Assignment Block 4 - Spamhaus

Hugo Bijmans [4253760]
Jorrit van der Spek [4174348]
Ben Hup [1150065]
Eveline Pothoven [4380509]
Lisette Altena [1526413]

Group 8

October 31, 2016

1 Introduction

This document is a report for the WM0824TU Economics of Cyber Security course at the Delft University of Technology. The aim of this report is to identify the underlying factors that influence the variance in the metrics defined in previous assignments. We do this by analysing the different actors, their incentives and their externalities. The different actors are analysed in the first three chapters. Afterwards, a different analysis takes place. In chapter five, factors are given which can influence the number of bots blocked in the given time period in a particular country. Some factors are mentioned and the expectations are given. In the last chapter, an analysis is done in order to prove or disprove those expectations. At last, a conclusion is presented.

2 Internet Service Providers

This chapter describes how Internet Service Providers (ISP) are involved in the SPAM issue concerning four distinct topics. First, concrete counter measures that ISPs could use to mitigate SPAM. Second, the distribution of costs and benefits after the counter measure is implemented. Third, what incentives could be to actors to implement the counter measure. Fourth, the role of externalities when counter measures are enacted.

2.1 Concrete countermeasures

This subchapter describes concrete counter measures that ISPs could use to mitigate SPAM.

A very stringent but easily implemented counter measure to block SPAM is to block port 25 for all users of an ISP. Mail Transfer Agents (MTA) use the Simple Mail Transfer Protocol (SMTP) over port 25 to receive e-mail. A MTA is a service running on an e-mail server. There is no feasible way to adapt the MTA by using another port because port 25 is hardcoded into the MTA. As such, the whole world needs to adopt using a new port number, which is almost impossible due to the lock-in effect. Moreover, using port 25 for SMTP is a standard defined by Internet Assigned Numbers Authority (Internet Assigned Numbers Authority (IANA), 2016).

However, it is possible to circumvent a port 25 block by an ISP. A user would need an MTA proxy accepting connections on the official port 25 and a user chosen alternative port (for example port 1025). A user can then send and receive e-mail on port 1025 to the proxy MTA which in turn connects to the recipient server on behalf of the original user. Receiving e-mail from an external party would mean querying the MX DNS records from the PC user inside the ISP network. The MX DNS records will point to the MTA proxy for receiving e-mail. When the MTA proxy receives the e-mail from the external party the e-mail is forwarded over port 1025 to the user inside the ISP network. A schematic representation is shown in Figure 1.

The only means that users are left with is using the webmail client of the ISP that can be protected to the ISP's liking and of course counters sending mass e-mail (e.g. SPAM).

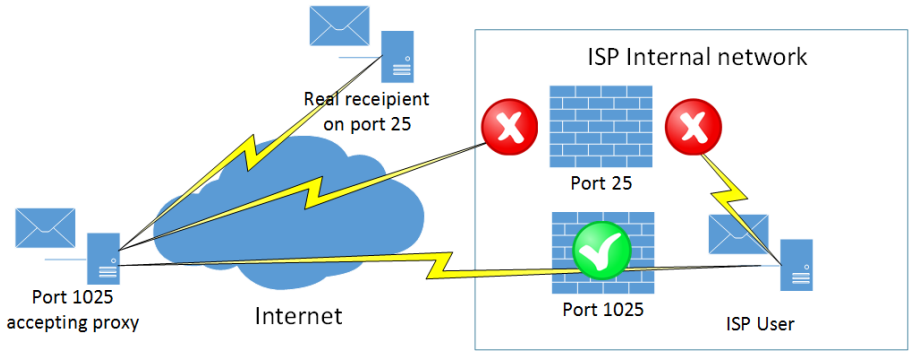

Figure 1: Blocking port 25 for all users of an ISP; but can be circumvented by using proxy

2.2 Distribution of costs and benefits

This subchapter describes the distribution of costs and benefits after the counter measure is implemented. The scenario to block port 25 would require an ISP to configure firewalls. Such action would mean direct costs due to manual labour of personnel of the ISP. In addition, indirect costs to the ISP are (angry) customers leaving the ISP for alternative ISP's that do not block port 25.

Costs to ISP users circumventing the port 25 block need to pay an annual fee to a MTA proxy. However, depending on the contract that the ISP has using other Autonomous Systems (AN), as the Internet is a network of networks, this extra traffic could mean extra costs for an ISP due to extra traffic via the MTA proxy. Nevertheless, e-mail traffic comprises only of a small portion of all data traffic on the Internet.

Benefits to ISP's would be less support questions about malware infections and other SPAM related incidents. In contrast, when a port block would be applied, in the early stage of execution users would call support more why they are not able to use their desktop e-mail clients anymore. However, after this initial period of extra support calls, the number of calls will decline below previous levels.

Benefits to users would be higher productivity, because less time is spent on processing SPAM e-mails (e.g. deleting the e-mails). Moreover, users could also, as an aggregate, gain productivity because malware has to pass the ISP's stringent security measures and thus the likelihood of infection of users will drop.

