Economics of Cyber Security

Łoin, Michał Meijerink, Mart Man, Ka-Wing Tubbing, Rico

October 19, 2017

1 Introduction

More and more organisations seem to pay more attention to the aspect of cyber security. Increasing popularity of cyber attacks among criminals introduced necessary changes in defensive strategies. One type of an attack is the Denial of Service (DoS) attack. The main goal of this attack is disabling a service or infrastructure by using all of the available resources, such as network bandwidth or CPU processing power. Withing this paper we will discuss a special case called Distributed Denial of Service (DDoS). In this instance, the attack performed using numerous computers, controlled by the adversaries. The main characteristics of this attack is its cheap cost, and significant consequences. Because of those advantages, DDoS attacks recently became available as a service. It is possible to order an attack against any service for marginal costs.

Nowadays, most of DDoS attacks are performed using botnets. Botnet is a group of computers infected by malware. This malware is used to control machines of other people, and finally combining them into large batches. this solution is highly beneficial. At first, it is a cheap source of numerous computers. Secondly, it helps adversaries to stay undetected, since any illegal actions are performed by machines that do not belong to them. A recent example is the Mirai attack [2]. Launched in 2016, the Mirai was designed to take control over Linux machines, mainly embedded systems and IoT devices.

In this paper we will discuss metrics that are used to measure a DDoS attack. At first we will explain what is the main security issue connected to it. Secondly, we will show the ideal metrics that could be used by the Internet Service Providers (ISPs). Later, we will explain what are different types of metrics that are used in practice when evaluating the DDoS attacks. Finally, we will analyse a dataset with information about victims, in order to give better understanding of economics behind attacks.

2 Metrics

2.1 Security issue

First, the security issue needs to be identified. The security issue is depended on the victims and the actors. We will identify multiple victims of DDoS attacks. After which this paper will focus on one group in particular.

In essence, the security issue which is posed by DDoS attacks, is the (limited) availability of a service. As this is too abstract to define proper and useful metrics, we will have to specify the exact actors and drill down to their specific security issue. By answering the following questions, as explained in [4]:

- Security for whom?
- Security of which values?
- Security from what?

2.1.1 For whom?

As identified in [7], most DDoS attacks are aimed at broadband internet users. This paper therefore focuses on internet users. Security against DDoS attacks for internet users will have to be executed by their ISP. Therefore, the ISP is an important actor.

2.1.2 Of which values?

Internet users expect their broadband connection to react quickly and with a certain speed. These are the values which are expected by users from their ISPs. However, a DDoS against a user will likely make the user experience limited or no internet connection.

From the users' point of perspective, the ISP is responsible that the internet connection is working slowly, as it is unlikely for a user to know he is on the receiving end of a DDoS attack. Therefore, the ISP will likely incur reputation damage. Besides the target of the attack, other users might also experience a slower connection if the size of the DDoS attack is sufficiently large. As such, the ISP will want to take action in order to keep its network from being flooded with attack traffic. For the ISP this all boils down to a minimising the monetary loss.

2.1.3 From what?

The main threat to the ISPs is thus the loss of connectivity or limited connectivity for their clients due to flooding of the network. The threat of the network being disrupted may result in trust loss by its users and thus the network needs to be protected from DDoS attacks.

3 Valuable metrics for ISPs

In this section metrics that are valuable to ISPs will be discussed; as will be explained why these metrics are valuable. One of the most crucial metrics of information security is return of security investment (ROSI) [6]. ROSI is quite similar to the well known ROI, but the purpose of ROSI is to measure how efficient security investments are. With this metric security decisions makers can predict if certain security measures are worth the investment. The value of ROSI can be determined by solving the formula in Equation 1, as defined in [6].

$$\texttt{ROSI} = \frac{\texttt{benefit of security} - \texttt{cost of security}}{\texttt{cost of security}} \tag{1}$$

The benefit of security is basically a mapping between the security level which can be mapped to prevented (financial) losses. The cost of security is trivially the amount of money put in the security systems. Once ISPs have these values, it is possible to determine how well security measures perform. In order to determine if security measures are performing well against a DDoS attacks, other metrics are a necessity.

Two of the most trivial metrics are size and duration of an attack. Besides these metrics, there are other metrics that are valuable to ISPs. The metrics can be used to recognise, monitor, mitigate and prevent DDoS attacks.

A DDoS attack might cause reputation damage for example, which means financial losses to ISPs. Trivially, losing money is never good for a company thus an ISP will be interested in the financial losses caused by DDoS attack. If the financial losses are too high, the ISP can, for example, try to put protective systems in place to prevent DDoS attacks and minimise the financial damage. In order to measure this financial damage a good metric would be the quality of service (QoS). If the QoS is poor then this can cause reputation damage, loss of customers and thus financial damage.

