DDoS Security Investment and Management

Alexandru Babeanu
Samarjeet Patil
Thanasis Pagiavlas

October 8, 2018

Introduction

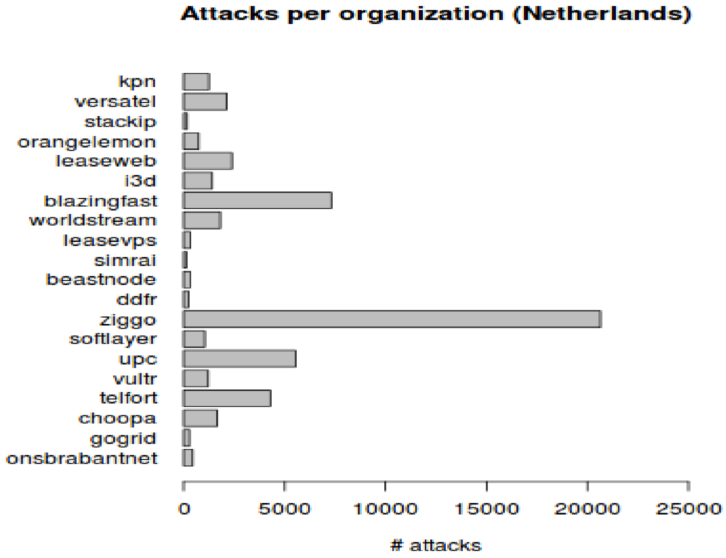
For any organization, after identifying the Risk, the second step is to formulate security strategies and evaluate the strategies. But organizations often fail to identify all the players involved and to formulate strategies considering the role of these actors.

In this document we have identified all the actors involved in the DDoS attack scenario and have outlined some strategies considering their role in the entire picture. But just outlining the strategies is not enough, we have to evaluate the strategies by evaluating their effectiveness and the cost. Accurately measuring these is difficult for any organization, the main reason being that security is not usually an investment that provides positive returns but loss prevention.[3]

In the last section we have calculated an approximate value of the Return Of Security Investment with the help of the dataset provided and some external reports.

Problem Owner

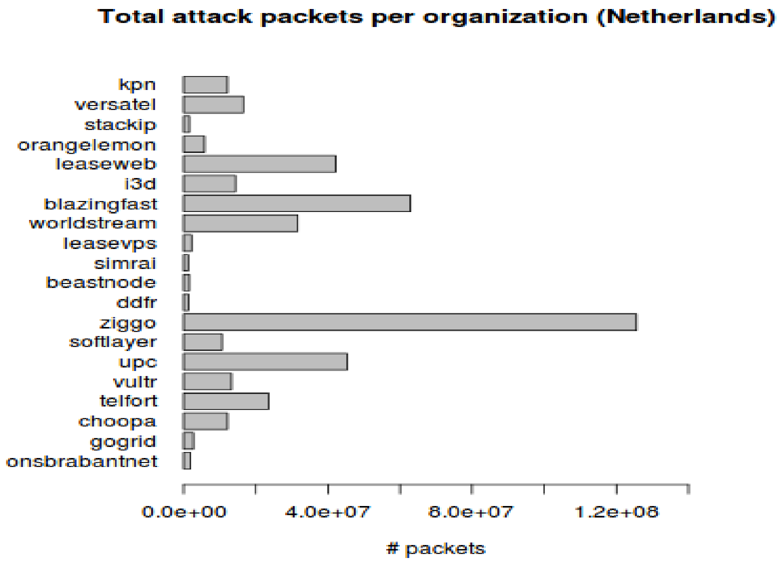
The main problem owners that mentioned in this document are Dutch companies who have detected DDoS attacks against them.