2.3 Actor incentive

This subchapter describes what incentives could be to actors to implement the counter measure.

Incentives for ISP's to block port 25 should to be economic loss and damage of reputation. For example, scanning e-mail activities requires an ISP to buy hardware, maintain this hardware and accompanied software by experts which has its costs. In addition, for ISP's it is economically quite convenient to block port 25 because damages to reputation and the cost of hardware, up-to-date software and experts add to subscription costs to users, severing competition. Furthermore, the reputation of an ISP is at stake when massive amounts of SPAM are sent from their users in their network. IP addresses might end up in a block list like a DNS-based Blackhole List (DNSBL) or Real-time Blackhole List (RBL). As a result other ISPs and other parties such as companies might be inclined to block an entire subnet (i.e. a whole block of IP addresses) which severs connectivity and thus the reputation of an ISP. Blocking port 25 for ISPs is thus incentivised by bad economic- and bad reputation consequences.

Another incentive could be governmental intervention dictating countering SPAM by blocking port 25. Especially from China and India originates a large amount of SPAM. This is mainly due to a lack of controls at the side of ISPs. When ISPs do not see the benefits of blocking port 25 themselves the government may exercise its jurisdictional power. Incentives to force ISPs to block port 25 could be of all kinds, including financial and administrative punishments.

Creating incentives to ISPs could also be organised by non-profit organisations, NGO's or a group of enthusiast experts. Legal actions could be informing

customers of an ISP that the ISP does not care about customer safety or customer productivity loss. The results might be that creating awareness among customers leads to customers changing ISP and in turn leads to an economical loss to the ISP. Moreover, when the loss of customers is massive enough, this incentive will lead to the ISP taking action to listen to its customers and prevent SPAM. In contrast, actions can be illegal like attacks against ISP servers (e.g. DDoS) to force an ISP to act on countering SPAM. This action might be seen as a last resort when ISPs do not care about a SPAM problem that leads to external severed safety and productivity loss.

2.4 Externalities

This subchapter describes the role of externalities when counter measures are enacted.

Externalities due to blocking port 25 by ISP's could be that SPAM needs to be delivered more intensively through ISP's that do not block port 25. In such case there is only a shift in delivery channels. Blocking port 25 needs to be, to some regional extent, a cooperative effort. At the borders of these regional sections (for example Europe) extra, collective, measures could be taken to counter SPAM which drastically lowers the cost of SPAM due to not needing to defend against SPAM within the region itself but merely at its borders.

Another externality could be that an ISP gains too much power. When customers start migrating, from ISPs that do not counter SPAM, to ISPs that do counter SPAM a change in power balance might occur. One ISP might gain customers due to favourable SPAM policies. However, this ISP might have poor policies concerning other cyber threat issues. Especially in customer behaviour it is difficult to predict what attitude customers have towards a favoured product or service (e.g. an ISP) and the alternatives (e.g. alternative ISPs) (Yang, 2014). The quality of the service of an ISP might depend on other factors than SPAM that weigh heavier for a customer that is unaware of the ISP contribution of SPAM due to its policies. However, when customers do decide to massively move to another ISP new problems like an emerging monopoly or lower Internet speeds due to a higher saturation of bandwidth might emerge in the ISP network.

3 The Department of Economic Affairs of the USA

3.1 Concrete countermeasure

This section will discuss a concrete countermeasure the Department of Economic Affairs of the United States of America can take to mitigate the security risk concerning SPAM. The department can take legal, regulatory and informational measures to mitigate the risk. The countermeasure that is chosen to be elaborated upon is an informational measure. More precisely, to educate individuals and businesses about SPAM. To do this a website is launched on which individuals and businesses can find information about spam and security measures they can implement. The websites main interest is for the users to gain knowledge about cyber security and thus stimulate self-protection.

3.2 Distribution of costs and benefits

The costs for the Department of Economic Affairs consist of the research they have to do, costs of hiring cybersecurity specialists to advise them and, promotional costs. The department itself does not have any direct benefits in terms of prevented losses by deploying the countermeasure. However, that is not the aim of the department. The aim is for individuals and businesses to self-protect and thereby prevent losses. This will make SPAM less beneficial for the attackers and reduce the amount of SPAM sent. In addition, the individuals and businesses do not have any direct costs by using the information and the measures stated on the website. If the website is known to them there is no reason for them not to use it. The individuals and businesses do have indirect costs because the website is government run, which means it is paid for by tax revenues. The exact benefits the cybersecurity information website has is not sure, but observations do suggest that such measures work in favour of enhancing security. At least, they increase market transparency for consumers (Bauer, 2009).