Besides these metrics, ISPs should have metrics to monitor attacks so they can act when an attack is happening. One way of doing this (besides looking at the number of packets heading towards a victim) is by observing which network protocols are misused to perform DDoS attacks [7]. If ISPs know how often a certain protocol is misused to perform DDoS attacks, it can put protective systems in place to monitor the most misused protocols. Also, by measuring the average packets sent and the average duration of DDoS attacks per protocol, the protective system could filter the packets more effectively by determining per protocol what is malicious traffic and what is not. Besides this, it is interesting to measure the success rate of preventing a DDoS attack which is performed with a certain protocol. Another helpful metric for ISPs is the frequency of DDoS attacks in certain areas. In areas where more DDoS attacks occur than others, several preventive measures can be taken such as placing DDoS defence systems so the network remains usable during an attack [3]. Finally it is valuable to determine to success rate of mitigating DDoS attacks. However, this is hard to measure since it hard to differentiate between attackers stopping an attack (voluntarily) and defending well enough to block an attack.

4 Metrics in practice

As already shown in previous section, there are numerous possible metrics to describe the DDoS attacks. In this part of the paper, we will discuss the metrics that are commonly used in practice, in comparison to the ideal ones. For the analysis we will be using the framework provided in the lectures, shown in Figure 4.

4.1 Control metrics

Control metrics allow us to measure the level of security by investigating what controls and defensive actions an organisation has performed. They are deterministic, which means they clearly show the important values. In addition, it is relatively easy to measure them. However, they do not consider the threat environment. When analysing availability of the services during DDoS attack, an obvious example is the *capacity of the network*. It is easy to measure, how much traffic a given infrastructure can take. It should be noted, that this metric does not fully correlate with the security against the DDoS, since the network would have to process request of viable customers, together with the blocking traffic.

4.2 Vulnerability metrics

With this group of metrics we are able to test our controls in the threat environment, in a controlled way. In other words, metrics in this category are derived during (penetration) tests and simulated attacks. The first control system that may be tested is the firewall. When analysing that system under a simulated attack, we can observe such values as *Percentage of Attack Traffic Dropped (PAtD)* and *Normal Packet Survival Ratio (NPSR)* [5]. PAtD shows how successful the firewall is

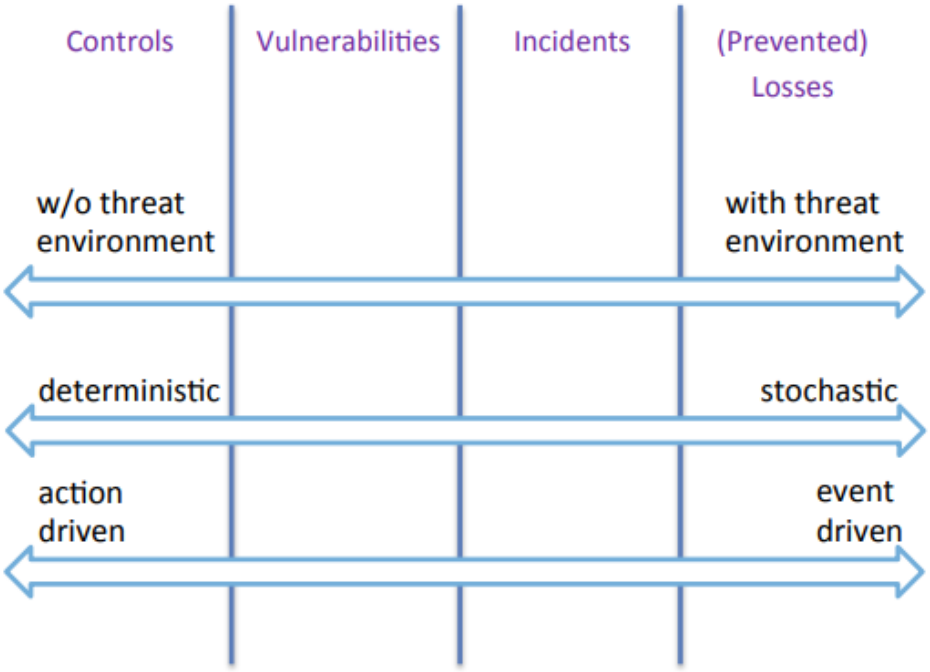


Figure 1: Types of metrics

in mitigating the attack, while the NPSR quantitatively helps to describe what is the effect of the DDoS for regular customers and internal systems. Both of those parameters can be computed in case of a detected attacks. Therefore, detection is another important job of the firewall system. *False negatives ratio* describe how many attacks are missed by it, while *false positives ratio* shows the unwanted disruption of the system for the clients. Another control that can be tested during testing is the *response time to the attack*. Many organisations decide to have a proper incident response team, that consist of specialists that will be the first to react to any abnormal event. Simulated attacks may show if the actions performed are sufficient, and in timely manner.

4.3 Incident metrics

This group of metrics is derived during actual attack, in a real life scenario. In case of the DDoS attack, there are several parameters that can be measured to characterise it. Some of the most commonly used are:

- *Duration* - how much time the attack lasted
- *Size* - how much traffic the attackers were able to produce
- *Origin* - where the attack was initiated
- *Type* - what technique was used to launch the attack, what protocols were exploited.

All of the above factors are directly related to the attack and its specification. They can be used to estimate possibilities of the attackers, or help to classify them. However, the most concerning aspect of an incident are the casualties. *Delay*, *number of lost packets* or *service downtime* are metrics that are commonly used to estimate the impact, what will later help estimate the cost of the attack.

4.4 (Prevented) losses metrics

The last group of metrics shows the benefits of implemented security measures, compared to the (eventual) losses. Ideally, any organisation would like to measure the exact amounts of money that was lost during an attack. Unfortunately, almost always that is impossible, even in case of past events. In case of future incidents, against which the company would like to be protected, to measure the potential loss one would have to predict the behaviour of an adversary, together with used techniques and tools. Despite the difficulty, there are some parameters that help estimating a cost of an attacks. As an example, we are able to measure *the amount of customers affected* by an attack.

5 Metrics defined from data set

The data in our data set has been collected via a set of amplifier honey pots from 2013 till 2015. It consists of

almost four million DDoS attacks, where an attack is defined by "the sequence of packets that includes at least 100 consecutive requests to the honeypots, "consecutive" means that there was no gap of 60 seconds or more between two packets" [7]. Each attack consists of attack date, protocol used to perform the attack, targeted IP address, host name of IP, country, duration (start time and end time) and number of packets. This section will study the collected data so that metrics that are valuable to ISPs can be designed. Next to this, the designed metrics will be evaluated.

The first metric that can be determined is the number of attacks per year, or the popularity of DDoS attacks. However, the number of attacks per year can be influenced by the number of individuals on the Internet. To overcome this issue the number of attacks should be normalised by dividing it by the number of individuals on the Internet. When this metric is used over time it can determine the popularity of DDoS attacks globally. In Figure 6 you can find the relative number of attack per year. Note that not all honey pots were deployed at the beginning of 2013. 2014 and 2015 seem to have almost the same number of attacks

However, most ISPs provide their services not globally but to specific areas. Therefore, for ISPs it is convenient to have metrics which can be applied to these areas. For example, the ISP Ziggo in the Netherlands can measure the global popularity of DDoS attacks, but can also measure it locally so Ziggo can determine if the current security measures are sufficient.

Certain application-layer protocols that rely on UDP are known for its usage to launch DDoS attacks. These protocols are QoTD, CharGen, DNS, NTP, SNMP and SSDP [1]. Some may be used more for than others for amplification attacks [7]. By measuring what protocol is used to perform DDoS attacks, it is possible to predict how large (amount of packets sent to target) and how long (time interval of an attack) an attack might be on average per protocol for example by computing the standard deviation of duration and size. In Figure 2 the number of attacks, per protocol, on the network of Ziggo and KPN are visualised. From this figure it is clear that the DNS protocol is predominantly misused. The SSDP protocol, however, is not used at all on the network of KPN in contrary to Ziggo where about 1500 attacks occurred. This could mean that KPN has better protection in comparison with Ziggo, but could also mean that KPN's network is not misused to perform SSDP DDoS attacks. In Figure 7, you can see that not all duration are the same per protocol. Same hold for Figure 8 that the number of packets are not the same for every protocol.

In Figure 3a boxplots of the duration and number of packets of DDoS attacks in the network of ISPs KPN and Ziggo are visualised. In each figure the network protocol that was used to perform the attack is shown as a boxplot, so a comparison can be made. For example in the case of Ziggo, in Figure 3a it is clear that the DDoS attacks that use the ssdp protocol last longer on average than the other protocols.

Another metric is the percentage of unique victims a country has in the network. This can give a hint on the incentives of the attacker. For example, if this number is relatively large in comparison with other countries it might mean that more personal attacks take place. This can be used together with the number of attacks in a year in the network to conclude if attacks are targeted at the same targets. Some entities attacked once or twice a year with little loses do not have to worry, while others being attacked every week should consider taking counter measures.

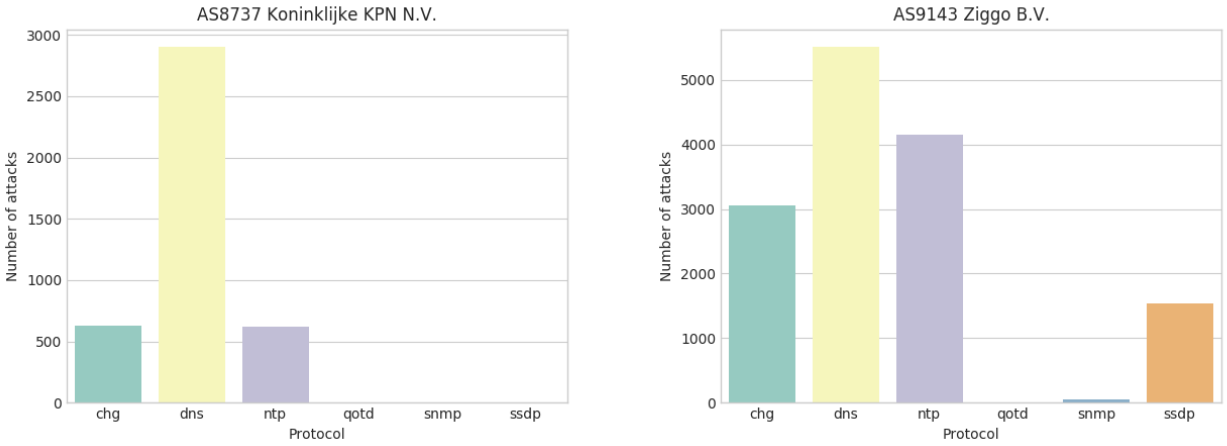
Figure 4 visualises the percentage of unique victims of the top six countries with the most DDoS attacks. This figure shows that the unique victims of China is a bit lower than the other countries. One possible explanation can be that in China DDoS-as-service is not as popular as in the other countries and thus entry barrier to perform/order a DDoS attack is higher.

When this metric is used on network level instead of on country level it can provide other insights to ISPs. In Figure 5 percentage of unique victims of two ISPs and one hosting provider is visualised. On the two providers networks, KPN and Ziggo, more unique victims occur than at LeaseWeb, the hosting provider.

6 Conclusion

In the paper we have shown different metrics that can be used to estimate the costs of the DDoS attack. Due to cheapness and ease of implementation, they became very popular form of cyber criminal activity. Because of that, studying their effects is crucial for numerous organisations. Existing estimates seem to focus mostly on the control metrics, since they are easiest to measure. However, it is almost impossible to discuss the potential impact, without taking into consideration the motivation of the attacker. Not every organisations are equally interesting as a target of DDoS attack, therefore they should not implement identical controls.

In addition to analysing techniques used in practice we have performed a study and analysis on a data set collected from amplifier honey pots. Based on the retrieved information different metrics were analysed. Duration, number of packets and type of abused protocol help describing the characteristics of the attack. Number of unique victims per country or different ISP help to recognise interesting targets for the adversaries. One should keep in mind, that multiple and differential metrics



(a) KPN

(b) Ziggo

Figure 2: Number of DDoS attacks performed per network protocol. In Figure 2a and Figure 2b the number of attacks performed on the autonomous system of KPN and Ziggo are visualised

are a key to proper estimation of cyber security issues.

References

[1] Alert (ta14-017a).

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou. Understanding the mirai botnet. In *Proceedings of the 26th USENIX Security Symposium*, 2017.

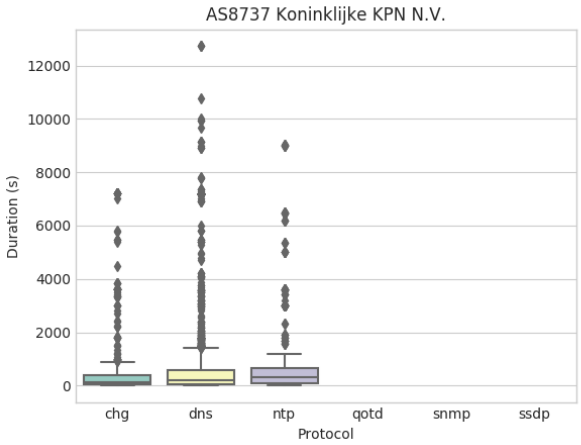
[3] P. E. Ayres, H. Sun, H. J. Chao, and W. C. Lau. Alpi: A ddos defense system for high-speed networks. *IEEE Journal on Selected Areas in Communications*, 24(10):1864–1876, Oct 2006.

[4] D. Baldwin. The Concept of Security. *Review of International Studies*, 23(1):5–26, 1997.

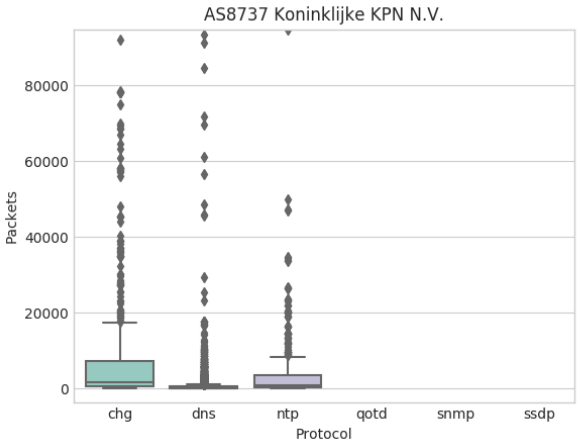
[5] A. Bhandari, A. Sangal, and K. Kumar. Performance metrics for defense framework against distributed denial of service attacks. *International Journal on Network Security*, 5(2):38, 2014.

[6] R. Böhme. *Security Metrics and Security Investment Models*, pages 10–24. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

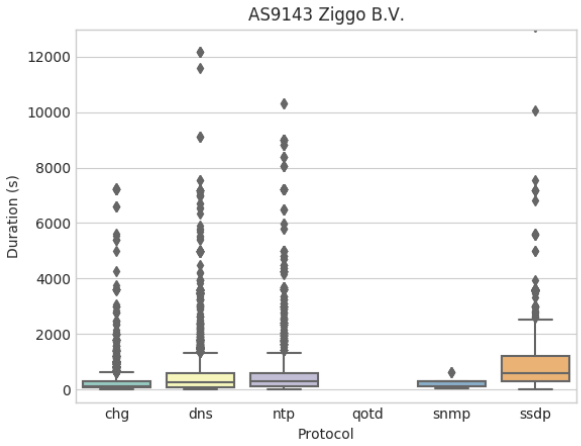
[7] A. Noroozian, M. Korczyński, C. H. Gañan, D. Makita, K. Yoshioka, and M. van Eeten. *Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service*, pages 368–389. Springer International Publishing, 2016.



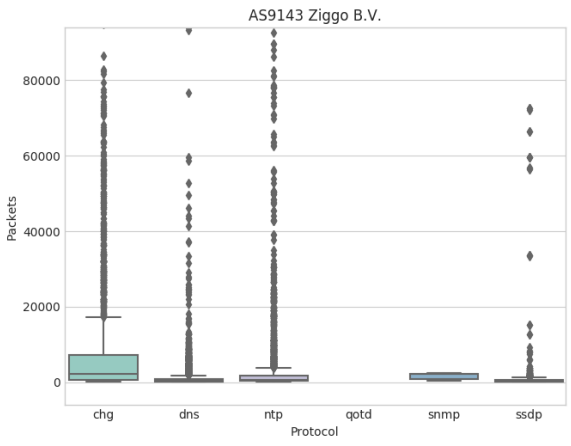
(a) Boxplot of duration on the network of KPN



(b) Boxplot of number of packets of KPN



(c) Boxplot of duration on the network of Ziggo



(d) Boxplot of number of packets of Ziggo

Figure 3: aa

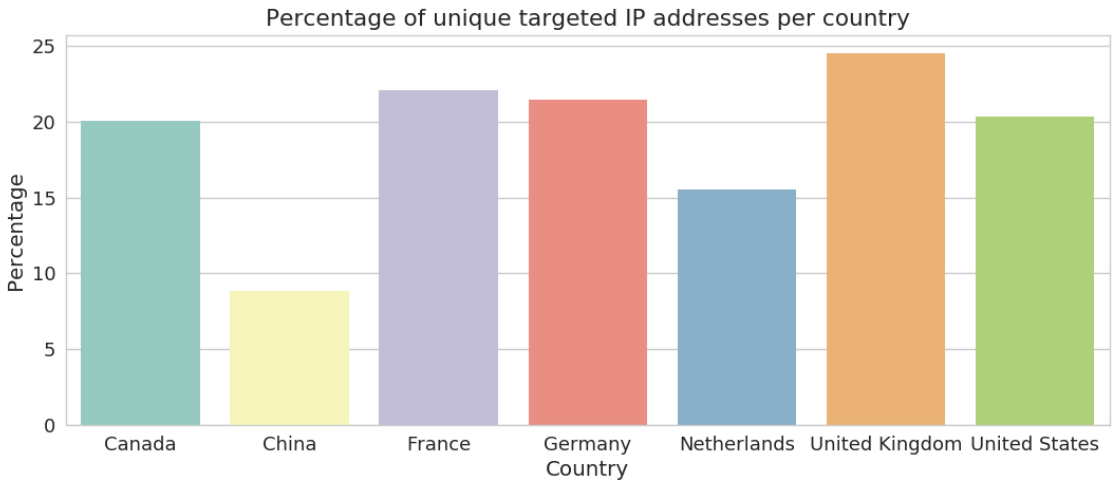


Figure 4: Unique country

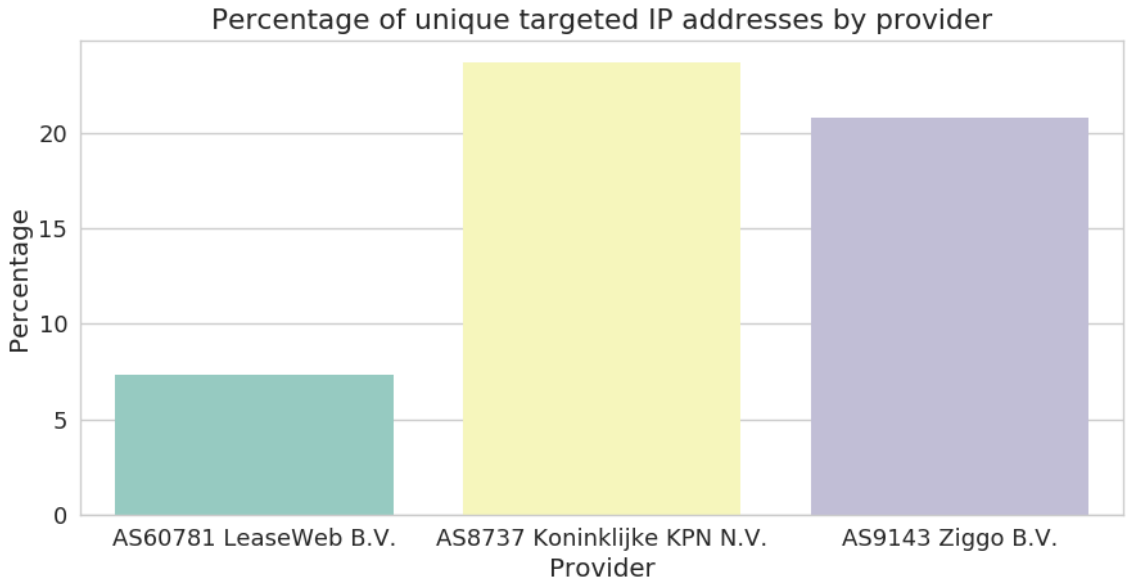


Figure 5: Unique provider

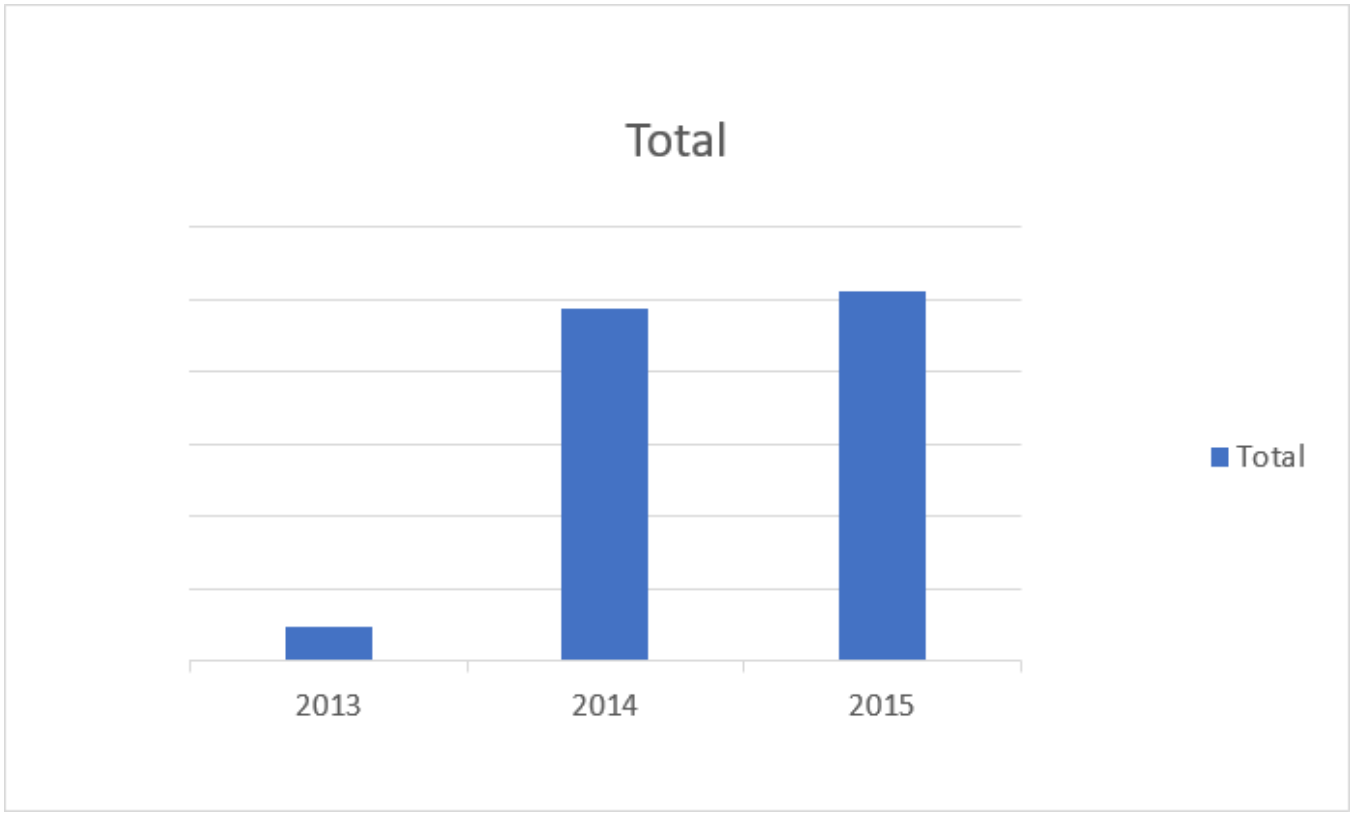


Figure 6: Total attacks per year

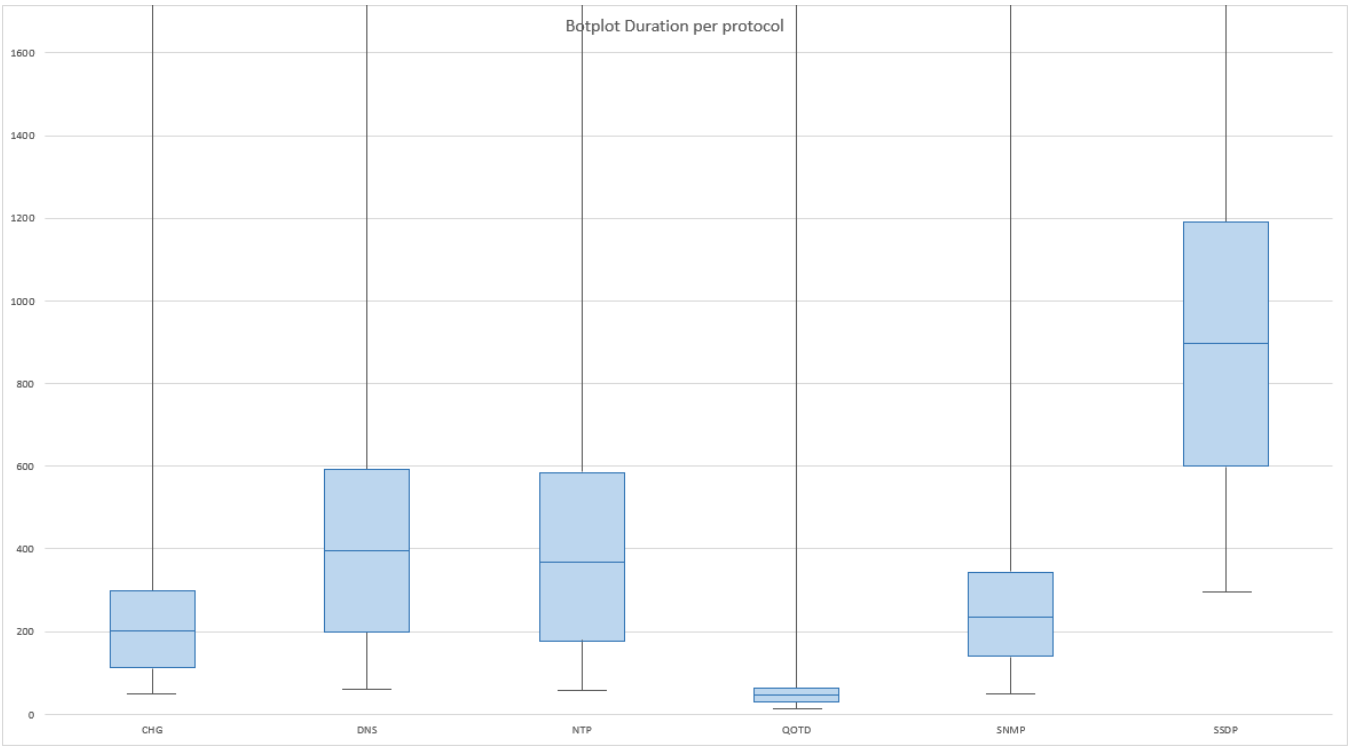


Figure 7: Duration of DDoS attacks in seconds per protocol. Note that the picture is zoomed in on the box and the maximum is outside of the graph.

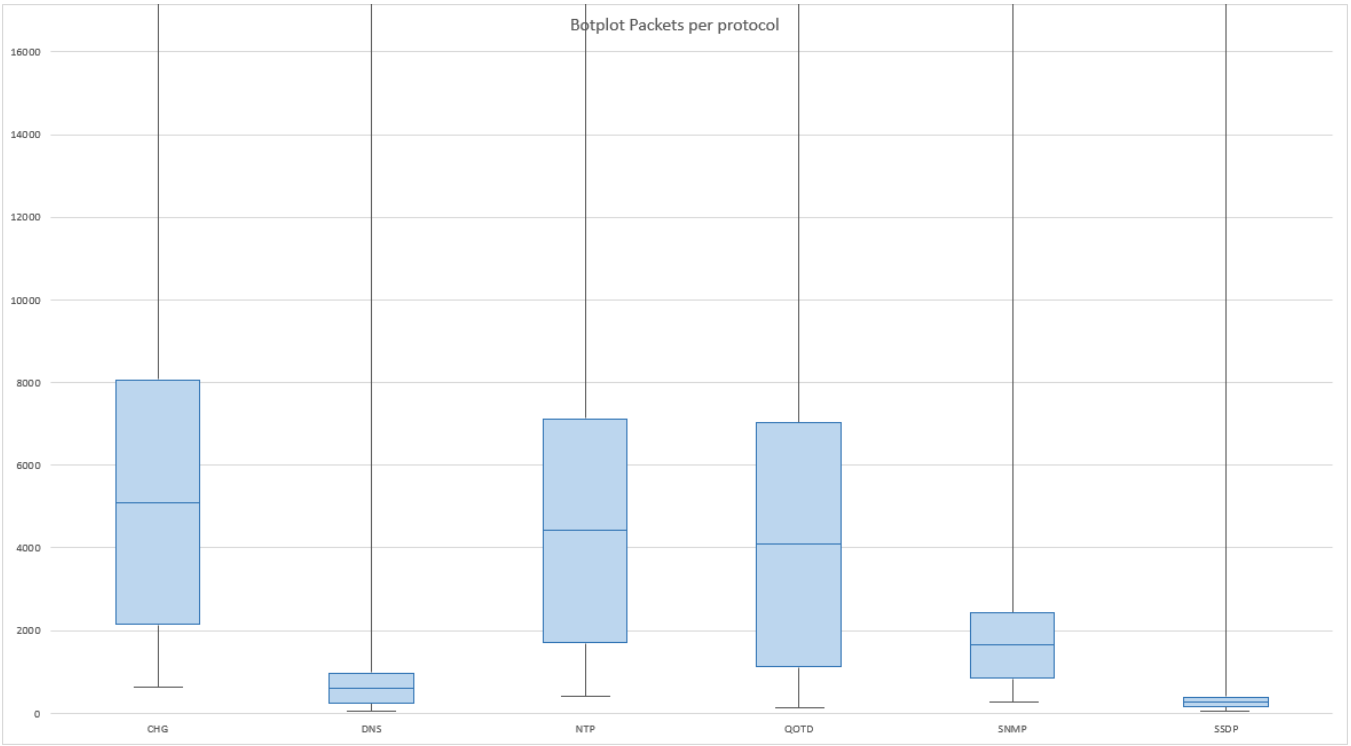


Figure 8: Size of DDoS attacks in number of packets per protocol. Note that the picture is zoomed in on the box and the maximum is outside of the graph.