Assignment Block 3 - Spamhaus

Hugo Bijmans [4253760]
Jorrit van der Spek [4174348]
Ben Hup [1150065]
Eveline Pothoven [4380509]
Lisette Altena [1526413]
Group 8

October 16, 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 problem owner's security issues concerning phishing, the risk strategies it can adopt and calculate the return on security investment (ROSI) for the problem owner. The Department of Economic Affairs in the United States of Amerika is chosen as problem owner and will be the main focus throughout the report. In chapter 2 the participation of the problem owner in the security issue of phishing will be elaborated. Subsequently, in chapter 3 metrics will be discussed that the problem owner can use to measure the performance of a chosen risk strategy. These risk strategies are explained in chapter 4. Chapter 5 and 6 give an overview of the other actors that influence the security issue of phishing and the risk strategies they can adopt. Then the return of security investment will be calculated in chapter 7 and lastly a conclusion will be presented.

2 The Problem Owner

The security issue chosen in our first assignment is phishing. Phishing is a kind of internet fraud where criminals attempt to obtain sensitive information like usernames, passwords or credit cards details (Alert Online, 2016). Phishing attacks tend to use spamming services, like spamming botnets, a lot. A fake bank website is made and a botnet is rented to send a SPAM message to vulnerable people. Even tough spamming is mostly an end-user problem, the problem owner chosen for this assignment is the Government of the attacked country. To reduce that scope even more, we will mainly focus on the Department of Economic Affairs. So in the Netherlands, this will be the Ministry of Economic Affairs (Dutch: "Ministerie van Economische Zaken"). But since the Netherlands isn't massively attacked by phishing/ spamming attacks in comparison to the United-States, the focus will be on the Department of Economic Affairs of the United States of America (Kaspersky, 2016).

The goal of the Department of Economic Affairs is to support and improve economic activity as much as possible. This organization works to create jobs and expand economic opportunities everywhere they can (State.gov, 2016). It does so by negotiating with various parties all over the world to ensure the economic growth of the United States remains high. Everything that can threaten this position is threatening the goal of the Department of Economic Affairs, so this actor will do whatever it's able to do to prevent that.

Since our security issue is phishing, the main risk for the Department of Economic Affairs is to lose economic momentum, the productivity of even real money due to phishing. Economic damage can be caused by simply the time spilled by employees on deleting or answering phishing mails, malware infections after a phishing attack or money stolen by fake bank website. So the Department of Economic Affairs has serious incentives to stop phishing from happening. The strategies it has to accomplish that are discussed in the next sections of this report.

3 Utility of defined metrics

In this section, the metrics necessary for the Department of Economic Affairs in the United States of America will be discussed. Metrics are very important to measure the performance of the to be chosen strategies. Therefore, it is important to know what relevant differences in security performance the defined metrics reveal. In the previous assignment, a few metrics concerning the dataset were defined and tested. If we apply them to the Department of Economic Affairs, some of them appear to be more useful than others. Here, the metrics useful for the Department of Economic Affairs – accurately revealing differences in security performance – will be discussed.

1. Top 10 country per botnet

Bots are not bound by geographic, national boundaries. A top 10 of countries can be established for big botnets, to show what botnet are best represented in which countries. This is relevant to measure, because the government can see its own performance compared to other countries. If the United States of America appears a lot in the top 10 countries where the big botnets operate, they know they perform less well than other countries. They can consider changing their strategy to make the public more aware of safe internet use for example.

2. Botnet activity per country

Each country experiences a different set of active bots sending SPAM. For each country, the top 10 of most active botnets can be calculated. For the Department of Economic Affairs, it is very useful to know the top 10 most active botnets in America. The Department can do further research into which characteristics of the botnet make that botnet especially successful in America. Following, this known characteristics can be used to specify the strategy. A better specified strategy, following on the characteristics of the most occurring botnets, should give a higher security performance. Following, the risk strategy can be updated and specified.

