely financial services. One important aspect to understand the motivation behind the attacks is to prosecute cybercriminals. This asks for a close cooperation between organisations and law enforcement institutions. In addition, As DDoS are increasing in power, inter-sectorial cooperation should be stimulated. An example could be cooperation between ISPs and financial institutions to be able to exclude between traffic from different countries or continents. Sharing knowledge both within and between sectors is encouraged. Organisations should share information about the reasons behind the attack, from which IP, and the bandwidth.

8.2 Suggestions for future research

As the research was initiated considering the boundaries defined by limitations, the following suggestions 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

[1] J. Armin, B. Thompson, D. Ariu, G. Giacinto, F. Roli, and P. Kijewski, “2020 cybercrime

economic costs: No measure no solution," *Proc. - 10th Int. Conf. Availability, Reliab. Secur. ARES 2015*, pp. 701–710, 2015.

[2] C. S. Alvarez, "Amplified DDoS Attacks: The current Biggest Threat Against the Internet." [Online]. Available: https://www.icann.org/news/blog/amplified-ddos-attacks-the-current-biggest-threat-against-the-internet. [Accessed: 26-Oct-2016].

[3] P. Holl, "Exploring DDoS Defense mechanisms," no. March, pp. 1–10, 2015.

[4] J. J. Santanna, R. Van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras, "Booters - An analysis of DDoS-as-a-service attacks," in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 2015, pp. 243–251.

[5] M. De Groot, "Unveiling Weaknesses of Booters," 2015.

[6] M. Karami, Y. Park, and D. McCoy, "Stress testing the Booters: Understanding and undermining the business of DDoS services," *Arxiv*, pp. 1033–1043, 2015.

[7] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, "Detecting DNS amplification attacks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5141 LNCS, no. October 2002, pp. 185–196, 2008.

[8] M. Karami and D. Mccoy, "Understanding the Emerging Threat of DDoS-As-a-Service," *LEET '13 Usenix*, pp. 2–5, 2013.

[9] J. J. Santanna, R. Durban, A. Sperotto, and A. Pras, "Inside booters: An analysis on operational databases," *Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015*, pp. 432–440, 2015.

[10] J. Van Den Berg, J. Van Zoggel, M. Snels, M. Van Leeuwen, S. Boeke, L. Van De Koppen, J. Van Der Lubbe, B. Van Den Berg, and T. De Bos, "On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education," *NATO STO/IST-122 Symp. Tallin*, no. c, pp. 1–10, 2014.

[11] R. Turner, "Tackling the DDoS Threat to Banking in 2014," 2014.

[12] S. T. Zargar, J. Joshi, D. Tipper, and S. Member, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS)," vol. 15, no. 4, pp. 2046–2069, 2013.

[13] A. Pras, J. J. Santanna, J. Steinberger, and A. Speretto, "DDoS 3.0-How terrorists bring down the Internet," *Int. GI/ITG Conf. Meas. Model. Eval. Comput. Syst. Dependability Fault Toler.*, pp. 1–4, 2016.

[14] J. Mason, "Mixing methods in a qualitatively driven way," *Qual. Res.*, vol. 6, no. 1, pp. 9–25, 2006.

[15] L. Krämer, J. Krupp, D. Makita, T. Nishizoe, T. Koide, K. Yoshioka, and C. Rossow, "AmpPot: Monitoring and defending against amplification DDos attacks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9404, pp. 615–636, 2015.

[16] PWC, "Economic crime: A threat to business globally," 2014.

[17] Wilson, "Every minute of every day, a bank is under cyber attack," 2013. [Online]. Available: http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10359563/Every-minute-of-every-day-a-bank-is-under-cyber-attack.html. [Accessed: 03-Nov-2016].

[18] A. R. Raghavan and L. Parthiban, “The effect of cybercrime on a Bank ’ s finances,” *Int. J. Curr. Res. Acad. Rev.*, vol. 2, no. 2, pp. 173–178, 2014.

[19] A. Nagurney, “A multiproduct network economic model of cybercrime in financial services,” *Serv. Sci.*, vol. 7, no. 1, pp. 70–81, 2015.

[20] EY, “Achieving resilience in the cyber ecosystem Rise of the cyber ecosystem,” *Insights governance, risk compliance*, no. December, 2014.

[21] E. Verschuur, “strategic feasibility of NFC mobile payments in the Netherlands? How the individual strategies of stakeholders affect the NFC mobile payment ecosystem as a whole,” 2012.

[22] Arbor Networks, “World Wide Infrastrucure Security Report 2015,” 2015.

[23] J. Krupp, M. Backes, and C. Rossow, “Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks,” no. i, pp. 1426–1437, 2016.

[24] C. Rossow, “Amplification Hell: Revisiting Network Protocols for DDoS Abuse,” *Proc. 2014 Netw. Distrib. Syst. Secur. Symp.*, no. February, pp. 23–26, 2014.

[25] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, “Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks,” *Imc*, pp. 435–448, 2014.

[26] M. Karami, “Understanding and undermining the business of DDoS booter services,” 2016.

[27] Imperva, “Global DDoS Threat Landscape,” *Glob. DDoS Threat Landsc. Q1 2016*, 2016.

