WM0824 Economics of Cyber Security
Assignment 2

Maria Simidžioski 4381319

Sam van Hooff 4247620

Tom Slooff 4492919

September 2019

1 Introduction

The problem owner of this security issue is an organisation that provides and manages an Autonomous System. This organisation provides Internet connection services to both individuals and other companies. These AS administrators can host websites for companies and also create websites themselves.

An important characteristic of these Autonomous Systems is that they are all connected to each other through public network facilities or access points (Usman 2013).

The functions of these systems include providing information location or searching tools, storage of information and hosting websites, system caching and transmitting digital data from one point to another in the network (Usman 2013).

The organisation that administrates these Autonomous Systems is able to observe the traffic that is flowing into/out of the network and because of this they can detect possible malicious behavior.

(Rowe, Reeves, and Gallaher 2009) argue that these providers could be in a good position to cost-effectively prevent certain types of incidents. In order to detect malicious behavior, The AS administrator could implement additional filtering, create policies that the users must follow and provide security advice. Other technical measures that can be taken are to apply Intrusion Prevention Systems (IPS) and secure their DNS server (Pijpker and Vranken 2016).

2 Actors & risk strategies TODO

There are multiple actors involved in, and influenced by, the security issue of website defacement. Typically those actors have a different function in the system as well as a (slightly) different perspective on the risk involved. In this section the different actors in the field and their definition of the risk of website defacement will be elaborated. Also, the risk management strategies an actor can follow are identified. Those strategies are subdivided in risk reducing, risk accepting, risk avoiding and risk transferring risk-strategies.

2.1 Autonomous System administrator

Risk definition and risk management strategies [risk definition]

Reduce risk

Accept risk
Avoid risk
Transfer risk

2.2 Customers of AS (website owner)

A customer of an AS administrator is defined as an entity paying the AS administrator for a domain on its net space, in other words the a website owner. A website owner is the actor most directly affected by a website defacement of its website(s). A defaced website can impose a website owner with costs ranging from costs for recovery to costs for unavailability of the web service.

A website owner does have the ability to influence the security issue of web defacement, since the vulnerability to this issue greatly depends on configuration of a webserver, as well as the security controls in place.

Risk definition and risk management strategies The risk of website defacement for website owners entails the the possible costs of recovery when a website is compromised and the costs of the unavailability of the service the website owner provides.
Reduce risk
- improve security - make website less atractive to attack for adversaries?

Accept risk
- do noting and accept possible costs of defaced website

Avoid risk
- stop hosting a website

Transfer risk
- insure the risk of website defacement

2.3 Regulatory authority

Regulatory authorities might have a great influence on the security issue of website defacement. By making new laws and enforcing them, regulatory authorities can influence the behaviour of different actors in the field. New laws might for example force AS administrators and website owners to take care of their security measures by imposing fines for negligence regarding their security. Also a legislator might decide to provide for more severe penalties for adversaries breaking the law. Increasing the risk for adversaries might cause some of them to stop.

Risk definition and risk management strategies [risk definition]
Reduce risk
Accept risk
Avoid risk
Transfer risk

2.4 Adversaries

Adversaries are the actors responsible for the defacement of websites. There are different types of actors with different motives. These motives can for example be political, patriotic, economic or terroristic. The goal of those adversaries is to make the targeted domain unavailable and/or broadcast their own message in the form of an alternative web interface.

The capability and motivation of the adversaries have a great effect on the security issue of web defacement, since the issue is the consequence of their actions. This actor will not be taken into account in further risk analysis, since their risk and their motives are opposite to the actors trying to mitigate the security issue of website defacement

Risk definition and risk management strategies [risk definition]
Reduce risk
Accept risk
Avoid risk
Transfer risk

2.5 Conclusion actor/risk analysis TODO

- Are there actors with different strategies? Why?
- have strategies changed significantly over time in a way that reduces or in-

creases risks?

3 The metrics

Two metrics were defined in the previous report. One relating to the reaction time and quickness of AS operators to respond to defaced websites, and one to capture the amount of defaced websites of an AS operator in relation to their size. Thus the first metric aims to measure the capabilities of the AS provider, while the second metric aims to measure the prevalence of the security issue in the networks of the AS provider.