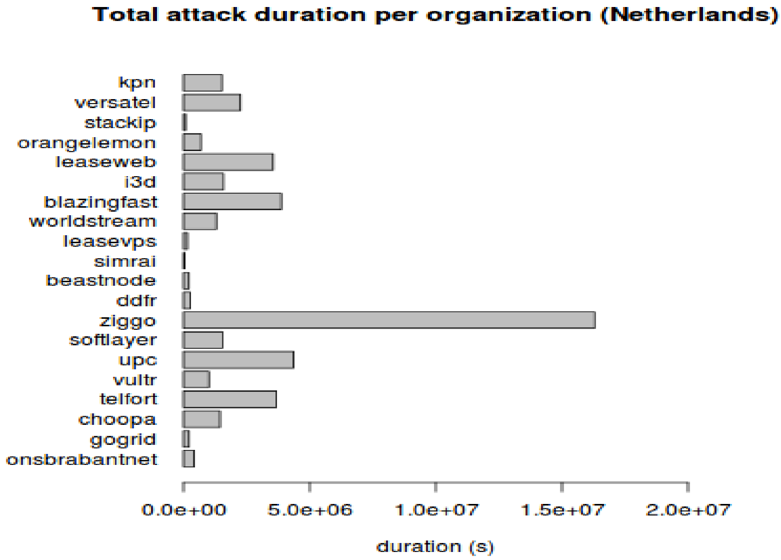
As we can see from the graph, the company that received the most DDoS attacks is Ziggo.It is understandable, because Ziggo is one of the biggest telecommunication companies in the Netherlands.

Comparison Of Security Performance using Security Metrics

In the previous paragraph we note that the most common victim of the Dutch companies is Ziggo, using as metric the number of attacks per organization



Using another metric we can see that the Ziggo organization was also the organization that received the most attack packets. But we also can observe some differences between the results of the two metrics. The Leaseweb organization is the third organization with the most attacks but it has not receive so many attack packages as the other companies.



Another metric is the total duration of the attacks per organization. Using this metric we can note that the organizations which were attacked the most, are not the organizations that the attacks last the most. Maybe they have a better security system than the others and detect and prevent the threat earlier. Maybe the attackers were not so skillful.

In conclusion we can observe that the most common target of all the attacks using each metric is the Ziggo organization.

Risk Strategies for the problem owner

Risk treatment [2] is the most important step in the process of risk management and consists of implementing protection measures which minimize the impacts of security issues. The risks identified and evaluated in previous stages can be divided and managed through four different control strategies:

1. Mitigation
2. Avoidance
3. Transference
4. Acceptance

In the context of DDoS attacks, measures that seek to mitigate risks include the use of firewall software that can block communication from malicious parties, the use of decentralized architectures to prevent service downtime or dynamic allocation of server resources to match the magnitude of the attack. These methods have to be implemented within budget limitations, so their main purpose is to mitigate the effects of attacks with common magnitude. After a certain point, the cost of protecting against a certain level of threat outweighs the likelihood or impact of that threat materializing. These methods have to be implemented within budget limitations, so their main purpose is to mitigate the effects of attacks with common magnitude. After a certain point, the cost of protecting against a certain level of threat outweighs the likelihood or impact of that threat materializing.

Risk avoidance refers to circumventing the risk by not engaging in the activity that generates it. For a server-hosting organization, DDoS attacks are not a risk that can be avoided.

Risk transfer refers to entrusting another organization with the management of a certain risk. A good example of risk transference is the purchase of insurance to ensure financial certainty and combat the variable cost risk of DDoS attacks.

Risk acceptance refers to the option of simply undertaking the risk. If the cost of treating the risk is greater than the impact and the likelihood of the risk occurring, the organization may choose to accept it, unless it is required not to for compliance reasons.

Actors influencing the security issue

Except for the problem owner there are also some other actors that influence this specific security issue:

The employees could be actors, for example if some employees are not so aware of cyber attacks or not so careful, it can be harmful for the company. It is possible for them to download a malware without knowing and turn their computer into a "zombie" that the attacker can use for attacks.

Other businesses that provide services to the company are other important actors, for example the ISP of the company. The internet provider should offer more protection to their clients. It is a win-win situation, if the providers protect the company from DDoS attacks or protect their own infrastructure while offering a comprehensive solution for the company.

Another significant actor is the government, which controls the regulations regarding cyber-law[15].

Risk Strategies the actors can adopt to tackle the problem

After analyzing the portion of the dataset that refers to attacks targeting services in the Netherlands, we came to the conclusion that Ziggo is the most targeted organization and that the DNS and CHG service is the most preferred by attackers. Among the various methods of mitigating the risk presented by these attacks[12], we mention the use of third party protection tools (e.g. Google Shield), the use of firewall software that can block communication from malicious parties, and the use of Intrusion Detection Systems that monitor the network for malicious activity in order to facilitate a threat-response from the targeted organization.