3.3 Actor incentive and externalities

It is the responsibility of the Department of Economic Affairs to support and improve economic activity as much as possible. Engaging in SPAM causes a lot of economic damage. However, the incentives of the individuals and businesses aren't sufficient to stop the negative externalities, which is the absence of self-protection. In most cases, the lack of incentive is caused by misunderstanding the risk of SPAM and the potential loss it can cause. The direct effect of the improved self-protection initiated by the information on the website will reduce the negative externality effect. The reduction of the negative externality effect and therefore some economic losses made by the individuals and businesses incentivize the Department of Economic Affairs to implement the countermeasure.

4 US Companies

4.1 Concrete countermeasures

US companies can lose up to 10 million dollars spending on lost productivity of their employees (Withworth, 2004). The most obvious countermeasure to be used by companies is a decent spam filter. The effectiveness of spam filters although differ a lot, just like the way it works. If email (for example) is filtered, a difference between legitimate mail and spam is made. Employees doing this by themselves costs a lot of time and money (and irritations probably). The classification of spam, separated by a spam filter, can be divided in four parts (Thorkilssen, 2004): true positive, true negative, false positive and false negative:

Table 1: Classification of Spam

	Classified as spam	Classified as no spam
Spam in reality	True Positive	False negative
No spam in reality	False Positive	True Negative

The spam problem is growing strong, meaning filters are having an increasingly hard time to separate legitimate mail from spam. Using SPF, DCC greylists and statistical filters like Naïve Bayesian is becoming more popular. SPF and DCC greylist focus on providing identification on the SMTP layer.

SPF stands for Sender Policy Framework. The hole in SMTP is that any client can assert any sender address, which is exploited by spammers to forge email (Thorkilssen, 2004). The SPF tries to close this hole by forcing the connecting client to identify himself by sending domain, making it unable for spammers to use non-existing domains. It makes it easier to identify spam.

DCC greylists are not like blacklists, rejecting mail absolutely, but requires mail from unfamiliar senders to be retransmitted by their ISPs SMTP clients (Thorkilssen, 2004). Most spam is sent via open proxies or software that do not use normal Mail Transfer Agents (MTA's). When unfamiliar senders are temporarily rejected, the normal MTAs will repeat transmission, but the spam sent through a proxy will not be retransmitted. DCC is a free software implementation of a greylist.

Naïve Bayesian is a statistical filter, used in most popular spam filtering software. It has proven to be very effective: up to 91.7% was correctly classified (Thorkilssen, 2004). The idea behind is that email is represented as a vector with attributes, and every attribute represents a word occurring or not. Then the formula looks at words matching with words in a category c. Then the probability is calculated a mail contains spam or not.

Employees of the company will still need some time to check their spambox on mails that are false negative classified, but it will decrease the amount of time and costs a lot if the company invests in a decent spam filter, combining SPF, DCC greylists and statistical filters. The combination has been proven to be quite effective (Thorkilssen, 2004). Besides that, the probability to be hacked by a virus sent through an email will be reduced.

4.2 Distribution of costs and benefits

Investing in a decent spam filter can cost quite a lot of money. The big question is: what are the clear benefits? According to Withworth (2004), US companies lost 10 million dollars on lost productivity. Besides that, every year employees waste two working days (more than 1200 minutes) dealing with spam (Caliendo et al., 2008).

Filtering rate can be seen as a measure of performance for spam filters. The false positive classified mails are the mails where employees can lose possibly important information. It are 'bugs' in the spam filter (Thorkillsen, 2004). If an employee is forced to go through their spam inbox a few times a day, he might see the true value of a spam filter. It is more annoying than deleting a false negative mail, coming through the filter occasionally. The error cost of a false positive should therefore be assigned a higher value than the false negative (Thorkillssen, 2004).

Besides this, another study argues the spam filter mechanisms increase further expenses on spam. The real cost-saving effects have been unclear so far. Caliendo, Clement, Papies and Scheel-Kopeinig (2008) argues the cost benefits should not be seen at the level of the entire company, but at the level of the employees. As said before: two working days per employee, that is a lot of

money. Costs savings is proven to accumulate to 439 minutes per employee per year (Caliendo et al., 2008).

Caliendo et al. (2008) also argues, to optimize costs and benefits, companies should use different strategies for different employees. They should use spam filters for users with little knowledge about spam, and thereby reducing costs. If a user is well informed or not very affected by spam, companies should not encourage the use of an expensive filter. Manual inspections appear to be more efficient for this group.

4.3 Actor incentive

As mentioned before, companies could reduce 'lost' spending on employees going through spam mails. Because the use of a decent spam filter for ingoing email is pure self-interest (not being hacked, keep your employees from unnecessarily time consuming, annoying work), there is certainly an incentive to use spam filters as a countermeasure.

Besides that, a company does not want to be the victim of spam sent out of their own name: so-called joe-jobs. If spammers know a company is weak regarding spam protection, they might pick that weak company earlier than a company with strong spam policy. Besides that, a joe-job is very bad for the reputation of a company. People will lose their trust and maybe transfer to a competitor. Again, this is an incentive to use spam filters as a countermeasure, solely for their own interest.