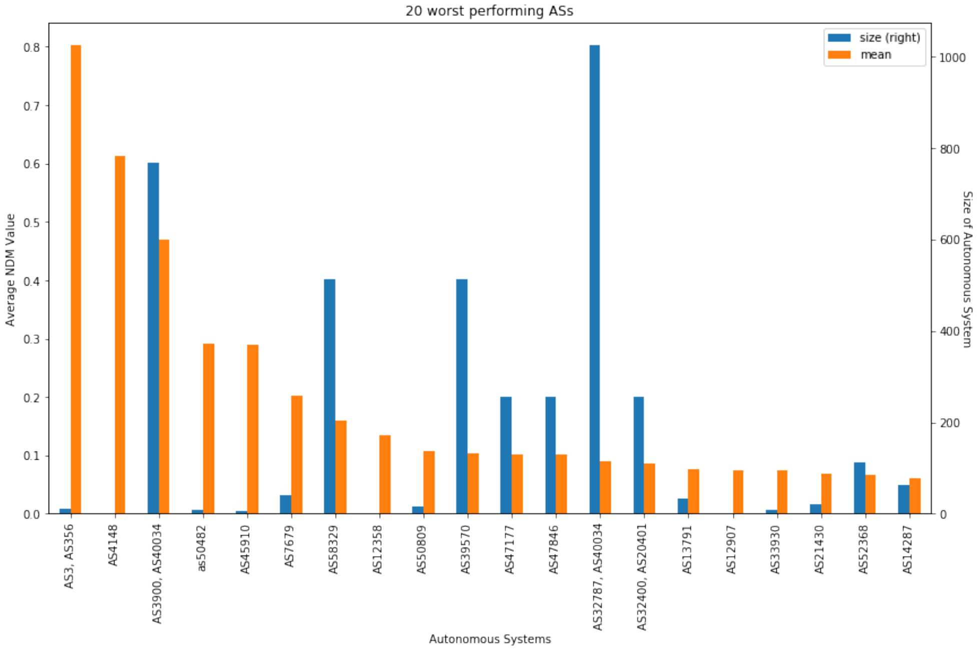


Figure 1: 20 ASs with highest average NDM value

Figure 1 shows the 20 Autonomous Systems (ASs) with the highest average normalized defacement count per month (NDM) value. One strength of the NDM is that it accounts for size, which means that large ASs don't have the disadvantage of a large count just because of their size. However, by normalizing the count this puts the smaller ASs at a disadvantage. This is because one attack in a small AS has a much larger impact on their NDM value. This can be seen when looking at figure 1, as all of the ASs with a high average NDM value have a small size compared to the mode of 4096. The mode is used here because of the few very large outliers on the right side.

