# DDoS Actors and Security Strategies

Alexandru Babeanu
Samarjeet Patil
Thanasis Pagiavlas

October 22, 2018

## 1 Actors involved in the security issue

Actors involved in the security issue:

- Ziggo - the problem owner; the most targeted company in the Netherlands according to our dataset
- owners of botnet-infected computers - unwilling/unknowing participants in DDoS attacks
- the Dutch government - policy maker

Ziggo could make use of an Intrusion Detection System to differentiate between attackers and actual clients, and filter out the attack packets. The deployment costs of this security measure would consist of the cost of purchasing and installing the software, the maintenance costs and the cost of training staff to work with the software. The benefits of this solution consist of lowering the risk of service downtime, which translates into preventing the reputation and financial losses associated with it. As long as the risk reduction is significant enough to potentially outweigh the cost of a security breach, the company has a sufficient incentive to adopt the security measure. The externalities of this security solution would mostly reflect upon the clients of the organization, since implementing the solution would make the provided service more consistent, while not doing so would run the risk of leaving the clients unable to access the service.

The private computer owners could make use of antivirus software to prevent their computers from becoming infected with malware and turned into botnets. The costs would be rather small for each individual, either a one-time purchase or a monthly subscription - depending on the business model of the antivirus software provider. The benefits would include the protection of the privacy and accessibility of personal data (there other types of malware besides botnets), preventing attackers from using private resources (bandwidth, CPU etc.), and avoiding legal repercussions (willingly engaging in DDoS attacks is

illegal). These personal benefits should constitute a sufficient incentive for individual computer owners to adopt security measures. The targeted organizations would also benefit off of people protecting their personal systems, since fewer botnets result in lower attack magnitudes. The unintentional involvement in DDoS attacks of infected computers is a good example of an externality where the organization under attack is the third party affected negatively by the lack of security measures in private computers.

The government could adopt policies and enforce security standards upon private users, software manufacturers, and organizations that provide services on the Internet, in order to combat the spread of botware. This would enforce a cost on all participating actors, while simultaneously benefiting them along with the government. The government does have an incentive in reducing the security threat of DDoS attacks, since it would like to protect both its systems as well as its citizens and businesses from this type of attack. An externality resulted from this countermeasure would be the reduction in the security risks of organizations that comply with these security standards. Another example of externality would be the legal repercussions suffered by those that choose (or are unable) to not comply with the policies.

# 2 Variation of metrics

Figure 1 shows the number of attacks per country where the attacks are greater than 100000. This can be used to asses the cybersecurity performance of these countries against the common risk i.e. DDoS attack. From the figure it is evident that the countries with highest number of internet users[1] are the ones with high number of attacks but there is a fascinating observation, i.e. Netherlands which is not a part of the top 20 countries with highest number of internet users is prone to such a large number of DDoS attack. The security performance of Netherlands can be assessed using the metric shown in figure 2.

The metric shown in figure 2 is used to measure the security performance of different organizations in the Netherlands. It can be seen that some of the organizations experience more attacks than the others. This variance in the security performance of the organizations is due to certain factors which are investigated in the following sections.