The difficult part is that the companies themselves cannot prevent spam attacks from happening: they can only make sure the emails won't come through the mail server. A spam filter doesn't prevent the bad guys from sending spam. There is an incentive to use spam filters as good as possible, but there is a huge lack of incentives for preventing spam from happening. It is more a defence shield than preventing the attack from happening in the first case. To prevent the attack from happening, and actually contributing to a solution for this security issue, collaboration between a lot of actors is necessary. The big problem is all those actors have different incentives, as shown in the other paragraphs.

For example, the ISPs will only care about their customers receiving spam, and not about customers sending spam themselves, because customers are customers and the ISP won't receive any complaints. The US companies do not have an incentive to put time and money in preventing attacks from happening, if the spam received is reduced to a minimum by using a filter.

To conclude there are incentives for US companies to use the countermeasure spam filters. The security issue will be solved for them, but is not tackled. This, because there is a lack of incentives to *prevent* attacks from happening in the first place. The different incentives for different actors makes it even harder to work together to tackle the security issue.

4.4 Externalities

Spam itself is a huge negative externality of advertising. Rao and David (2012) made an estimation that American companies and consumer face almost 20 billion dollar of costs each year due to spam. They also state this figure would be much higher if there were no investments in anti-spam technology by companies. The estimated gains for the spammers fluctuates around 200 million dollars per

year. This makes the externality ratio (external costs / internal benefits) around 100:1 (Rao and David, 2012). The externality ratio for spam appears to be a much higher ratio than for other externalities: think of the classic example of air pollution because of traffic (ratio 1:100).

Many firms already invest in technical solutions to reduce the social cost of spam. However, the problem does not go away with it, but the losses due to spam are reduced. To solve externalities, two popular methods are legal measures and economic measures.

The US government did an effort to make acts that make spam illegal. One of those acts is the CAN-SPAM act: Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. The problem is that this act doesn't seem to affect the illegal advertising market. Much spamming was already illegal, and jurisdictional boundries impede spam prosecutions.

The most used solution to correct a negative externality in economics is introduce a Pigouvian tax (Rao and David, 2012). The proposition is to introduce a postage stamp on email. This will not affect regular users, but sending millions of emails all the time won't be profitable anymore. But companies will also not be happy with this tax: sending newsletters or confirmations of your order at an online website will costs too much.

Although the Pigouvian tax may not solve the externality of spam, the key lays here. Raise the cost of doing business for the spammers by intervening in their margins, which makes spamming less profitable. To do this, a lot of collaboration between actors with different incentives is necessary.

5 Factors explaining variance in the metric

In the first assignment, different metrics were defined to analyse the Spamhaus CBL dataset, which lists blocked IP addresses due to botnet infected spamming. In this section it is investigated which factors could explain the variance in the metric *top 10 countries of blocked IP addresses*. These factors explain why certain countries are more attractive target for botherders and thus pose an additional security risk. First, possible factors and its expected influence are described and then a statistical analysis is performed to explore the actual correlation with the metric.

5.1 Expectations

Four factors, which are expected to have an impact on the number of bots blocked per country, are investigated: gross domestic product (GDP), internet speed, intelligence and internet piracy.

It is expected that countries with a higher GDP will have a higher number of blocked bots. The GDP is the total monetary (market) value of all final goods and services produced in a country during a certain period of time, mostly a year. Changes in a country's GDP are an important indicator of a country's welfare development (Callen, 2012). It is supposed that countries with a high GDP, and are thus economically performing well, will have more bots. These countries will probably have more computer devices and as a consequence have more devices which can be infected.

Secondly, it is expected that countries with a higher internet speed will have a higher number of blocked bots. The computers in these might be more attractive for a botmaster, because it facilitates the performance of tasks.

Thirdly, it is supposed that the average intelligence in a country affects the number of blocked bots. People in the countries with a lower average IQ, might more easily be infected, because they unknowingly install malicious software. People who are less aware of the risks they face, are less likely to download security and are an attractive target for an attacker.

Lastly, a relation is expected between piracy rates and the number of blocked bots. It is assumed that cheap software, offered to control the machine, is more likely to be installed by users of pirated versions of software. Next to that individuals with pirated software may be less likely to download security updates, which makes them an attractive target for an attacker.

5.2 Statistical analysis

The GDP and the number of Bots blocked per country

A data set with the GDP of all countries in 2016 (World Economic Outlook Database, 2016) is used to perform a statistical analysis using SPSS. First of all, the correlations between the numbers of bots blocked per country and the gross domestic product was analyzed. The following results can be obtained:

Table 2: Results correlation tests SPSS

Test	Value	Significance
Pearson correlation	0.446	0.000
Kendall's tau	0.675	0.000
Spearman's rho	0.859	0.000

As can be seen in table 2, some correlations were found. All the tests indicate a correlation, although not every test suggests a strong one, but every test is significant. So it's possible to say that there is indeed a correlation between the number of bots blocked in a country and the GDP of that particular country. This is also made visible when plotting this data in a graph.

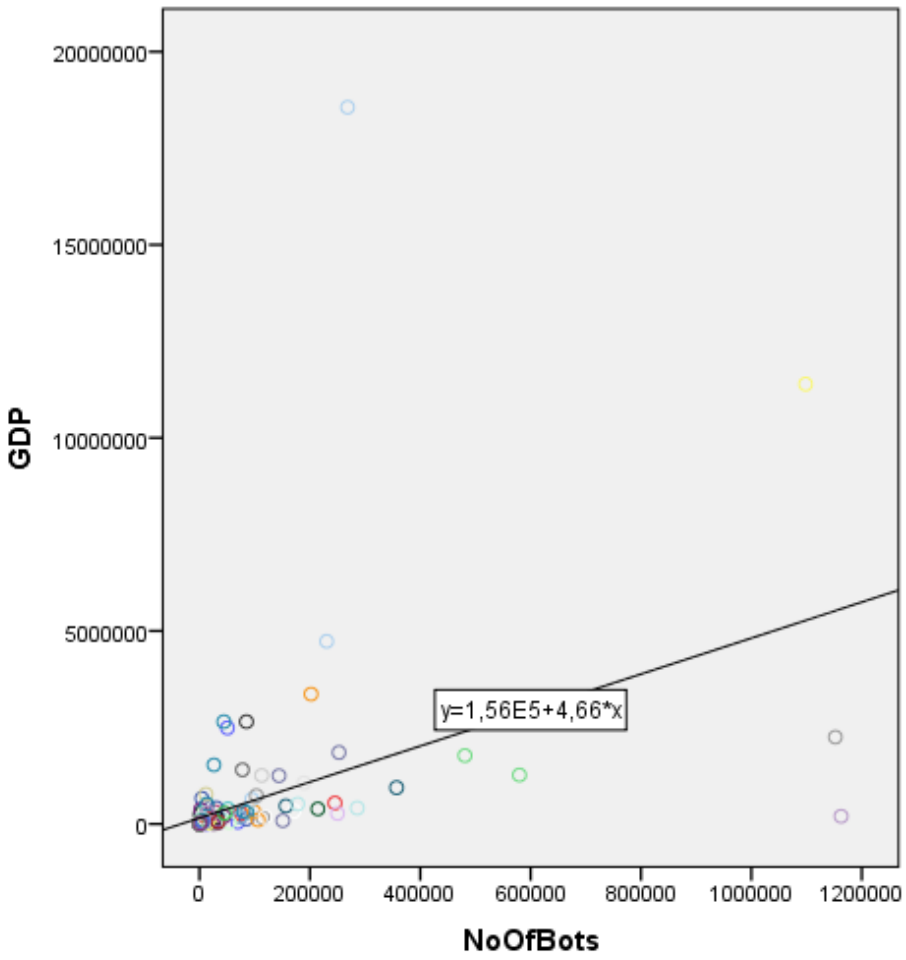

Figure 2: Scatter plot GDP and Number of Bots per country

The average internet speed and the number of Bots blocked per country

The average speed of countries is measured in MBps (Akamai, 2016) and can be correlated with the number of bots blocked per country. It's an interesting to see whether a fast or a slow internet connection will be nice conditions to host a botnet. The following correlations can be found.

Table 3: Results correlation tests SPSS

Test	Value	Significance
Pearson correlation	-0.247	0.034
Kendall's tau	-0.163	0.040
Spearman's rho	-0.236	0.043

The values in the presented table indicate that when the internet speed

increases, the number of bots blocked per country will decrease. In other words, a country with low internet speeds will host relatively more infected computers. It's hard to say whether low speed is indeed a nice condition for botnet or it's just because countries with high internet speed have a better infrastructure. And this infrastructure can have botnet prevention methods implemented. The correlation can be made visible with this scatter plot.

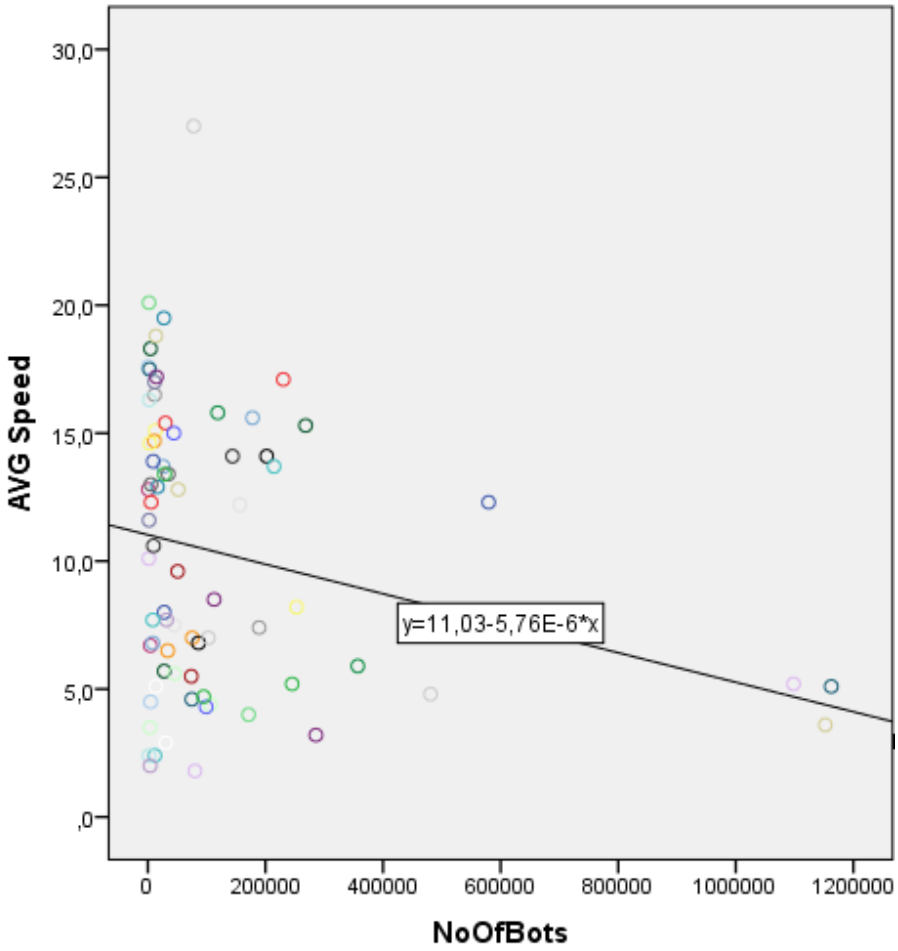

Figure 3: Scatter plot Average Internet Speed and Number of Bots per country

The average IQ and the number of Bots blocked per country

If you're smarter, is your computer less likely to become infected? That's the question answered here. Combining average IQ data from all over the world (IQ Research, 2016) with the blocked IP addresses in our data set, will give some insight. The results can be seen in table 4.

Table 4: Results correlation tests SPSS

Test	Value	Significance
Pearson correlation	0.237	0.002
Kendall's tau	0.355	0.000
Spearman's rho	0.485	0.000

A clear correlation between the average IQ and the number of bots blocked in a country can be seen. All our tests indicate a significant correlation, but not a very strong one. This means that when the average IQ of a country increases, more computers will get infected. The results of this test can be made visible with the following graph.

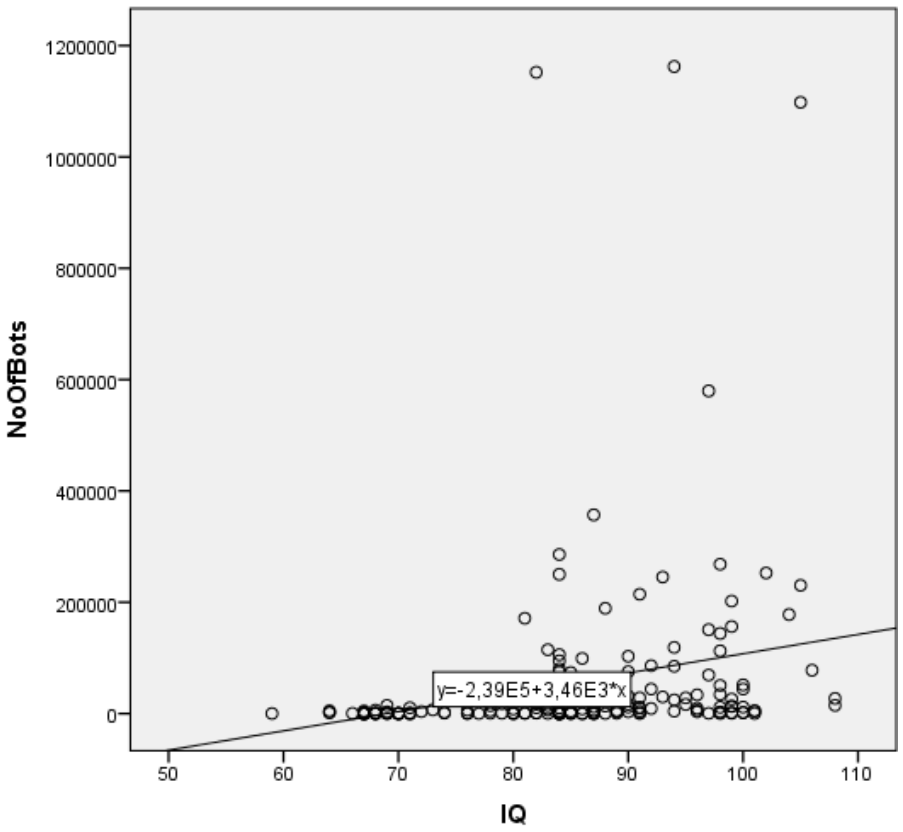

Figure 4: Scatter plot IQ and Number of Bots per country

The piracy rate and the number of Bots blocked per country

Downloading movies, music or applications illegally from the internet can cause trouble for your PC since a lot of downloads contain malware. This malware can be used to setup a botnet. So, if more people in an country call themselves online pirates, will the number in bots be higher or lower? That's what this section is all about. The results of an analysis with data of piracy rate in different countries (TorrentFreak, 2016) can be seen in the following table.

Table 5: Results correlation tests SPSS

Test	Value	Significance
Pearson correlation	-0.398	0.005
Kendall's tau	-0.409	0.000
Spearman's rho	-0.584	0.000

A very interesting correlation can be seen between the piracy rate in a country and the number of bots blocked in a country. The higher the piracy rate is, the lower the number of bots blocked in that particular country. All the tests indicate a significant and quite strong correlation. The results can be made visible with the following graph.

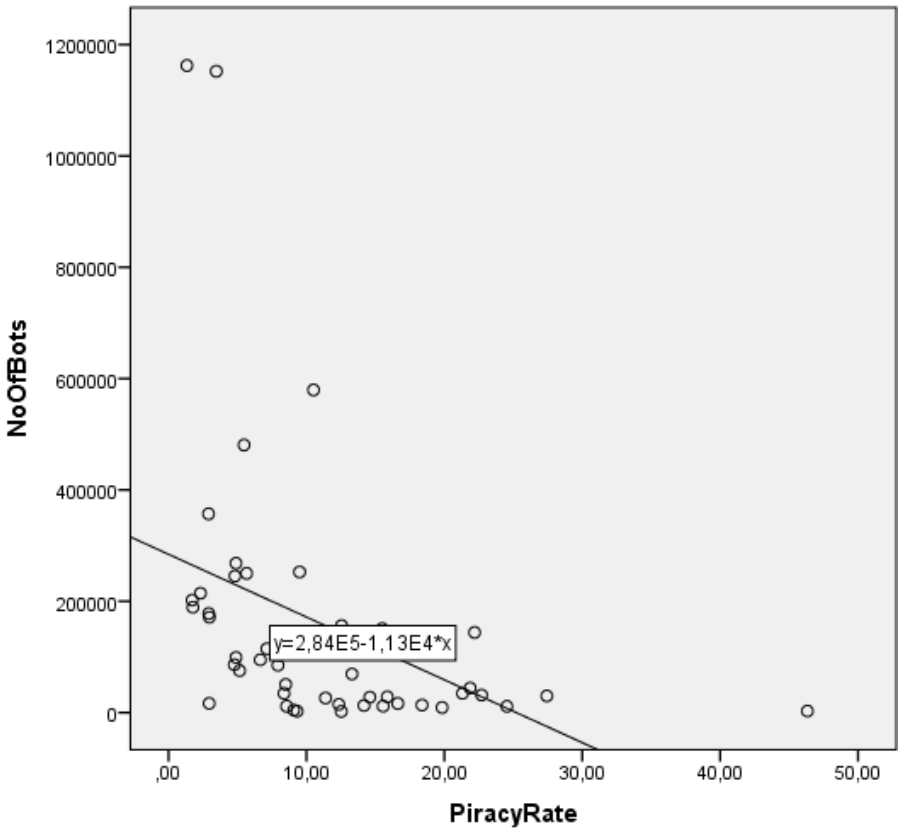

Figure 5: Scatter plot Piracy Rate and Number of Bots per country

Correlation between factors

All the investigated factors seem to be correlating well with the number of bots blocked per country in the given period. Therefore, it's interesting to see whether these factors also correlate with each other, because if one factor correlates with all the others, the analysis is weakened. The correlation of all the factors can be seen In the following table.

Table 6: Results correlation analysis of influencing factors SPSS; **. Correlation is significant at the 0.01 level (2-tailed).

		PiracyRate	GDP	AVG Speed	IQ
PiracyRate	Pearson Correlation	1	-,200	,435	,231
	Sig. (2-tailed)		,173	,004	,118
	N	49	48	42	47
GDP	Pearson Correlation	-,200	1	,091	,274
	Sig. (2-tailed)	,173		,442	,000
	N	48	184	73	170
AVG Speed	Pearson Correlation	,435	,091	1	,739
	Sig. (2-tailed)	,004	,442		,000
	N	42	73	74	72
IQ	Pearson Correlation	,231	,274	,739	1
	Sig. (2-tailed)	,118	,000	,000	
	N	47	170	72	176

The correlation table shows clear correlations between the average speed and the GDP of a country. Not much of a surprise, since investments in infrastructure can only be paid when the GDP is high. An interesting correlation can be found between the IQ and GDP and between IQ and average internet speed. Your internet connection speed is apparently a good indicator for the average intelligence in your country. None of the factors correlate with all the other factors, so we can use them all in our analysis.

Multiple regression model

In the previous sections, all factors were investigated individually. In this way individual correlations can be seen, but not the actual contribution to the number of bots in a country with the other factors taken into account. Therefore, one needs to make a model with all the factors in it. This is done in this section, with use an of linear multiple regression model. In this model, the number of bots blocked in a country is chosen as a dependent variable, and IQ, piracy rate, GDP and average connection speed as independent variables. The results can be seen in the tables below.

The most influencing factors of the number of botnets per country are the average internet speed and the average IQ of a country. Surprisingly, with all the other factors taken into account, the GDP isn't a very influencing factor anymore. This also applies to the piracy rate of a country, which has a non-significant contribution to the amount of bots blocked per country. The model with the four factors included has a decent R value, which means that it's able to calculate half of the values correctly, based on this factors.

Table 7: Multiple regression model

	Unstandardized Coefficients		Standardized Coefficients		
	B	Std. Error	Beta	t	Sig.
(Constant)	-578398,774	160486,030		-3,604	,001
GDP	,023	,010	,266	2,255	,030
AVG Speed	-19825,679	4654,221	-,753	-4,260	,000
IQ	10063,619	2236,782	,765	4,499	,000
PiracyRate	-3297,552	2140,405	-,194	-1,541	,132

Table 8: Correlation coefficient (R value)

R	R Square	Adjusted R Square	Std. Error of the Estimate
,750	,563	,516	101510,896

6 Conclusions

This report aimed to investigate the underlying reasons behind the variance in the metric *top 10 countries of blocked IP addresses*. Therefore, first three actors (Internet Service Providers, the Department of Economic Affairs of the USA and US companies), which are involved in the security issue were analysed. This study clarifies why, despite all possible countermeasures, the security issue still exists. This is mainly caused by the contrasting incentives of the different actors and the externalities resulting from their actions. For example, US companies do not have an incentive to put time and money in preventing attacks from happening. If the spam received, is reduced to a minimum by using a filter. The security issue will be solved for them, but the issue itself is not tackled.

Secondly, four factors, which could explain the variance in the metric top 10 countries of blocked IP addresses were investigated: a country's GDP, average internet speed, intelligence level and piracy rate. An analysis in SPSS was done to investigate the correlation between the individual factors and the number of blocked IP addresses in a country. All the investigated factors correlate well with the number of bots blocked per country in the given period. The most influencing factors of the number of botnets per country are the average internet speed and the average IQ of a country. A country with low internet speeds will host relatively more infected computers and when the average IQ of a country increases, more computers will get infected. It is hard to say whether these conditions are indeed the cause for a higher number of infections. Countries with a high internet speed, have a better infrastructure and have probably botnet prevention methods implemented.

References

[1] Akamai. (2016). *Akamai's [state of the internet] Q2 2016 report.* Retrieved October 21, from https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-connectivity-report-q2-2016.pdf

[2] Bauer, J. M., & Van Eeten, M. J. (2009). *Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy, 33(10), 706-719.* Retrieved October 29, from http://www.sciencedirect.com/science/article/pii/S0308596109000986

[3] Caliendo, M., Clement, M., Papies, D. and Scheel-Kopeinig, S. (2008). *The cost impact of spam filters: Measuring the effect of information system technologies in organizations.*

[4] Callen, T. (2012, March 28). *Gross Domestic Product: An Economy's All.* Retrieved October 23, from http://www.imf.org/external/pubs/ft/fandd/basics/gdp.htm

[5] International Monetary Fund. (2016). *World Economic Outlook Database.* Retrieved October 23, 2016 from http://www.imf.org/external/pubs/ft/weo/2016/02/weodata/index.aspx

[6] Internet Assigned Numbers Authority (IANA). (2016, October 20). *Service Name and Transport Protocol Port Number Registry.* Retrieved October 22, 2016, from iana.org: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[7] IQ Research. (2016). *World ranking of countries by their average.* Retrieved October 21, 2016 from https://iq-research.info/en/page/average-iq-by-country

[8] Rao, J. M. and Reiley, D. H. (2012). *The economics of spam.* The Journal of Economic Perspectives, 26(3), 87-110.

[9] Thorkilssen, H. W. (2004). *SPAM—Different approaches to fighting unsolicited commercial email: A survey of spam and spam countermeasures.* Network and System Administration Research Surveys, 1, 45-55.

[10] TorrentFreak. (2016). *Europe Has The Highest Online Piracy Rates, By Far.* Retrieved October 28, 2016 from https://torrentfreak.com/europe-has-the-highest-online-piracy-rates-by-far-160801/

[11] Whitworth, B. and Whitworth, E. (2004). *Spam and the social-technical gap.*Computer, 37(10), 38-45.

[12] Yang, L. W. (2014). *Distinctively Different: Exposure to Multiple.* Journal of consumer research, Vol. 40, 973-992.