Assignment Block 4
SPAMhaus

DRAFT

Group 8
Jorrit van den Spek, Hugo Bijmans, Eveline Pothoven, Ben Hup, Lisette Altena

WM0824 Economics of Security

Table of Contents

1. Introduction

To be written

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 counter measures

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).

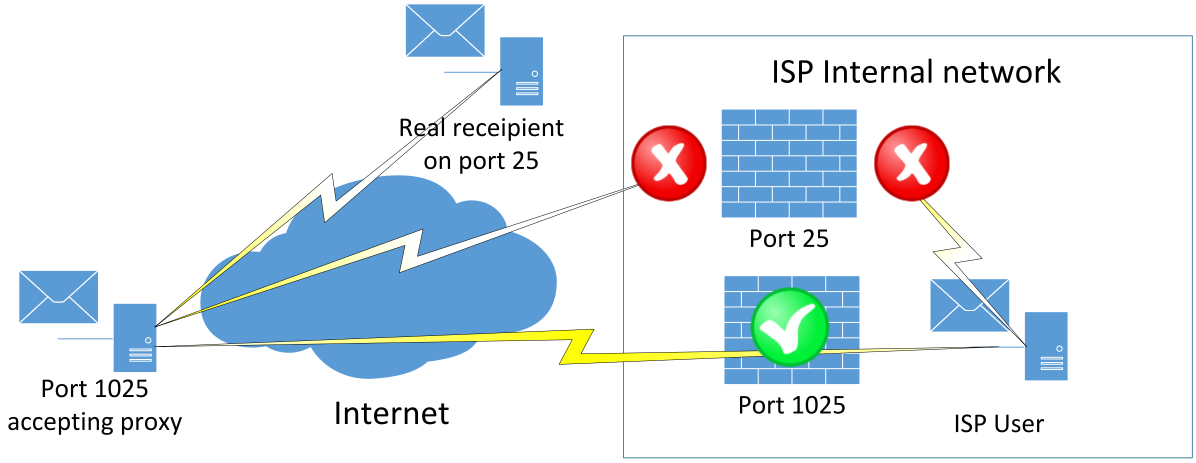


Figure 1 Blocking port 25 for all users of an ISP; but can be circumvented by using proxy

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 to ISP's would need to be economical loss and damage of reputation. Scanning e-mail activities requires an ISP to buy hardware and maintain this hardware and accompanied software by experts which also cost money. 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. Another incentive could be governmental intervention dictating countering SPAM by blocking port 25.

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.

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. To mitigate the risk the Department of Economic Affairs should educate the citizens and private sector about SPAM. A concrete countermeasure to accomplish this is launching a website on which citizens and businesses can find information and easy cybersecurity implementations on dealing with SPAM. The websites main interest is for the users to gain knowledge about cyber security because most users are misinformed about how to deal with SPAM. The website will help them implement sufficient cyber security measures.

3.2 Distribution of costs and benefits

Costs for the department: research and hosting the website.
Benefits for department: less economical loss due to SPAM, if campaign shows a positive effect more budget will be allocated to the department.
The actors involving the countermeasure are the businesses and citizens of the United States of America. They do not have any direct costs if the countermeasure is implemented. However, they do have indirect costs because the website is government run, which means it is paid for by tax revenues. These indirect costs are merely a fraction of the potential benefits the cyber security information website has.
Businesses and citizens' benefit because they can make use of the security measures, which are listed on the website to help them prevent future losses by SPAM.

3.3 Actor incentive

It is the department of economic affairs' responsibility to support and improve economic activity as much as possible. Engaging in SPAM causes a lot of economic damage. This is the reason the department of economic affairs has a major incentive to stop employees of businesses and us citizens from engaging in SPAM.

3.4 Externalities

Large government investing in cybersecurity leave less budget for other projects that also help improve the economic growth of America.

4. US Companies

4.1 Concrete counter measures

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:

	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, 200). 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

To invest 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 dollar on lost productivity. Besides that, every year employees waste two working days (more than 1200 minutes) dealing with SPAM (CALIENDO ET AL.).

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 can be seen as bugs in the SPAM filter (THORKILSSEN, 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 once in a while. The error cost of a false positive should therefore be assigned a higher value than the false negative (THORKILSSEN, 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.).

(CALIENDO ET AL.) 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 to SPAM protection, they might pick that weak company earlier than a company with strong spam policy.

4.4 Externalities

To be written

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

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

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.

Furthermore 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.

Lastly, 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 an attractive target for an attacker.