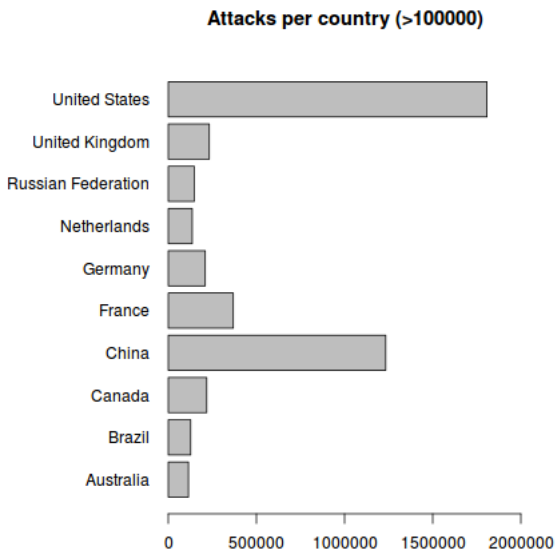


Figure 1: Attacks per country

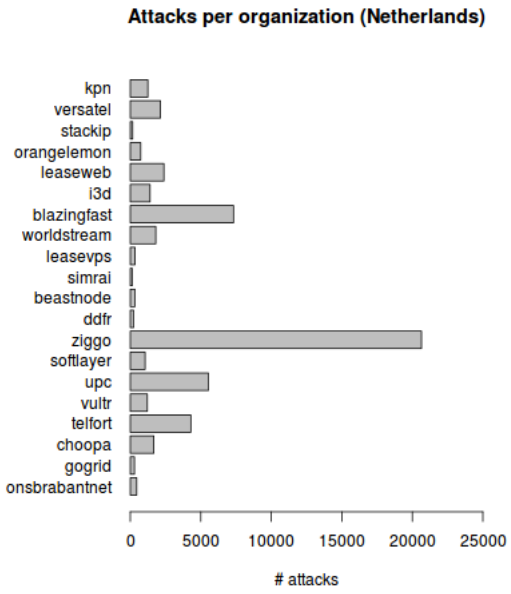


Figure 2: Attacks per organization in Netherlands

## 2.1 Factors explaining the variance in the security metrics

The variance in the security performance among organizations measured by the metric can be caused by several factors. Firstly, the size of an organization and their position in the market. A bigger firm has a bigger customer base which provides a better incentive for attackers. Even a smaller firm can experience more attacks if it has a prominent place in the market. Secondly, the type of service provided by the organization. For the data in hand it can be seen that the most attacked organization in the Netherlands is Ziggo, the largest cable provider in the country. Thirdly, it also depends on the type and properties of Autonomous Systems, i.e. the network in which the organizations reside [2]. In the given data we have AS types like educational, hosting, ISPs - mobile,broadband and others, as shown in figure 4. It is seen that ISP Broadband AS are more prone to such attacks. It also depends on the type of service protocol used, as it is seen that DNS is more targeted compared to the other service protocols. The next factor are the regulators and policy makers. The compliance policies and regulation implemented by the government play a vital role as it can influence most of the underlying drivers of the DDoS attack, such as botnets. Lastly, the attacker's motivation, which are mostly profit driven, also account for the variance.

To summarize, there are multiple factors influencing the metrics and causing variance. These impact of these factors is hard to quantify which in turn causes difficulty in data collection for future references.

## 2.2 Factors and the data to substantiate their role

According to the dataset at hand, the two main factors for the variance in the security metric are the Autonomous System i.e. the network in which the organization resides and the protocols used.

From the dataset which comprises of data of honeypots which have monitored 135945 attacks across unique victim IPs and ASes in the Netherlands. Figure 3, shows the graph for the number of attacks per protocols in Netherlands within the span of 2 years i.e. from 2014-2015. It is evident that a large portion of attack target the DNS protocol ( 49.57%), followed by NTP( 30.55%), CHG( 10.83%), SSDP ( 8.70%), SNMP ( 0.26%) and QOTD ( 0.07%) respectively.

The next major factor is the Autonomous System i.e. the network in which the victim resides. AS is referred as victim network because it is the network which routes the traffic for the victims. The ASes monitored are divided into 3 broad categories namely Broadband ISP's, hosting providers and others, based on the CAIDA's classification of ASes, where the others comprises of ASes which are not classified as broadband ISP's or hosting provider.

Figure 4 shows the number of attacks in the Netherlands for each AS category. From this we can see that majority of the attack victims are in the broadband ISPs. Table 1 shows the number of attacks in the Netherlands grouped by AS category and targeted service. We can show that the risk of a DDoS attack

for broadband ISPs is 3 times higher than the risk for other AS categories, by calculating the odds of such an attack targeting a broadband ISP:

$$Odds = \frac{P(\text{broadband-ISP})}{P(\text{other})} = \frac{24465/total}{(5719 + 2350)/total} = 3.03$$

One of the reasons for these results is the high number of individual users in broadband ISP and the ease of access to booter software. According to some reports, in the Netherlands DDoS is a widespread phenomenon even among the schoolkids as a result of easily accessible booters and just to follow the trend [4].