3. Top 10 Internet Service Providers (ISP) that host botnets

Devices are connected to the Internet via an Internet Service Provider (ISP), including bots. Certain ISPs could be more likely to host bots then others. This metric gives us a difference in security performance: if the government knows which ISPs host more bots, they could use this metric to give incentive to ISPs to clean up and support customers in keeping their devices clean, and therefore reach a better security performance than before.

4. Top 10 SPAM sending countries

Not all countries send the same amount of SPAM, and there is no international set of laws telling countries to control this. A top 10 of sent SPAM per country gives a metric, usable to decide which countries pose an additional security risk. It defines directly which countries perform better on security performance. For the Department of Economic Affairs this is very useful to know. Not only do they know their own international reputation, but also do they know to which countries they need to pay extra attention or protection to concerning internet traffic. This can be processed in the strategy of the Department of Economic Affairs.

5. SPAM sent via Tor node

Not all SPAM is directly sent from a bot's IP address. It might be possible that certain bots use the Tor network to send SPAM. This metric gives insight in how much percent uses the Tor network to send SPAM to remain anonymous. The government could enact policies against Tor, in collaboration with Internet Security companies and ISP's. If the percentage SPAM sent via Tor node can be reduced significantly by certain strategies, the security performance can be improved.

4 Risk strategies

Risk strategies can be followed by the problem owner to reduce a security issue. Risk strategies are part of a broader risk management plan as defined in ISO 27001 (ISO.org, 2016). Broadly, there are four potential strategies that can be used to handle risk:

1. Avoid risk: circumventing risk; for example by ceasing activities altogether
2. Mitigate risk: reducing the impact or likelihood (or both) of risk
3. Accept risk: accepting negative (or positive) impact of a risk
4. Transfer risk: outsourcing risk to a third party or parties that manage the risk for you

In the context of the SPAMhaus data set and the three actors (i.e. government, cyber security companies (CSCs) and Internet Service Providers (ISPs)) the potential strategies can be defined as follows:

1. Avoiding risk means:
   (a) Government – cutting citizens from the Internet or at least firewalling the country from access to other nations (e.g. like the great firewall of China). Another less rigorous intervention would be only blocking all e-mail related protocols (e.g. POP3, IMAP and SMTP)
   (b) CSCs – can advise their clients to stop using e-mail
   (c) ISPs – have the technical expertise and blocking power to in fact block all e-mail related protocols from all devices in a certain country
2. Mitigating risk:
   (a) Government – Informing citizens, own governmental departments and the private sector about SPAM and creating awareness of potential threats that can materialize in an impact with certain behavior of these actors. Furthermore, the government has more stringent and permanent options to consider as the *trias politica* divides jurisdiction into three segments. First, the legislative branch is able to create new laws to defend against SPAM. Second, the executive branch is able to execute laws that have been passed (e.g. police officers). Third and finally, the judicial branch applies laws and convicts individuals and organizations when the law is broken.
   (b) CSCs – have (tacit) knowledge to inform companies and other organizations to consult, create awareness and give practical advice how to mitigate cyber risk.
   (c) ISPs – can mitigate risk by educating their support staff on SPAM and botnets. Support staff will be better able to detect and give assistance to out of the ordinary computer behaviour when clients describe it (e.g. slower computer phishing, and slow Internet connection). ISPs can also execute a law passed by the legislative branch of government, for example, to block SPAM or preemptively scan e-mails for viruses, malware and worms.

3. Accept risk:

    (a) Government – can accept the risk by just letting SPAM happen and leaving citizens and organizations to self-organize

    (b) CSCs – can also accept SPAM risk and focus on other forms of risk that might have a higher impact

    (c) ISPs – can accept the SPAM risk by leaving customers at their self-organizing power

4. Transfer risk:

    (a) Government – could enact a law for customers to share the risk of (im)material damage to customers. This way customers might collectively help each other as shared knowledge about SPAM and its risk directly influences the premium each customer has to pay for the 'SPAM insurance'.

    (b) CSCs – could advise customers on a safer cyber environment and might offer insurance against risk at the principle that a customer must install a minimum amount of security to mitigate risk and if risk nevertheless materializes then is covered by insurance.