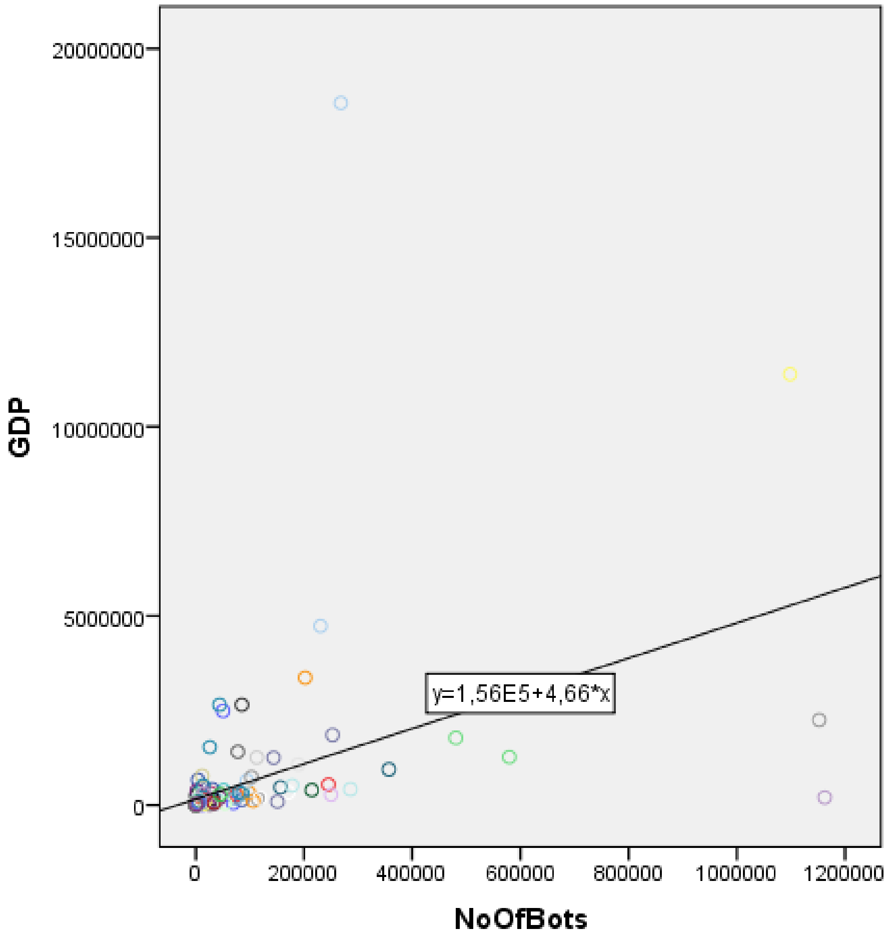
5.2 Statistical analysis

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:

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

As seen in the table above, 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.

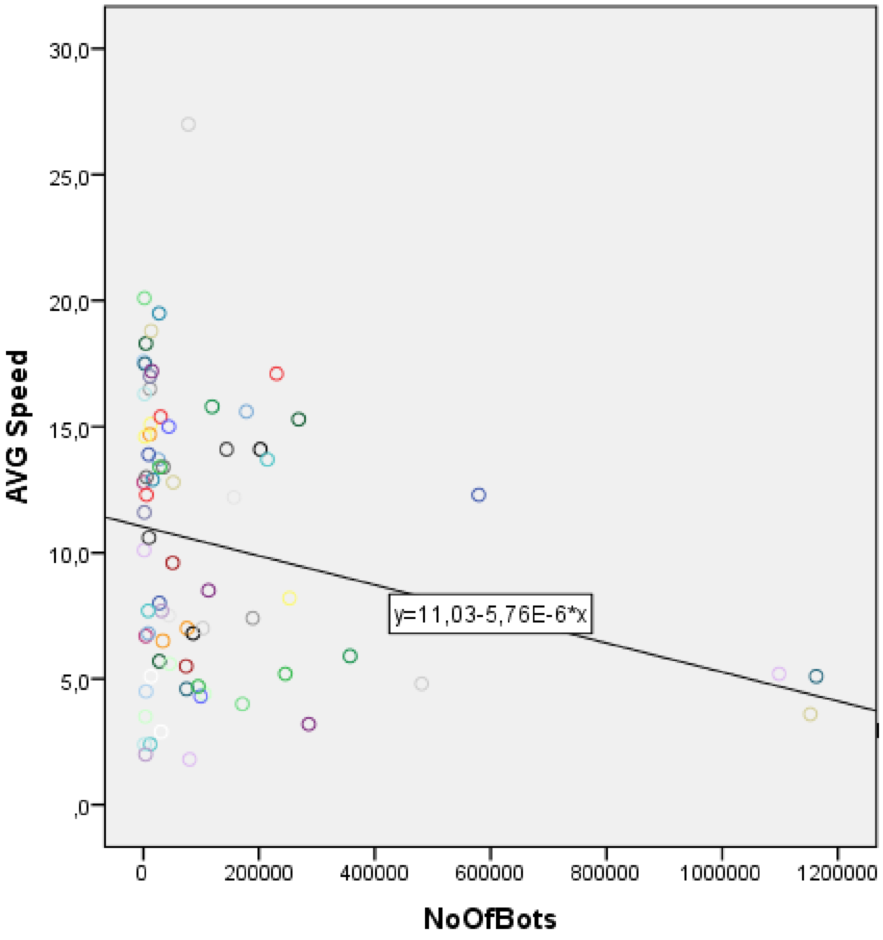


The average internet speed and the number of Bots blocked per country

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.

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.



The average IQ and the number of Bots blocked per country

To be written

5.3 Conclusion statistical analysis

To be written

6. Conclusion

To be written

References

World Economic Outlook Database. (2016, 21 October). Retrieved 2016, from International Monetary Fund: http://www.imf.org/external/pubs/ft/weo/2016/02/weodata/index.aspx

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

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

Callen, T. (2012, March 28). *Gross Domestic Product: An Economy's All*. Retrieved October 23, 2016, from International Monetary Fund: http://www.imf.org/external/pubs/ft/fandd/basics/gdp.htm

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

Thorkildssen, 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.

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