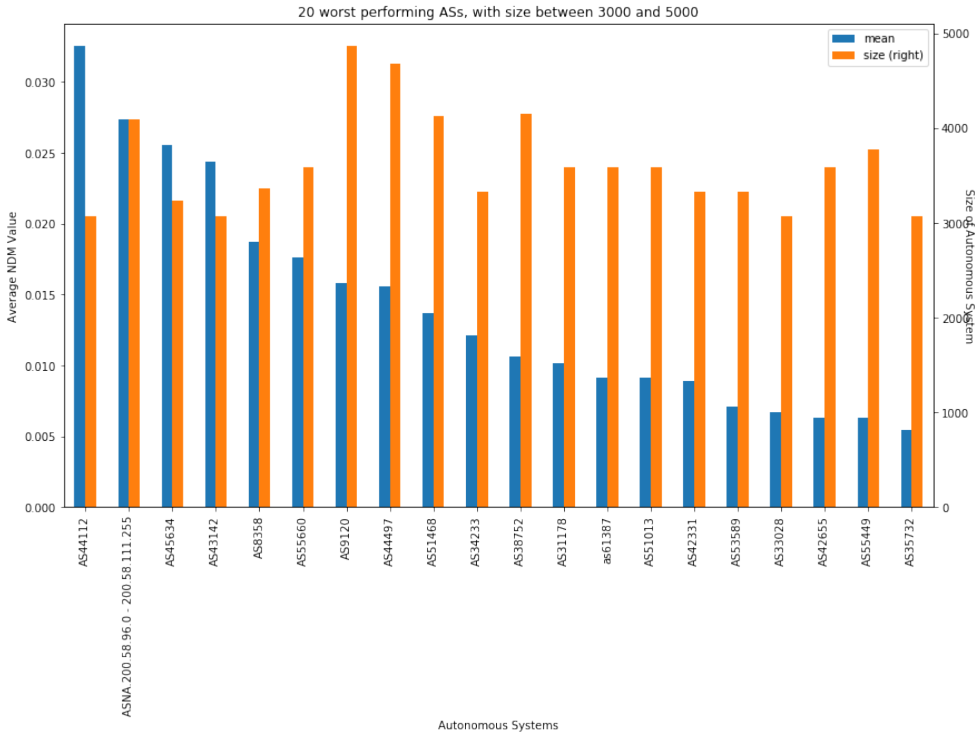


Figure 2: 20 ASs with highest average NDM value, with size between 1000 and 8000

To find ASs to compare using the metrics, it is therefore beneficial to account for the size component when comparing their average NDM value. Furthermore taking a larger AS usually has the benefit of more incident data. Figure 2 shows the highest average NDM values for ASs with size between 3000 and 5000. 2 Ass with similar size, but different average NDM value are picked and evaluated further using the created metrics. AS44112 and AS35732 are the ASs with the highest and 20th highest average NDM in this size range, respectively. Furthermore they both have a size of roughly 3000. These ASs will be compared further.

Figure 3 shows how the NDM values changed for AS44112 and AS35732 over time. The figure shows there are trends in the number of attacks occuring for each AS, although AS44112 consistently has higher NDM values. For both ASs the number of attacks dropped after a small peak in the end of 2014. Especially before 2014, AS44112 has some months with a lot more attacks relative to AS35732.

The normalized defacement count per month (NDM) indicates the security level

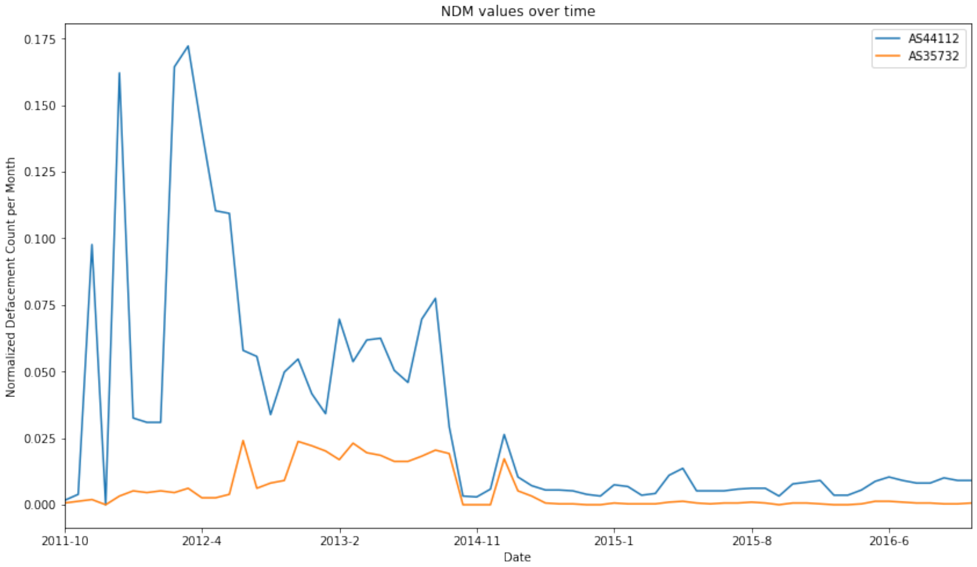
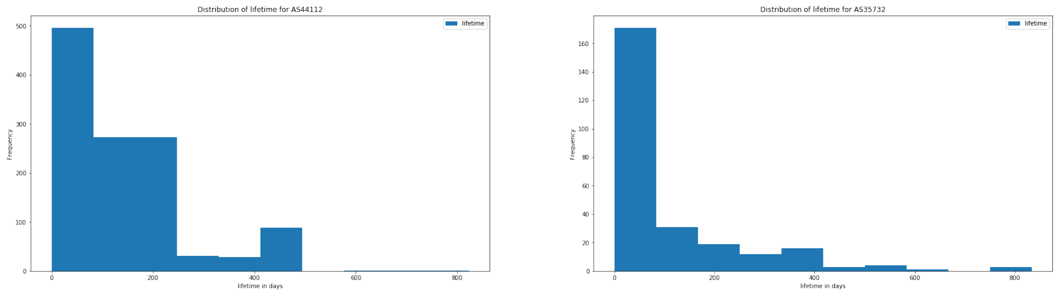