    (c) ISPs – could also offer customers insurance with the rule that a customer must install a minimum amount of security to be applicable to receive insurance. When a risk materializes in an impact the customer will be covered for damages.

5 Other actors influencing security issue

In the previous and this report are defined three actors: government, Cyber Security Companies (CSCs) and internet Service Providers (ISPs). There are many other actors influencing the SPAM security issue. The most important identified for this report are:

1. **Botnet masters** – are the shepherds of a botnet and access bots via Command and Control nodes (C&C's). Bots will not send SPAM or do anything without an explicit instruction given by a C&C. Destroying the C&C's immobilizes the shepherds flock. Closing C&C's is effectively a root-cause solution by both stopping the SPAM and stopping control over botnets.

2. **Consumers** – are individuals and households that connect to the Internet for information and all kinds of offered services. Consumers are one of the most important actors influencing SPAM security risk. Awareness of consumers means that they could change their behavior to prevent falling victim to SPAM related accidents. If less consumers click on the links embedded in SPAM, then operating a C&C will not be profitable and thus a Botnet Master will seek his income from other criminal activities.

3. **Businesses** – are connected to the Internet to create value for customers. Besides consumers also businesses and it personnel can be made aware of SPAM impact and security policies. Moreover businesses should focus

on the security of e-mail servers and devices besides merely focusing on whether an application is working.

4. **Money mules** – are the actors that withdraw money stolen from consumers. C&C's deposit stolen money in a real bank account. Money mules are random anonymous people that go to an ATM and withdraw the money while withholding a percentage for their service. The money is dropped off at a certain physical location and gathered by the botnet masters. Stopping the recruitment of money mules by botnet masters would be a near root-cause solution as the money does not reach the botnet masters. In addition, Botnet masters do not want to withdraw the money from a bank account themselves in order to stay anonymous.

5. **Programmers (malware code writers)** – are the actual creators of C&C's and write the code to infect new devices that, after infection, are added as a bot to a botnet. Stopping botnet code writers from writing botnet related code would also be a root-cause solution. However, this is nearly impossible as every human being has the fundamental right to have privacy at home. Moreover, a malicious person can write the botnet code in the privacy of his home where the privacy is protected by law.

6. **NCSC: National Cyber Security Centre** – Is part of the Dutch "National Coordinator Counter-terrorism and Security" (Dutch: Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)). The NCSC aims at an open, stable and safe information society. NCSC cooperates within an international network of cyber security specialists known as Computer Emergency Response Teams (CERT). The NCSC consists of both private and public organizations which would in principle mean that the NCSC has both production and blocking power to counter SPAM and botnets (Bruijn & Heuvelhof, 2008). The NCSC also creates awareness in the public and private sector.

7. **Wombat Security Technologies** – Has been chosen as a security leader in the cyber security industry by Gartner (Technologies, 2015). Wombat Security Technologies is focused at creating awareness for its clients. Moreover, the focus lies with three core activities (Cyber Security Excellence Awards, 2016). First, learning science principles, second automating attacks and training, and third integrated solutions at minimized cost. Wombat Security Technologies activities transcends mere awareness creation as the company offers the theoretical and practical implementation know-how. Cyber security leaders such as Wombat Security Technologies could have a positive influence at lowering SPAM by lowering botnet infections through awareness and cyber security implementation in booth private and public sectors.

Some actors like botnet masters and botnet programmers play a primary role in the activation and maintenance of a botnet that sends SPAM. Furthermore, money mules are located close to the root-cause of the SPAM problem as they withdraw the stolen money from malicious phishing SPAM and physically bring it to the botnet masters. Consumers and businesses also play their part in the SPAM security issue as they are responsible for clicking on links in (phishing) e-mails and leaving their guard down and not creating and enacting security policies so new botnet infections may occur.

6 Possible risk strategies

In this section, the risk strategies of the actors described in the previous section will be discussed. These actors are the botnet masters, the consumers, businesses, money mules, the malware programmers, the National Cyber Security Centre (NCSC), and Wombat security Technologies. The sociotechnical nature of the system ensures that these actors have different and even conflicting strategies. These conflicting strategies will be pointed out and the change of these strategies throughout will be given.