[28] T. Matthews, “Incapsula Survey: What DDoS Attacks Really Cost Businesses,” 2014.

[29] Arbor Networks, “Worldwide Infrastructure Security Report 2016,” 2016.

[30] A. Briney and F. Prince, “Does Size Matter ?,” no. September, 2002.

[31] S. Tajalizadehkhoob, H. Asghari, C. Gañán, and M. van Eeten, “Why Them? Extracting Intelligence about Target Selection from Zeus Financial Malware,” *Work. Econ. Inf. Secur.*, pp. 1–26, 2014.

[32] A. Torres, “Incident Response : How to Fight Back,” *Sans Inst.*, no. August, p. 28, 2014.

[33] A. Noroozian, M. Korczy??ski, C. H. Ga??an, D. Makita, K. Yoshioka, and M. Vaneeten, “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)*, 2016, vol. 9854 LNCS, pp. 368–389.

[34] R. Preyadharsini and K. Deepa, “Duplicate Record Detection Using Progressive Sorted Neighborhood Method,” *Avinashilingam*, no. February, 2016.

[35] A. Bakshi and B. Yogesh, “Securing cloud from DDOS attacks using intrusion detection system in virtual machine,” *2nd Int. Conf. Commun. Softw. Networks, ICCSN 2010*, no. fig 1, pp. 260–264, 2010.

[36] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, “Service resizing for quick DDoS mitigation in cloud computing environment,” *Ann. des Telecommun. Telecommun.*, pp. 1–16, 2016.

[37] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions,”

Comput. Secur., vol. 30, no. 8, pp. 719–731, Nov. 2011.

[38] L. E. Cohen and M. Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach A ROUTINE ACTIVITY APPROACH*," *Source Am. Sociol. Rev. Am. Sociol. Rev.*, vol. 44, no. 44, pp. 588–608, 1979.

[39] F. Ngo and R. Paternoster, "Cybercrime Victimization: An examination of Individual and Situational level factors.," *Int. J. Cyber …*, vol. 5, no. 1, pp. 773–793, 2011.

[40] J. Pescatore, "DDoS Attacks Advancing and Enduring : A SANS Survey," *SANS AInstitute InfoSec Read. Room*, 2014.

[41] G. Bougaardt and M. Kyobe, "Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa," *Electron. J. Inf. Syst. Eval.*, vol. 14, no. 2, pp. 167–178, 2011.

[42] S. Jin and D. D. S. Yeung, "A covariance analysis model for DDoS attack detection," *Commun. 2004 IEEE Int. …*, vol. 4, no. c, p. 1882–1886 Vol.4, 2004.

[43] Y. Pierrakis and L. Collins, "Banking on Availabilty," no. April, pp. 1–43, 2013.

[44] K. Kark, R. a. Dines, S. Balaouras, and L. Coit, "Security Organization 2.0: Building A Robust Security Organization," p. 18, 2010.

[45] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, "Human Factors and Information Security : Individual , Culture and Security Environment," *Sci. Technol.*, no. DSTO-TR-2484, p. 45, 2010.

[46] M. Lagazio, N. Sherif, and M. Cushman, "A multi-level approach to understanding the impact of cyber crime on the financial sector," *Comput. Secur.*, vol. 45, no. 0, pp. 58–74, 2014.

[47] S. W. Brenner, "'At light speed': Attribution and response to cybercrime/terrorism/warfare," *J. Crim. Law Criminol.*, vol. 97, no. 2, pp. 379–476, 2007.

[48] C. Wueest, "The continued rise of DDoS attacks," pp. 1–31, 2014.

[49] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1073–1080, 2012.

[50] E. Rescorla, "Is finding security holes a good idea?," *IEEE Secur. Priv.*, vol. 3, no. 1, pp. 14–19, 2005.

[51] E. Rescorla, "Security Holes... Who Cares?," *Proc. 12th USENIX Secur. Symp.*, pp. 75–90, 2003.

[52] S. Kraemer, P. Carayon, and J. Clem, "Human and organizational factors in computer and information security: Pathways to vulnerabilities," *Comput. Secur.*, vol. 28, no. 7, pp. 509–520, 2009.

[53] J. (2003) Wilson, M., & Hash, "Building an Information Architecture Checklist," *Organization*, vol. 2, no. 2, pp. 1–70, 2003.

[54] D. Kelley, "Insights from the 2016 IBM X-Force Threat Intelligence Report," 2016.

[55] International Telecommunication Union (ITU), *Measuring the information society report: 2014*, vol. 8, no. 3. 2014.

[56] B. Karabacak, S. Ozkan Yildirim, and N. Baykal, "Regulatory approaches for cyber security of critical infrastructures: The case of Turkey," *Comput. Law Secur. Rev.*, vol. 32, no. 3, pp. 526–539, 2016.

[57] E. L. Deci and R. M. Ryan, "Commentaries on 'The "What" and "Why" of Goal Pursuits: Human Needs and the Self-Determination of Behavior,'" *Psychol. Inq.*, vol. 11, no. 4, pp. 269–318, 2000.

[58] D. van Moorsel, "Target selection regarding financial malware attacks within the Single Euro Payments Area," 2016.

Appendix

Table 4: 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