Figure 3: NDM Values over time for AS44112 and AS35732

of the network of an AS provider. If the NDM has a low value, this means that there are few defacements occuring per month relative to the size of the network. This can be due to several reasons, of which the implemented security for the AS provider is one. However, it could also be due to factors such as attacker behavior or the content of the websites it is hosting. In order to compare the relationship further, the distribution of response times can be used.



(a) Histogram of lifetime for AS44112

(b) Histogram of lifetime for AS35732

Figure 4: Lifetime histograms

Figure 4 shows the lifetimes of AS44112 and AS35732 respectively. The first notable thing is that AS44112 has a higher frequency count than AS35732, as can be seen on the y axis. Furthermore the distribution is quite comparable between the two ASs. However, AS44112 handles a larger proportions of defacements after longer than 100 days. Whereas AS35732 handles most defacements in less

than 100 days. It seems that both ASs have a few 'outlier' defacements which took more than 400 days to handle.
Based on these distributions it can be concluded that both suffer from some outlier cases which drag up their average lifetime. However AS44112 has a less clear exponential distribution and lets more cases linger for more than 100 days. Thus based on the given data, the security behavior of AS44112 seems to be a factor in why their NDM values are higher than those of AS35732.

To conclude, the metrics designed in the previous report together form a framework to evaluate the level of security in an AS. Firstly by comparing the normalized amount of attacks per AS, and then evaluating the lifetime metric to estimate the involvement of the AS provider in this level of security. AS44112 was compared to AS35732 to show how the metrics can be used to find the involvement of the AS operator in the level of security, as compared to external factors.

4 Analyzing the risk strategy

In this section the chosen risk strategy will be analyzed and the costs and benefits of the chosen strategy will be discussed. Based on these costs and benefits, the Return on Security Investment (ROSI) will be calculated.

4.1 Costs involved in the strategy

The strategy that is chosen by the Autonomous System administrators/providers is penetration testing.Two types of penetration testing exist, namely, black box penetration testing and white box penetration testing. (Rowe, Reeves, and Gallaher 2009) have examined a medium sized ISP provider that has approximately 3000 employees and provided estimates on the security costs of this organisation. This organisation had 17 employees that worked on IT security and the total cost for this labor was approximately $\$2,325,306$ per year, this means that for each employee $755 is spent per month per year.
The possible costs involved in the chosen strategy are:
The cost of hiring employees for pentesting The costs

4.2 Benefits of applying the strategy

Applying penetration testing has several benefits for Autonomous System administrators. A pentest is able to find weaknesses in a system and can provide evidence or disprove the perceived level of security in the organisation (Wilson 2003). Additionally, the reputation of the organisation can be protected if these pentests are applied adequately and redundant costs can be reduced.

4.3 ROSI calculation

The Return on security investment (ROSI) is:

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

5 Conclusion

References

Pijpker, Jeroen and Harald Vranken (2016). "The role of Internet Service Providers in botnet mitigation". In: *2016 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, pp. 24–31.

Rowe, Brent, Douglas Reeves, and Mike Gallaher (2009). *The role of internet service providers in cyber security*. Institute for Homeland Security Solutions.

Usman, Shuaibu Hassan (2013). "A REVIEW OF RESPONSIBILITIES OF INTERNET SERVICE PROVIDERS TOWARD THEIR CUSTOMERS'NETWORK SECURITY." In: *Journal of Theoretical & Applied Information Technology* 49.1.

Wilson, Marcia J (2003). "CISSP,"Demonstrating ROI for Penetration Testing (Part Four), 7 October 2003". In: *URL: http://www. securityfocus. com/infocus/1736.*