The botnet masters control the botnet via C&C. It is the only way for them to communicate with the bots. It is essential that the C&C is protected because without it the botnet masters can't reach their network and thus make money. To reduce the risk the botnet master should use a way to communicate to the bots via the C&C that anti-virus/malware software will not detect. One popular C&C communications technique is to use publicly available DNS servers rather than the systems inside a private network. Advanced-persistent-threat actors try to use public DNS services to avoid logging within the private network and risk detection. (James Ringold, 2014) The goal to protect the C&C servers is the direct opposite of what the problem owners, mentioned in the previous section have namely, to disrupt the C&C. The consumers and business also have conflicting strategies because they are the ones targeted.

Strategies used by consumers are listed in the category risk mitigation and risk transfer. The consumers can mitigate the risk by installing firewalls, make back-ups and don't open untrustworthy emails. Consumers can also transfer the risk toward the ISP. In this case, a contractual agreement of financial compensation with the ISP is formed.

Businesses are targeted a lot by SPAM, The annual cost due to the loss of productivity through spam is estimated to be around $20 billion. This is because a percentage of an employee's time is spent browsing and deleting individual spam messages during a given day at work. (Malik A. Feroze, 2015) Businesses have a lot of the same risk strategies as the consumers but cannot accept certain risks for legal reasons. To make sure privacy data of costumers and other sensitive data is not leaked, employees should be trained in recognising SPAM. A proactive strategy, such as staff training and adoption of innovative strategies in a timely fashion, can yield significant benefits at reasonable costs. (Brent Rowe, 2006)

Money mules make the withdrawals from the bank accounts the money generated by the botnet are transferred to. The names of the botnet masters or the money mules are not registered to these bank accounts which leave them anonymous. The withdrawals are physically done at ATMs which make them irrelevant for cyber security risks strategies.

Malware programmers are the coders that create the C&C's and write the code that infects the machines. Malware uses various techniques to camouflage them to not be easily visible and make their lifetime as longer as possible. Although, camouflage approaches cannot fully stop the analysing and fighting against the malware, but it make the process of analysing and detection prolonged, so the malware can get more time to widely spread. (Babak Bashari Rad, 2012) To reduce the risk to get their malware detected the programmers need to keep investing in new techniques to camouflage the malware.

Governments have begun to develop national cyber-security strategies to outline the ways in which they intend to address cyber insecurity. In many states where critical infrastructural systems in areas such as utilities, finance and transport have been privatised, these policy documents are heavily reliant upon what is referred to as the 'public–private partnership' as a key mechanism through which to mitigate the threat. (Madeline Carr, 2016) The National Cyber Security Centre (NCSC) is such a public-private partnership. The private organisations join the partnership to reduce the systematic risk and to transfer risk toward the government. The partnership is also very useful to the government because it reduces information asymmetries. The correlation between economic growth and national cybersecurity ensures that the different parties in the NCSC cooperate well.

Wombat Security Technologies is the market leader in the cyber security industry that deals with SPAM. They are a commercial business that sells training programs in information security awareness. Wombat Security Technologies does not have direct risk strategies toward SPAM but they sell solutions to actors that have these risk strategies. This makes Wombat Security Technologies indirectly a big influence in combating SPAM.

The actors described above have clear opposite interest concerning SPAM. On the one hand there are the criminals and on the other hand, there are the actors targeted by the criminals. Recently the latter group have changed their strategies toward working together in partnerships. This helps to reduce information asymmetries and thus mitigate the risk. But the constant change in threats and vulnerabilities ensures that all actors always have to keep changing their security strategies throughout time.

7 Return on security investment

To accurately assess the cost and effectiveness of the intended strategy, in this section, the return on security investment (RoSI) is calculated. Therefore the costs and benefits of following the strategy are estimated. There are some caveats to the application of the method and the reliability of the results in this case. These are described in the last paragraph of the section.

