Hunting Booters

Analysing the DDoS phenomenon from the point of view of law enforcement

Jan P. Koenders

TU Delft

j.p.koenders@student.tudelft.nl

November 22, 2016

Abstract

DDoS attacks are one of the most prevalent and widely spread type of cyber attack, targeting thousands of internet users and organisations every day. The Dutch police records official reports and investigates DDoS attacks, yet does not know what their sample of the DDoS environment looks like and how it compares to the population as a whole. In this article the reseacher compares and joins the police data-set to a honeypot data-set dubbed AmpPot. Analysis of the data-sets shows that attackers have very little technical knowledge and that the DDoS phenomenon is in the middle of a commoditisation, allowing almost everybody to execute an attack. Furthermore, the police case files differ widely in quality and as such often lack vital investigative information. A comparison of the two data-sets indicates that the victim demographics are different yet other matricies such as duration and protocol usage are the same, which can be attributed to a standardised DDoS as a service environment. In the future a international selection of law enforcement data-bases should be added in order to get a more extensive data-set and to compare the validity of law enforcement databases against the DDoS environment as a whole to allow for comparison between countries.

I. Introduction

Throughout the four-some decades the internet has existed [1], it has gone through a myriad developments and evolutions. It quite possibly represents one of the biggest developments in recent history, which not only changed peoples lives around the world, but also did so at an incredible pace [2]. Major societal change seldom comes without issues and trouble makers, the internet is no exception to this rule. Cyber- and cyber enabled crime have been on national and international news for years now [3] [4] [5], more often than not the articles speak of major outages of vital infrastructure or banking services. Underlying these outages are often a simple attack methodology called Distributed Denial of Service attack or short DDoS [6] [7]. DDoS attacks work by overloading a certain system or service with illegitimate traffic such that legitimate users will not be able to access them [8].

While 20 years ago DDoS attacks were still in their infancy, and only used by highly capable criminals or activists, they are now the prime example of the commoditisation of cyber crime [9]. Attacks can be bought online via paypal or using cryptocurrency and only require a target IP address to be executed through so called booter services[10]. In fact DDoS attacks executed via one of the cyber crime for service platforms have been noted by many high school age teenagers to be an almost daily occurrence. The result of these attacks are large financial losses on the side of the victim, be it due to loss of potential customers or protection services to mitigate the attack. While hacktivisim or a simple joke used to be the prime reasons for attackers to execute DDoS attacks, intentions have changed and DDoS for bitcoin or in other words extortion with threat of a DDOS attack has become a frequent reality.

A lot of research has been done on the DDoS phenomenon, in particular the technical methodologies used to execute these attacks such as the usage of botnets and amplifiers or

reflectors as well as the combination of the two [11] [12] [13]. Likewise, mitigation techniques such as filtering malicious requests or identifying compromised bots have been analysed many times by academia around the world [14] [15] [16]. Less focus has however been given to the attackers and the victims themselves. This research does just this by taking the unique opportunity of viewing the DDoS problem from the point of view of the Dutch police and comparing that to known DDoS statistics. The purpose of this is to get understanding of what kind of DDoS attacks are being reported to the police and as such define the view of law enforcement in the Netherlands. To reach this goal, the following two research questions will be answered:

What do DDoS attacks reported to the Dutch police look like and how can these cases be classified?

How does the Dutch police data compare to data available about the DDoS population as a whole and what insights can be gathered by combining the two?

Section two of this paper discusses the methodologies used to both query as well as analyse the data-set. The results of the police case file analysis are presented in section three, while section four discusses the differences between the police data as well as the AmpPot data. Section five goes into the return of investment on the side of the attacker, meaning how much damage can a certain investment into a booter service result in. To finish off, section six will facilitate the discussion and conclusion.