Return Of Security Investment(ROSI)

$$ROSI = \frac{(RiskExposure \cdot RiskMitigated) - SolutionCost}{SolutionCost}$$

$$RiskExposure = SingleLossExposure(SLE) * AnnualRateofOccurance(ARO)$$

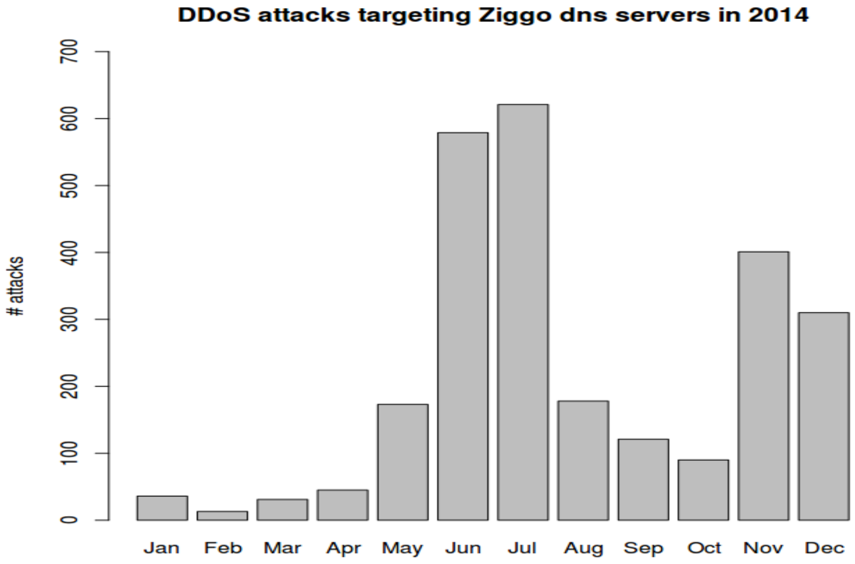
We are calculating the Return Of Security Investment(ROSI) [1] for the strategy of the organization to enhance its network filtering and using a new high-end Intrusion Detection System(IDS). This would be a new enhanced double layer protection for the organization but we have to note that this would not mitigate the attacks completely because these are dynamic in nature and the attackers might find alternate ways to attack.[11]

For now, ROSI is calculated by considering one of the highly target organization in Netherlands according to the dataset in hand , i.e. Ziggo, which is a Telephone service company with close to 22000 attacks within a span of 2 years. So, considering the company and the strategies suggested let's find the ROSI.

As we know Return Of Security Investment(ROSI)[6] is calculated by calculating the Risk Exposure, Percentage of Risk Mitigated and the cost of the solution, lets find these components.

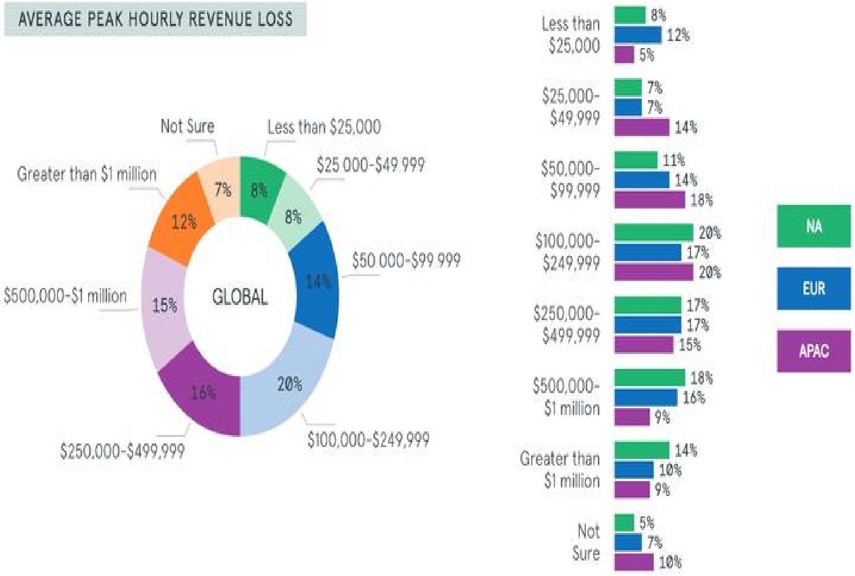
Risk Exposure:

To quantify the Risk Exposure(RE), we have to find the projected cost of the security incident and multiply it with its estimated annaul rate of occurance. Since the total cost of a single DDoS event varies depending on the certain factors such as the duration of attack, timing of the attack etc we will take the approximate projected cost for a DDoS attack with average duration calculated from the dataset.



The Average downtime from the dataset is 8305 secs (i.e. 2.3hrs) in a day, so considering the downtime will cause productivity loss[7] that comprises of the following:

1. loss of productivity by the employees due to system's unavailability.
2. unavailability of service to the customers
3. loss of potential revenue by new customers



This will be somewhere around (EUR 215,000) per hour (according to report by Neustar in 2017)[10] in the peak hours so we might consider an approximate value of EUR 200000.

Considering that the risk exposure per year would be approximately 15 million Euros.

Percentage of Risk Mitigated:

Quantifying the risk mitigated will also be an probabilistic value since the solution and risk can not be isolated. We can state that with the help of the strategy, the organization will manage to mitigate the issue to an approximate value of 80 to 85 percent.

Solution Cost:

Solution cost as we know is not just the Cost Price of the solution but also include the cost of implementation. The cost of an high end IDS is approximately EUR 8500 per server and the cost for enhancing packet filtering firewall will be approximately EUR 18,000. The implementation will also cause certain losses like Application downtime while implementation, workshop to educate the employees about the new technology. Since the attackers are strategic, the attacks are dynamic, hence there will be security patches for any new loophole is encountered.

Considering everything the probable Solution cost can be considered somewhere around EUR 300000 approximately.

Calculating Return of Security Investment(ROSI)

By this we can get a probable value of ROSI,

$$ROSI = \frac{(15000000 \cdot 0.80) - 300000}{300000} = 39\%$$

or

$$ROSI = \frac{(15000000 \cdot 0.85) - 300000}{300000} = 41.5\%$$

So we will have a ROSI   39% - 42%

That suggests that the security investments will probably provide a return of 39-42%

References

[1] Tyler Moore, Scott Dynes, Frederick R. Chang: "Identifying How Firms Manage Cybersecurity Investment". WEIS, 2016.

[2] Abhinav Gajja, Deepam Vipinchandra Shah, Dheeraj Asnani, Edgar Daniel Perez Riveros, Johannes Leo Zutt L'Hotellier, Narendrakumar Chandrakumar, Tejas Kale: "Assessing and Controlling Risks associated with Denial of Service (DoS) attacks on organizational networks". Information Security Consulting, The University of Melbourne, 2014.

[3] Introduction to Return on Security Investment.Helping CERTs assessing the cost of (lack of) security[Deliverable – December 2012],European Network and Information Security Agency.

[4] Payload Based Signature Generation for DDoS Attacks- Kareem M. I. A. Fouda,University of Twente,2017.

[5] Honeypots for Distributed Denial of Service Attacks NathalieWeiler Computer Engineering and Networks Laboratory (TIK), Swiss Federal Institute of Technology ETH Zurich, Switzerland.

[6] Return On Security Investment (ROSI)– A Practical Quantitative Model. Wes Sonnenreich,Jason Albanese and Bruce Stout,SageSecure.

[7] How to Analyze and Reduce the Risk of DDoS Attacks-NETSCOUT

[8] Implementation of Honeypot to Detect and Prevent Distributed Denial of Service Attack. Irwan Sembiring,Faculty of Information Technology,Satya Wacana Christian University.

[9] Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN. Neelam Dayal,Shashank Srivastava,Motilal Nehru National Institute of Technology,Allahabad,India.

[10] Analysing The Impact Of A DDoS Attack Announcement On Victim Stock Prices. Abhishta, Reinoud Joosten, L.J.M.Nieuwenhuis, University of Twente.

[11] A Model for Evaluating IT Security Investments.Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan.

[12] A survey of distributed denial-of-service attack,prevention, and mitigation techniques.Tasnuva Mahjabin, Yang Xiao, Guang Sun and Wangdong Jiang

[13] Impact Analysis of DDosAttacks.Mrs.S.Thilagavathi,Dr.A.Saradha Head, Department of Computer Science, Terf's Academy College of Arts Science Tirupur, Tamilnadu, India Head, Department of Computer Science and Engineering,Institute of Road and Transport Technology Erode, Tamilnadu, India

[14] DoS and DDoS Attacks: Impact, Analysis and Countermeasures Nikhil Tripathi, B.M. Mehtre. Institute for Development and Research in Banking Technology (Established by Reserve Bank of India)Hyderabad, India

[15] Organised Cybercrime in the Netherlands Empirical findings and implications for law enforcement G.Odinot, M.A. Verhoeven, R. L.D. Pool,C .J. de Poot