7.1 Costs of following the strategy

The US government announced in the Cybersecurity National Action Plan (CNAP) that over $19 billion will be invested in cybersecurity as part of the President's Fiscal Year 2017 Budget (The White House, 2015). A new campaign will start to raise public awareness of the individual's role in cybersecurity and training that helps people to spot phishing attacks and other related threats. It is estimated that one fifth of the total cyber security budget ($3.8 billion) will be used for this campaign.

A major part of the costs from phishing results from financial theft. Therefore companies in the financial sector are recommended to take steps. American Express and Visa, spend $30 million to improve the security of their systems (The White House, 2014).

Furthermore there are companies that offer employee training on phishing. Ponemon institute conducted research on the value of employee training. Specifically, the effectiveness of the training program of security education company Wombat. Ponemon Institute conducted research on the cost of phishing and value of training for businesses with a representative sample of 377 organizations located in the United States. According to this research, the estimated fee of training per employee is $3.69 (Ponemon Institute, 2015).

To calculate the total cost for the training, the fee per employee is multiplied with the number of employees in the US, who qualify for the training, namely those with email access. There are currently 125 million full-time and 27 million part time employees in the United states (Statista, 2016a; Statista, 2016b) of which 39% have access to corporate email systems (Ponemon Institute, 2015). This leads to the total cost for the training of $218.74 million.

Therefore, the total costs of following the strategy are $4.3 billion.

7.2 Benefits of following the strategy

The benefits of a strategy correspond to the expected prevented losses. The costs from a cyber event can be differentiated among first and third party losses. First party losses are the costs which are a direct result from the incident. In the case of phishing this may include the dollar value of financial theft. Third party losses relate to the costs from private legislation, or fines or fees brought by government agencies. Table 1 shows the costs of phishing, retrieved from a research of Romanosky (2016), which investigated the costs of cyber incidents. In this research 12000 cyber events in the United States were examined, of which in 7.3% of the observations (or 921 instances) financial data was available.

Table 1: Costs by event type (in millions)(Romanosky, 2016)

Event type	N	Mean	SD	Median	Mina	Max
Data Breach	602	5.87	35.70	0.17	0.00	572
Security Incident	36	9.17	27.02	0.33	0.00	100
Privacy Violation	234	10.14	55.41	1.34	0.00	750
Phishing	49	19.99	105.93	0.15	0.01	710
Total	921	7.84	47.28	0.25	0.00	750

These costs are incomplete however. It does not include lost revenue, sales and market valuation. Furthermore intangible or nonfinancial costs like lost reputation or productivity are not considered. Although, research of Ponemon Institute (2015) has shown that 48% of the total costs are caused by productivity losses.

Ponemon Institute conducted research on the cost of phishing for businesses with a representative sample of 377 organizations located in the United States. The number of employees of these companies range from less than 100 to more than 75000, on average 9552 users with email access. The cost analysis includes all factors mentioned above. Based on these factors, shown in table 2, the overall cost of phishing for an average-sized company in the sample is estimated to be \$3,77 million annually.

Table 2: Summarized calculus on the cost of phishing (Ponemon, 2015)

	Estimated cost (\$)
The cost to contain malware	208,174
The cost of malware not contained	338,098
Productivity losses from phishing	1,819,923
The cost to contain credential compromises	381,920
The cost of credential compromises not contained	1,020,705
Total extrapolated cost	3,768,820

To calculate the total annual loss from phishing for companies, the average annual cost for a company is multiplied with the number of companies in the US. Table 3 shows a list with the amount of businesses in the United States ranked by its number of employees. Taking into account all small-sized businesses would give a skewed image. Here 99.83% of the companies have less than 500 employees, although in Ponemon's research these companies account for 43% of the researched group. Therefore, only companies with more than 250 employees are considered in this calculation. These category accounts for 67711 companies. Calculation shows that the total annual loss from phishing for companies is \$255.3 billion.

Table 3: USA business list - employee size profile (DMDatabases, n.d.)