| AS Category | Service | | | | | |
|---|---|---|---|---|---|---|
| | chg | dns | ntp | qotd | snmp | ssdp |
| ISP-broadband | 6511 | 24465 | 11375 | 0 | 88 | 3719 |
| Hosting | 1679 | 5719 | 5177 | 1 | 133 | 1511 |
| Other | 586 | 2350 | 1454 | 0 | 5 | 372 |

Table 1: Number of attacks by AS category and service type (Netherlands)

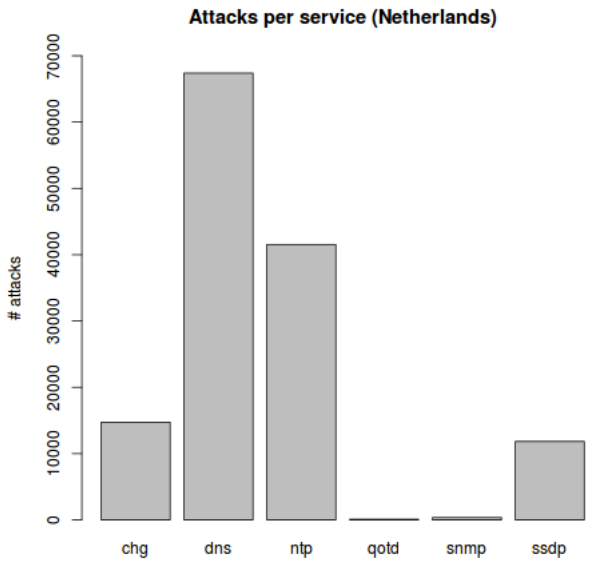


Figure 3: Attack per service

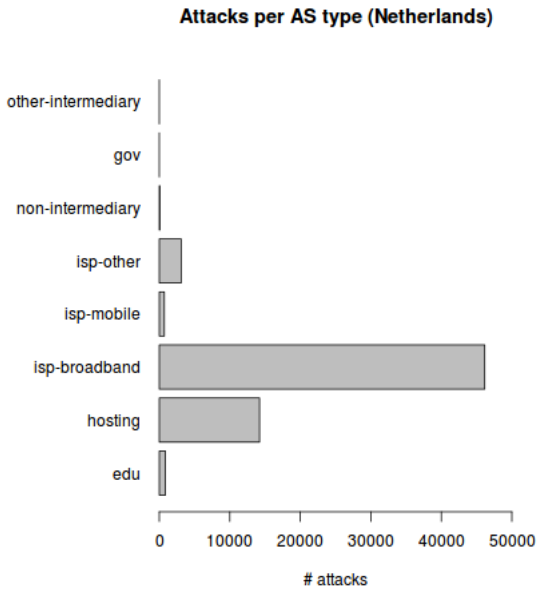


Figure 4: Attack per AS type

# 3 Conclusion

The security performance of the organizations within a country based on the security metric i.e. number of attacks per organization varies depending on various factors. These factors and their impact are hard to quantify and therefore, the records available are prone to subjectivity, which questions the precision of the data collection and its use in the future.

# References

[1] The stats of Internet user around the world. https://www.internetworldstats.com/top20.html

[2] Arman Noroozian1(B), Maciej Korczyński, Carlos Hernandez Gañan, Daisuke Makita, Katsunari Yoshioka, and Michel van Eeten: "Who Gets the Boot? Analyzing Victimization by DDoS-as-a-Service". Springer International Publishing, Switzerland, 2016

[3] J.J. Santanna, A. Sperotto: "Characterizing and mitigating the DDoS-as-a-Service" phenomenon. In: A. Sperotto, G. Doyen, S. Latr'e, M. Charalambides, B. Stiller. (eds.) AIMS 2014. LNCS, vol. 8508, pp. 74–78. Springer, Heidelberg (2014)

[4] State of the Internet / Security Q4. Technical report Akamai (2018). https://www.stateoftheinternet.com/

[5] DDOS report for the first semester of 2018. https://www.nbip.nl/en/2018/08/13/ddos-report-first-semester-2018-download/