II. Methods

Central to this paper and to answering the above stated research questions is the data analysis of two data-sets. The first data-set is the administrative system of the Dutch national police, containing all case files recorded by police officers around the country. To get a DDoS specific data-set from the administration system a querying methodology was developed utilising a number of keywords as well as various types of categorical features of the system. The keywords were developed in two ways, first a visit was payed to a regional police force to discuss various DDoS cases and how they were investigated. From these discussions in conjunction with a number of test searches one could deduce that officers, depending on their knowledge level, would either simply use the name such as "DDoS", "Denial of Service" or any synonym, describe the tool used to execute an attack such as stress, amplifier or booter, or would simply describe the symptoms resulting from the attack on the side of the victim such as "network down", "server down" or "network outage". The final collection of keywords used to extract the data-set was defined as follows: dosaanvallen, DDoS, dos, dos, Denial of service, flooding, flood, booted, booter, stressed, stresser, amplification, platleggen, netwerkaanval. The categories used to filter the results were based on all categories used for cyber related cases such as the cyber crime category and the fraud category. The final result of this methodology is an overview of cases that matched the various criteria. Naturally, many of these cases were false positives due to one of the keywords being mentioned in a non-DDoS related case. A big offender in that regard was the keyword "DoS", as it yielded cases that would mention a "DOS prompt" referring to the Microsoft command prompt. To filter the mentioned cases and to delete them from the final set, all case were read, finally yielding a data-set of 209 cases.

The reason for this extensive methodology lies in the age of the administrative system and with it the limited possibilities for officers to categorise a cyber crime case correctly [17] [18], as well as the limited knowledge of officers which hence limits the quality and use of proper teams in the official reports they create. The second data-set is the AmpPot data as collected by Krämer, et al. [19] and supplemented by Arman Noroozian [20]. This data-set consists of logs of amplification attacks gathered via eight honeypots set-up to collect data on six of the most popular amplification protocols,

namely: DNS, NTP, CharGen, SSDP, SNMP and QoTD.

The police administrative system is built on plain-text case files, supplemented with a number of limited categorical features. Most of these targeting more traditional types of investigative clues such as a description of the location where the a crime occurred as well as the exact date and time. Due to this, categorising and analysing the case files had to be done by hand, meaning all 209 cases files were read manually. The AmpPot data-set allowed for more automated work, as all data was already neatly parsed into a database allowing for quick analysis via the Python add-on Pandas. Since the data-set was created by logging the activity on a number of honeypots impersonating amplification servers, the data contains multiple data-points per DDoS attack. For example three different honeypots may show an attack on one IP address all at the same time utilising the same protocol. One may assume this to be one attack that utilises all three honeypots as an amplifier, since the combination of factors is so unique. Thus, throughout the analysis an attack is defined as all connections made with the unique combination of target IP, protocol used and the date and hour the attack started on. To trace attacks from the police data to the AmpPot data-set, a bash script using regular expressions was used to extract all victim IPs and the corresponding attack times noted in the police reports. These could in-turn be crossmatched to data-points in the AmpPot data-set.

III. Findings I

Analysing the DDoS cases on a general descriptive level, one may identify a number of basic statistics as represented in table 1. As such, of the 209 cases gathered from the police system, 144 cases fall into the 2 year period of 2014-2015 in which the AmpPot data was recorded. In 34 of the 209 cases was a victim IP noted while 27 mentioned a suspect throughout the investigation. In only 21 cases did the report state any attack specifics such as the protocol used or the amount of packages arriving.

Table 1: *Summary of cases gathered from police system*

Queried for analysis	209
2 year period 2014-2015	144
2014	58
2015	86
Victim IP is mentioned	34
Suspect is mentioned	27
Attack vectors mentioned	21

In his paper Jose Nazario [21] noted 5 types of- or motivations for attacks: Home user attacks to nag or anger somebody, retaliation attacks on anti-spam/anti DDoS instances, extortion attacks, attacks on internet infrastructure such as DNS servers, and politically motivated attacks. In his eyes these types can be deduced by looking at the victims that were attacked as well as the strength of the attack. Utilising the inherent structure of the police reports, as described prescribed by in the criminal law (Wetboek van Strafvordering) and more specifically in article 163, one can execute the very same methodology as used by Nazario to check whether these types are present in the Dutch police data-set as well. In addition to the information used by Nazario, the police case files yield both the personal insight of the victim as well as 21 interviews with the attackers themselves, hence allowing for a more detailed approach. Analysing the case files in said way, shows that two of Nazario's categories don't show up in the police data at all, namely the attacks on anti-spam/anti DDoS instances and attacks on internet infrastructure such as DNS servers. Politically motivated attacks do in fact occur, however they are very limited in their quantity and only represent relatively ineffective attacks. Both the home user attacks to nag or anger somebody as well as the extortion attacks are very much present in the attacks. Generalising the attacks much like Nazario, the categories would take the following shape:

High school curiosity, denoting teenagers playing with booter services to see what happens and to nag one another by "turning off

the internet" temporarily. This category of attackers doesn't have malicious intent and often simply acts out of boredom. Secondly, there are the gamers and bullying attacks, these attacks lead back to the origin of DDoS cases where players of online video games DDoSed each other in order to gain a competitive advantage over another [10]. The bullying is a more serious type, often executed by the same age-group, resulting in teenagers being pressured to do things often also relating to online gaming. Lastly there are the extortion cases, these cases are often synonymous with the DDoS for Bitcoin movement often noted on national news, where large organisations or hospitals are extorted with the threat of a large DDoS attack. These extortion attacks, while clearly executed with criminal intent, barely lead to actual attacks and more often than not are sent by people trying to bluff their way into a big payday.

Categorising the attacks by their victim demographic demonstrates that almost half of the cases are focused on companies, while both the educational and home broadband victims represent about a quarter each, tailed by a small group of attacks on governmental targets.

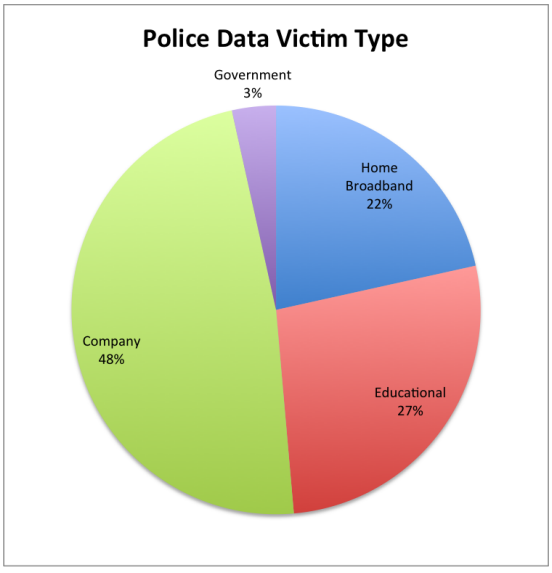

Figure 1: *Victim distribution as noted in the police data*

Zooming in on the relatively large company group, accounting for 67 reports in absolute terms, shows that the IT services and Media & Entertainment categories account for half of the attacks. It is important to note that the Media & Entertainment category, with its 25% also includes gaming related companies, which are so often connected to the DDoS phenomena. Additionally, it's notable that both the financial industry as well as the telecom businesses (which include ISPs) are victim to the same amount of attacks. Furthermore, the public sector e.g. health care and infrastructural services are the target of 13% of the reports, hence more than both telecom and the financial industry. Lastly, the other category accounts for 13% of cases. The "other" category contains a diverse set of business, everything from travel agencies to private contractors, thus showing that all kinds of organisations may become the victim of a DDoS attack.

The educational victims exhibits a clear picture of 90% of the cases being related to high schools while higher professional education accounts for a further 8% and universities for the remaining 2%. It's interesting to note that high schools actually account for 26% of all cases and are thus the single most targeted organisation type according to police reports. The home broadband victims are for 68% gaming related victims, while another 13% targets teenagers for none gaming related reasons. A further 19% are of the miscellaneous category, and cannot be categorised further. Lastly, the governmental group accounting for 3% of all attacks or 5 reports in absolute terms, consists of various ministries as well as one report by the police themselves.

While most DDoS related cases go unsolved simply due to their complex nature as well as the usage of spoofing and booter services, the educational sector proves that the opposite is possible. In all education related cases identified above, two-thirds supplied a suspect in the original police report, while cases where high schools were targeted this percentage goes up to 74%.

To get a better understanding of the attackers executing these attacks, 21 interrogations

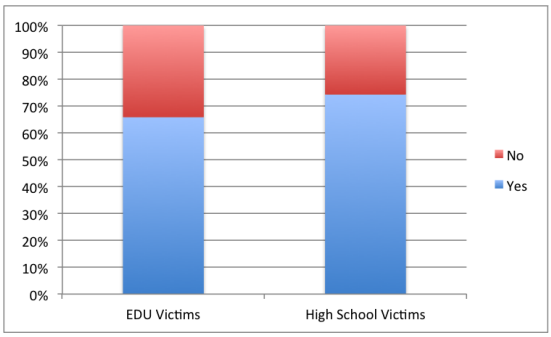

Figure 2: *Suspect supplied in original report*

were analysed. It was the goal of this analysis to get a better insight into the knowledge level of the attackers, both on a technical as well as legal level. Since the interrogations were already held, it wasn't possible to add specific questions however, due to the standard procedure, which includes standard set of questions, used for the interrogations the most important questions could be answered.

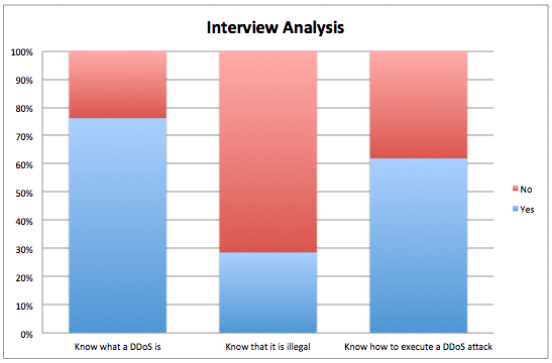

Figure 3: *Analysis of Interview with attackers*

It's important to note that the interrogations were all with attackers between the age of 14 and 16 and as such may not be valid for older attackers. Figure 3 below displays the results of the analysis. As visible not all attackers actually realise what the attack they executed is called nor how to execute one. The reason for this is that many of the attackers found links to booters online or were encouraged by chatrooms to try-out a booter service, without actually understanding what it meant. Furthermore, only roughly 30% of the attackers know that their actions are illegal by law.

IV. Findings II

Using the AmpPot data-set as a point of reference, representing the Dutch DDoS environment as a whole and as such what actually happens, allows the researcher to execute a comparative study. This comparison sheds light on how the sample of the DDoS population the police gets to view, compares to the actual environment. These insights may in turn help the police to reach those victims that have previously been avoided reporting the attacks. As indicated in table 2, the data-set shows 53,055 attacks on 22,580 unique IPs over the period 2014-2015.

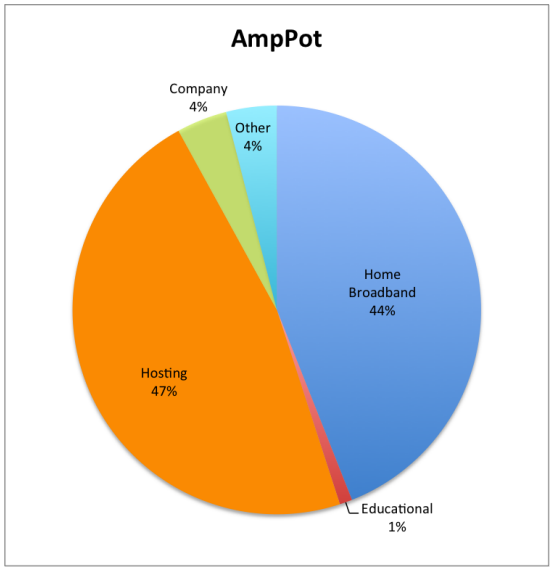

Figure 4: *Victim distribution as noted in the AmpPot data*

Figure 4 is a representation of the victim demographics as found in the AmpPot data-set. Since the AmpPot data-set does not contain specific victim descriptions, a proxy needs to be used. The proxy used to categorise the attacks are the Autonomous Systems the IP addresses belong to. Autonomous Systems (AS) are "a set of routers under a single technical administration" [22] or domain that works under a single routing policy. The AS classification

was in large done by various actors at the TU Delft in order to create papers such as that of Arman Noroozian. Since the classifications between the police data-set and the AmpPot data don't match perfectly, a number of changes have been made. The AmpPot data makes use of the following categories: Hosting, Edu, ISP-broadband, ISP-mobile, ISP-other and Non-intermediary. EDU and ISP broadband are the same as defined by the police data, Hosting is part of the company category in the previous definition and non-intermediary proofs upon manual inspection to be all companies as well. ISP-mobile describes ASes containing mobile internet users and ISP-other are ASes belonging to major ISPs but that could not be categorised further. To make the comparison to the police data easier, the non-intermediary category is renamed to company and isp-mobile and isp-other are joined under the a additional other category. Since hosting is such a strong category it retains its own category.

Table 2: *Summary of cases gathered from the AmpPot data-set*

Type of cases	Number of cases
Number of attacks	53055
Unique IPs attacked	22580

As visible the two figures differ significantly, most notably the educational category only accounts for 1% of all DDoS attacks according to the AmpPot data while it accounts for 27% of all police reports. Equally large is the difference between the amount of targeted broadband connections, the AmpPot data-set argues that these account for 44% of all attacks while they only account for 22% of the police reports. The discrepancy between the two data-sets in regard to attacks on companies is rather small however, in the AmpPot data-set these are represented by not only the company category but also the Hosting category, hence accounting for 51% of all attacks while they account for 47% the police reports. Note, that hosting companies are the largest sub-set of these companies, accounting for 47% of the attacks according to the AmpPot data-set yet only 6% of all police reports. There may be a multitude of reasons for the differences in the willingness to report a attack as described by a number of authors [23] [24] [25] [26]. As an example, one may look at the perceived probability of catching the attacker. For schools for example, the perceived probability is fairly high since in many cases they already have a suspect. This is due to the methodology used by most of the school attackers. As read in the case files, the attackers usually connect to the schools wifi network utilising their personal account and then surf to a booter service at which point they simply let the booter attack their own public IP address. Due to the wifi connection, the public IP address of the attacker is the same as the IP address of the school, hence causing an internet outage. Due to the use of a personal account however, it's fairly easy for network administrators to find out which student browsed to a booter site seconds before an attack.

Combining the two data-sets by tracing IP addresses found in the police reports in the AmpPot data, allows for investigating the police cases in more detail as the AmpPot data enriches the attack vectors often not mentioned in the case files. One of the most interesting attack vectors may in fact be the amplification protocol used. Figure 5 depicts the usage of these protocols and hence indicates the most prominent protocols of these reports. When comparing these to the overall distribution (DNS = 40.33%, NTP = 30.89%, CharGen = 14.32%, SSDP = 14.12%, SNMP = 0,24% and QoTD = 0.07%) one may find an even clearer picture in the police cases. Especially DNS and NTP to some extent seem to be the weapon of choice for most booters. A reason for this may be the inherent nature of protocols such as DNS and NTP, which are basic services of the internet that cannot be changed significantly and as such also consist of a vast number of servers worldwide, while something like QoTD simply doesn't exist all that much anymore.

Furthermore, there is the duration a attack lasts. If no vital infrastructure has been damaged, the duration is the actual length of the denial of service and thus the target will be

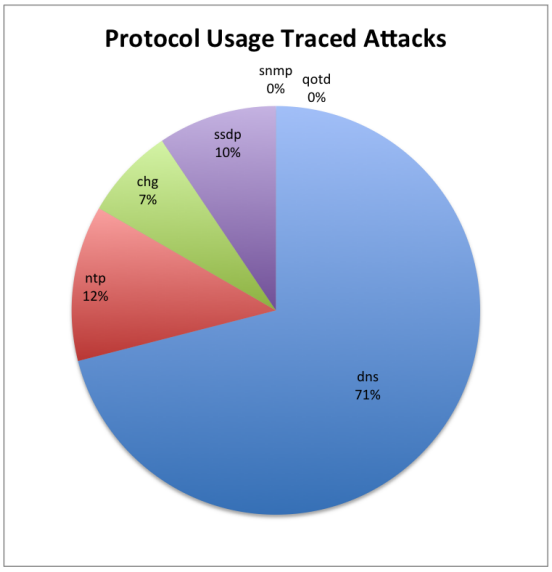

Figure 5: *Amplification Protocol of Traced Attacks*

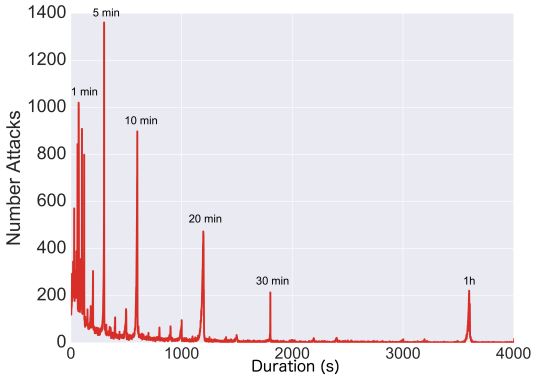

Figure 6: *Attack Duration in the Nethelrnads based on the AmpPot data-set*

reachable again once it has passed. Figure 6 displayed to the right gives an insight in the overall lengths found over all attacks as noted in the AmpPot data-set. The most notable indicator are the peaks at several full minute marks such as 1min, 5min, 10min, 20min, 30min and 1hour. When looking at the continuation of the graph displayed, one can identify the same peaks albeit decreasing in size at full hour intervals. An explanation for these peaks lies in the subscription model used by booters, whom sell subscriptions with these very durations as main differentiator between the packages [10]. Overlaying the traced attacks with the lengths displayed in figure 6 shows that they fall right inline, with the majority of the traced attacks being 5min long with additional peaks at 10min, 20min and 30 min.

One last vector to look at is on the side of the victim. While a DDoS attack in its simplest form targets one IP address, which in turn corresponds to one victim, in reality it is not always that clear cut. In fact, in many cases one IP address accounts for a multitude of victims. One example is the usage of shared hosting, which has become more and more popular throughout recent years. The idea behind shared hosting is that if a customer only has a small website to host, and as such does not need an entire server, they may share one with multiple other customers. This solution is both more efficient and cheaper for all participants. The downside of solutions such as this, is that if one of the customers is attacked, all of them will be victim since they share the same IP address. The AmpPot data allows the researcher to get an idea of the domain count underlying the IP addresses victim to an attack. On the level of the whole population, 22% of all attacks have more than 1 domain, meaning more than one victim to an attack. Looking at the traced attacks this is almost exactly the same with 21%. This result is rather significant as it proves that the number of DDoS victims is much higher than a simple count of the uniquely attacked IP addresses. Furthermore, the damages per DDoS attack may be much higher than previously thought since there are many more victims. Conversely, one may argue that solutions such as shared hosting are usually selected for none critical infrastructure.

V. Findings III

The previous two sections focused on the descriptive and categorical classification of DDoS attacks and how the cases brought to the police compare to the overall DDoS problem. This section utilises another piece of information found in the police data-set namely, the dam-

Table 3: *Costs data extracted from the police reports*

Number of cases noting costs	16
Average victim costs	€15,352
Minimum victim costs	€1,740
Maximum victim costs	€70,000
Median cost DDoS service	$4.00

ages incurred by the DDoS victims. Naturally, most of the victims such as home broadband users could not state a monetary value for their damages other than time lost online. Bigger organisations such as schools and companies however, were able to provide a higher level of detail, resulting in a large count of qualitative descriptions such as "30h x 1000 students = 30,000hours that couldn't be spent using the online education environment" as well as a 16 count of cases with precise monetary values.

Table 4: *Internal Victim Cost factors based on police reports*

Internal Costs:
Unavailable sales website
Inactive employees
Labour costs to repair/bring up the system
"Loss of face"

The first point of interest is the type of damages that are actually incurred by the victim. The reports mention a number of factors that either create costs internally or externally. On the internal side displayed in table 4, there is a loss of income incurred by a website or service being offline, hence no new customers can get in contact with the victim organisation. Secondly, employees of a system may not be able to work while the attack is ongoing, hence the cost of the employees is part of the damages. Thirdly, costs created by repairing the system should it be damaged and to bring it back online. Lastly, there is a certain monetary value attached to the "loss of face" of an organisation that was brought down by a DDoS attack. On the external side depicted in table 5, there are cost incurred through the mitigation of a DDoS attack as well as costs incurred by third party investigative institutions or consultancy companies. Generally speaking, while not all 16 cases mention every single one of the listed factors, the external costs make up the majority of the costs with external consultancy companies providing the highest bills.

Table 5: *External Victim Cost factors based on police reports*

External Costs:
DDoS mitigation services
Third Party Consultancy services
Third Party Investigative services

Table 3 indicates the data extracted from the police reports, indicating an average cost of €15,352.21 over the 16 cases. Knowing the average damages imposed on the victim poses an interesting question, how do the costs on the side of an attacker compare to the costs on the victim side? In other words; how much damage can one Euro spent on a booter service do to a victim? To answer this question, one must get a better picture of booter services. As discussed in the introduction to this paper, the DDoS as a service industry has grown immensely in its size and popularity, a quick google search suffices to see just how big and diverse the offerings are. From a pricing point of view, Hutchings and Clayton have done extensive research on 63 sites noting that prices of monthly subscriptions range between $0.19 and $14.99 with a median of $4.00 [10]. In some cases, the service providers even allow prospective buyers to test their service for free [27]. To answer the question stated above, the equation denoted in equation 1 and 2 will be executed. To be able to utilise the data given by Hutchings and Clayton whom state their values in US dollars, a conversion rate of $1 = €0.89 is used.

$$\frac{\text{Ave. damages}}{\text{Med. cost booter service}} \tag{1}$$

$$= \text{Ave. damages p. euro spent on a booter} \tag{2}$$

$$\frac{15,352.21}{3.56} = 4,312.42 \tag{3}$$

Redoing the same calculation for the maximum and minimum values yields €19,662 and €489 of damages per euro spent on a DDoS booter respectively. One attack that could be traced in its entirety that also indicated a monetary value for damages incurred, recorded €3,000 of damages for an NTP based attack with a duration of about 20min and a load of about 4,000 packets (that is per amplifier used in the attack). It's important to note that this attack is four times as long as the median attack duration and as such may create more damage than a median length attack. One may conclude that the costs on the side of the victim are between 3 and 4 orders of magnitude larger than the costs on the side of the attacker, hence portraying the danger of a DDoS attack.

VI. Discussion and Conclusion

Throughout this paper the DDoS phenomenon was analysed from the law-enforcement point of view. Looking at DDoS attacks from the view of the police yields a number of interesting insights of both the police data-set as well as how that compares to the DDoS Phenomenon in the Netherlands as a whole as represented by the AmpPot data-set. The results of this analysis are split into three findings sections. Findings I indicates only a small percentage of all cases files include technical details such as IP addresses and an equally little share of the cases indicate a suspect. Overall it may be concluded that the cases lack depth and detail and as such are hard to investigate and analyse in a statistical manner. Furthermore, the attack types as described by previous research do not match the ones identified in the police cases, indicating that the police data-set is a bad representation of the population as a whole as it's lacking major archetypes. Furthermore, most of the attackers have very little knowledge regarding the execution of DDoS attacks nor the implications and results of said attacks, yet are able to execute them. This adds to the notion of the commoditisation of cyber crime, the idea that a cyber crime and in this case a DDoS attack becomes so easy to execute that almost everybody can execute them.

Throughout Findings II the police data-set is combined with the AmpPot data-set allowing the researcher to compare the two as well as to trace attacks noted in police case files to the AmpPot data-set in order to get a deeper insight in the attack itself. Throughout the analysis is became clear that the victim demographics differ significantly and that while the educational victims are over represented in the police data the broadband users are underrepresented compared to the AmpPot data-set. This substantiates the differences between the two data-sets further. Tracing the attacks also allowed the researcher to get an understanding of the number of domains connected to a victim IP. In 20% of the cases more than one IP was connected and as such the number of victims is even higher than a simple attack count could indicate. Furthermore, since many of the victims of DDoS attacks choose not to go to the police, all the investigators have to go on is the report of one victim which may in fact not be the targeted victim. As such evidence may be lost as the intended victim never reports the attack. Lastly, since the attack durations as well as the protocols used are almost equal across the board, one may identify a standardisation across the various booters not only on the service level but also on a technical level.

The last step of the analysis focuses on the costs made, both on the side of the victim as well as the attacker. The results are clear, attackers using booter services to DDoS their victim have very little costs compared to the victims, whom end up with costs three to four magnitudes higher. Crime as a service is a big topic and booter services fall right into this category, not only do they provide service to everybody interested without requiring any prior knowledge, they also advertise on the clear web and as such are just one google search away. As such this analysis shows that having a crime just a click away commodities it and thus becomes a normal tool for many. To extend the results found throughout this paper, future research should make use of more law enforcement datas-sets as the majority lack detail in

such a way that analysis is almost impossible. Furthermore, it would be of interest to see exactly what the damages incurred by the victims are as to understand what the most important cost factors are in mitigating a DDoS attack.

References

[1] Barry M Leiner, Vinton G Cerf, David D Clark, Robert E Kahn, Leonard Kleinrock, Daniel C Lynch, Jon Postel, Larry G Roberts, and Stephen Wolff. A brief history of the Internet. *ACM SIGCOMM Comput. Commun. Rev.*, 39(5):22–31, 2009.

[2] World-bank. Internet users as percentage of population, 2015.

[3] Peter van Ammelrooy. Hackers gijzelen ook Nederlandse computers voor losgeld, 2016.

[4] Rob Davies. UK businesses battling huge rise in cybercrime, report says, 2016.

[5] Spiegel. Computerangriffe auf Streitkräfte: Bundeswehr zählte 71 Millionen Cyberattacken 2015, 2016.

[6] Even Cooke, Farnam Jahanian, and Danny McPherson. USENIX SRUTI '05 Technical Paper. *USENIX*, SRUTI, 2005.

[7] Jelena Mirkovic and Peter Reiher. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput. Commun. Rev.*, 34(2):39–53, 2004.

[8] Jelena Mirković, Gregory Prier, and Peter Reiher. Attacking DDoS at the source. In *Netw. Protoc. 2002. Proceedings. 10th IEEE Int. Conf.*, pages 312–321. IEEE, 2002.

[9] Labs. Kaspersky. DDOS Intelligence Report Q3 2015. Technical report, Kaspersky, 2015.

[10] Alice Hutchings and Richard Clayton. Exploring the Provision of Online Booter Services. *Deviant Behav.*, 2016.

[11] Kim-Kwang Raymond Choo. The cyber threat landscape: Challenges and future research directions. *Comput. Secur.*, 30(8):719–731, 2011.

[12] Usman Tariq, ManPyo Hong, and Kyungsuk Lhee. A comprehensive categorization of DDoS attack and DDoS defense techniques. In *Adv. Data Min. Appl.*, pages 1025–1036. Springer, 2006.

[13] Abbass Asosheh and Naghmeh Ramezani. A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. *WSEAS Trans. Comput.*, 7(7):281–290, 2008.

[14] Christos Douligeris and Aikaterini Mitrokotsa. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Comput. Networks*, 44(5):643–666, apr 2004.

[15] José Jair Santanna and Anna Sperotto. Characterizing and Mitigating the DDoS-as-a-Service Phenomenon. pages 74–78. Springer Berlin Heidelberg, 2014.

[16] Hadi Asghari. *Botnet Mitigation and the role of ISPs*. PhD thesis, Delft, 2010.

[17] Marianne Junger, Lorena Montoya, Pieter Hartel, and Margo Karemaker. MODUS OPERANDI ONDERZOEK NAAR DOOR INFORMATIE EN COMMUNICATIE TECHNOLOGIE (ICT) GEFACILITEERDE CRIMINALITEIT. Technical report, Twente, 2013.

[18] Joost Visser and Pieter Jan 't Hoen. BVH Software Risk Assessment Rapport t.b.v. vts Politie Nederland. 2008.

[19] Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow. AmpPot: Monitoring and Defending Against Amplification DDoS Attacks. In *Res. Attacks, Intrusions, Defenses*, pages 615–636. Springer, 2015.

[20] Arman Noroozian, Maciej Korczynski, Carlos Hernandez Ganan, Daisuke Makita, Katsunari Yoshioka, and Michel Van Eeten. Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service. 2016.

[21] Jose Nazario. DDoS attack evolution. *Netw. Secur.*, 2008(7):7–10, 2008.

[22] John Hawkinson and Tony Bates. Guidelines for creation, selection, and registration of an Autonomous System (AS). 1996.

[23] S. van der Weijer and W. Bernasco. WODC | 2674 - Aangiftebereidheid. Technical report, NSCR, Amsterdam, 2016.

[24] Jochem Tolsma. Aangiftebereidheid: Welke overwegingen spelen een rol bij de beslissing om wel of niet aangifte te doen? *Proces-verbaal, aangifte en Forens. Onderz. Cah. Politiestud.*, 21:11–32, 2011.

[25] Robert C Davis and Nicole J Henderson. Willingness to report crimes: The role of ethnic group membership and community efficacy. *Crime Delinq.*, 49(4):564–580, 2003.

[26] Kristina Murphy and Julie Barkworth. Victim willingness to report crime to police: Does procedural justice or outcome matter most? *Vict. Offender.*, 9(2):178–204, 2014.

[27] Mohammad Karami, Youngsam Park, and Damon McCoy. Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services. *arXiv Prepr. arXiv1508.03410*, 2015.