Employees	Quantity	% of total	Cumulative
10,000+	1,811	0.01%	100.00%
5,000-9,999	1,707	0.01%	99.99%
2,500-4,999	4,180	0.02%	99.98%
1,000-2,499	7,158	0.04%	99.96%
500-999	15,811	0.09%	99.92%
250-499	37,034	0.20%	99.83%
100-249	162,103	0.89%	99.63%
50-99	297,156	1.63%	98.74%
25-49	843,158	4.63%	97.11%
10-24	1,339,184	7.36%	92.47%
5-9	2,100,398	11.54%	85.12%
2-4	7,580,324	41.64%	73.58%
1	5,814,654	31.94%	31.94%
	18,204,679	100.00%	

Considering that businesses have only 39.9% of the breaches (table 4), the total annual loss from phishing is \$639.8 billion.

Research of Ponemon Institute showed that Wombat Security Education's training program results in a net-long term improvement in fighting phishing scams of 47.75%, see table 5 (Ponemon Institute, 2015).

So, the total benefits of following the strategy would be:

$Losses \cdot \%lossesmitigated = \$639.8 billion \cdot 47.75\% = \$305.5 billion$

Table 4: Five industry sectors affected by breaches in 2015 (Urrico, 2015)

Industry	% of breaches
Businesses	39.9
Medical/healthcare	34.8
Banking/credit/financial	9.6
Educational	8.3
Government/military	7.4

Table 5: Proof of concept results (Ponemon, 2015)

	Improvement
Company A	99%
Company B	72%
Company C	54%
Company D	26%
Company E	62%
Company F	69%
Average improvement	64%
Expected diminished learning retention over time (1-75%)	25%
Average net improvement	47.75%

7.3 Calculating RoSI

The return on security investment is calculated with

$$RoSI = \frac{RiskExposure \cdot \%RiskMitigated - c}{c} \tag{1}$$

Filing in the values determined in the previous paragraphs, gives:

$$RoSI = \frac{\$639.8B \cdot 47.75\% - \$4.3B}{\$4.3B} = 70 \tag{2}$$

7.4 Reflection

The reliability of the calculated RoSI is low for several reasons. Among others, considerable simplifications are made. Firstly, in calculating the cost of implementing the strategy, the cost of training per employee is considered equal for all organizations. However, this value largely depends on the size of the organization. Furthermore, in calculating the benefits of implementing the strategies the results of Ponemon's research are used. Although, this research is based on businesses, the losses in all sectors are considered to be comparable. Yet, the losses from phishing in the health care industry might be considerably higher.

Besides, there are also limitations in drawing inferences from Ponemon's research, because it was a survey. Non-response bias and self-reported results should always be considered when interpreting the survey results (Ponemon Institute, 2015). It should be considered that the costs of an (cyber)incident are often evaluated inconsistently.

8 Conclusions

This report aimed to analyze the actor field of this problem, to identify the problem owner of phishing SPAM and to see which other actors have their influence on the problem of phishing emails. The chosen problem owner is the Department of Economic Affairs of the United States of America. To keep the economic position of the USA as high as possible, this actor has a massive incentive to keep economic damage caused by phishing attacks as low as possible. Metrics to help this actor to limit the economic damage mainly focus on the geographic of phishing attacks. Knowing the locations of your attackers is one of the most important knowledge to have. In order to deal with the risk of the attacks, four potential strategies where defined. Avoiding risk and accepting risk where not the most suitable strategies for the Government to use, but mitigate the risk by informing citizens about the risk of opening suspicious emails was. The most important other actors in this problem field are the botnet masters (shepherding the botnet), businesses (loosing money due to loss in productivity) and consumers (personally victimized by the phishing attacks). In order to formulate solid policies on how to tackle this problem, the problem owner needs to take those actors into account. Finally the return on security investment is calculated of a mitigating strategy, training your staff to detect phishing mail. A RoSI of 70 is calculated, which means that training your staff to not click on suspicious emails can save your company a lot of money. After analyzing the problem field, its actors and their strategies, one can conclude that mitigating the risk is the best strategy to use in order to reduce the damage caused by phishing attacks. Informing your employees at business level and your citizens at country level will lead to a safer cyberspace for everyone.

References

[1] Alert Online. (2016). *Phishing — Alert Online.*. Website visited on 6-10-2016, via `https://www.alertonline.nl/experts/wat-is-phishing`

[2] Bruijn, H. d., & Heuvelhof, E. t. (2008). *Management in Networks: On multi-actor decision making.* Abingdon, Canada: Routledge.

[3] Carr, M. (2016). *Public-private partnerships in national cyber security strategies.* International Affairs, 92(1), 43-62. `http://onlinelibrary.wiley.com/doi/10.1111/1468-2346.12504/full`

[4] Cyber Security Excellence Awards. (2016, February 12). *Wombat Security Technologies.* Retrieved October 12, 2016, from Syber Security Excellence Awards: `http://cybersecurity-excellence-awards.com/candidates/wombat-security-technologies/`

[5] DMDatabases. (n.d.). *USA Businesses List.* Retrieved from: `http://dmdatabases.com/databases/business-mailing-lists/how-many-businesses`

[6] Feroze, M. A., Baig, Z. A., & Johnstone, M. N. (2015). *A Two-Tiered User Feedback-based Approach for SPAM Detection.* ICSNC 2015, 22.

[7] Greenberg, A. (2015). *Report: Phishing costs average organization $3.7 million per year.* Retrieved from `http://www.scmagazine.com/report-phishing-costs-average-organization-37-million-per-year/article/435037/`

[8] KasperskyLab. (2016). *Securelist: SPAM and Phishing in q1 2016.* Website visited on 6-10-2016, via: `https://securelist.com/analysis/quarterly-SPAM-reports/74682/SPAM-and-phishing-in-q1-2016/`

[9] ISO.org (2016). *ISO/IEC 27001 - Information security management.* Website visited on 10-10-2016, via: `http://www.iso.org/iso/home/standards/management-standards/iso27001.htm`

[10] Ponemon Institute. (2015). *Cost of Phishing and Value of Employee Training*, 16.

[11] Rad, B. B., Masrom, M., & Ibrahim, S. (2012). *Camouflage in malware: from encryption to metamorphism.* International Journal of Computer Science and Network Security, 12(8), 74-83.

[12] Ringold, A. R. (2014, June). *Command-and-control servers: The puppet masters that govern malware.* Website visited on 10-10-2016, via: `http://searchsecurity.techtarget.com/feature/Command-and-control-servers-The-puppet-masters-that-govern-malware`

[13] Rowe, B. R., & Gallaher, M. P. (2006, March). *Private sector cyber security investment strategies: An empirical analysis.* In The fifth workshop on the economics of information security (WEIS06).

[14] Romanosky, S. (2016). *Examining the costs and causes of cyber incidents*. Journal of Cybersecurity, tyw001. http://doi.org/10.1093/cybsec/tyw001

[15] State.gov. (2016). *Bureau of Economic and Business Affairs*. Website visited on 6-10-2016, via: http://www.state.gov/e/eb/index.htm

[16] Statista. (2016a). *Monthly number of full-time employees in the United States from September 2015 to September 2016 (in millions, unadjusted)*. Retrieved from: https://www.statista.com/statistics/192361/unadjusted-monthly-number-of-full-time-employees-in-the-us/

[17] Statista. (2016b). *Monthly number of part-time employees in the United States from September 2015 to September 2016 (in millions, unadjusted)*. Retrieved from: https://www.statista.com/statistics/192342/unadjusted-monthly-number-of-part-time-employees-in-the-us/

[18] Technologies, W. S. (2015, October). *Gartner Names Wombat Security a leader*. Retrieved October 12, 2016, from wombatsecurity.com: https://info.wombatsecurity.com/wombat-named-a-leader-2015

[19] Urrico, R. (2015, September 11). *Government Launches Anti-Phishing Campaign. Credit Union Times*. Retrieved from http://www.cutimes.com/2015/09/11/government-launches-anti-phishing-campaign?slreturn=1476081013

[20] The White House. (2014). *FACT SHEET: Safeguarding Consumers' Financial Security*. Retrieved from https://www.whitehouse.gov/the-press-office/2014/10/17/fact-sheet-safeguarding-consumers-financial-security

[21] The White House. (2015). *FACT SHEET: Cybersecurity National Action Plan*. Retrieved from https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan