Spamhaus

Security Investments

Felix W. Dekker, Nick Ho Sam Sooi, Jorai Rijsdijk, Jakob S. Kok

Group number
6

GitHub
https://github.com/Erackron/EoC/

---

1. Introduction

In this report, the previously described Spamhaus dataset will be used to assess the security level for a certain security decision maker compared to other countries. Specifically, the perspective of a cybersecurity agency of a country will be taken. Furthermore, various risk strategies will be discussed. These strategies allow the agency to treat the risk and reach an acceptable risk level. In addition to this, the stakeholders influencing the security issues will be identified. These stakeholders are also able to adopt certain risk strategies which have implications for the strategy of the agency and the security issue itself. Finally, the Return on Security Investment (ROSI) will be calculated for a specific risk strategy in order to assess the effectiveness of the strategy in treating the risk at hand.

2. Scope

First of all, it is key to further scope the problem to the perspective of a single cybersecurity agency. For the purpose of this analysis, the cybersecurity agency of Vietnam has been chosen as the focal point, since the analysis in our previous report has shown a high infection rate in this country and a specifically high percentage of infections with regard to the Gamut botnet (see Figure 1). According to the McAfee Labs Threats report of March 2016, the Gamut botnet was responsible for 21% of all spam in Q3 of 2015[1], which makes it an interesting target for our analysis, especially with Vietnam having a larger than average proportion of infections by the Gamut botnet.

In addition to this, a specific metric needs to be chosen for comparison between different countries. The metric that will be used for this purpose is the bot type infection rate per country. This metric shows the relative amount of infections per botnet in a country and therefore gives insight into which botnets are currently the most dangerous, and indirectly tells something about where the current vulnerabilities are.

---

[1] Measured from the relevant graph provided in
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2016.pdf

3. Security performance comparison

The metric allows us to gain insight into the distribution of botnets in different countries. As shown in the figure below, each country has a different distribution of botnet infections, and in particular, Vietnam has a disproportionate amount of Gamut infections. Disproportional amounts of infections by particular bots indicate general weaknesses relative to other countries, and thus reflects the weakest points in a country's defences. The national agency in Vietnam can learn from other countries' approaches on how to deal with the security issue by looking at their methodologies, technical implementations and regulations.

Furthermore, this insight can provide good indications on where investments are needed. Since Vietnam has a disproportionate amount of Gamut infections, general awareness and technical control mechanisms for this virus should be incorporated on a national and company level.

On the other hand, Vietnam has a surprisingly low percentage of the Conficker virus, which is by far the most distributed botnet across the world. One could argue that this implies better defences implemented in Vietnam towards this virus, but in fact, it can have many possible explanations. Factors like attacking behaviour might play a role and it is complicated to draw valid conclusions from the data.

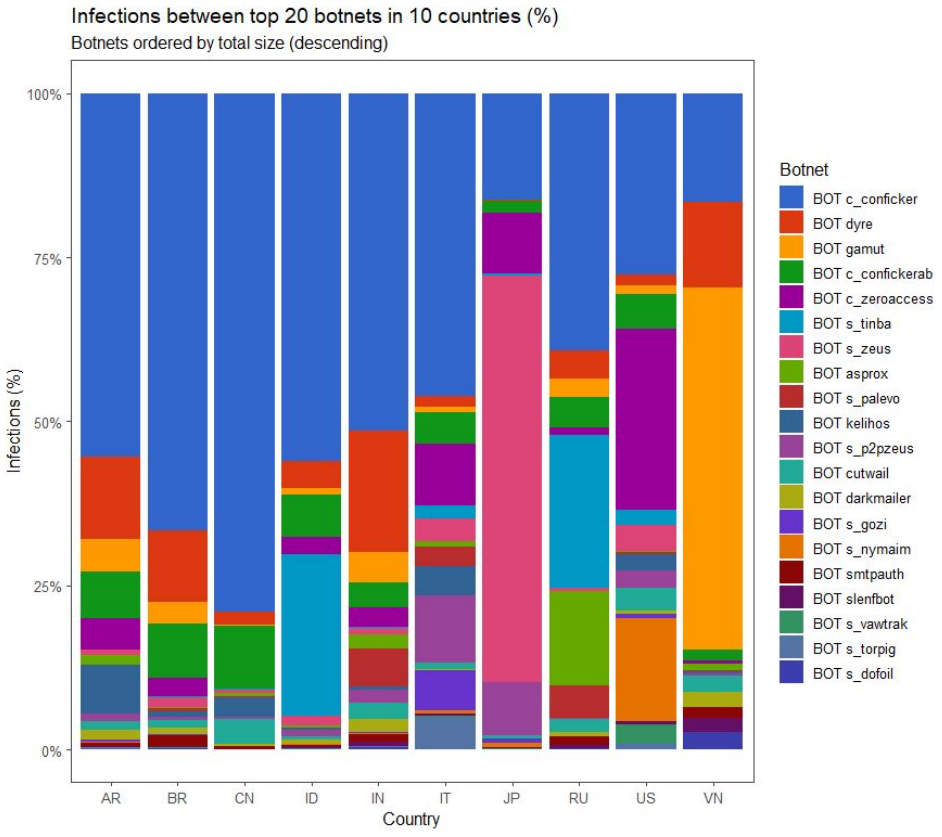


Figure 1: Infections between top 20 botnets in 10 countries

4. Strategy identification

This section will focus on determining the various risk strategies Vietnam can adopt in order to treat the aforementioned risk. There are four high-level strategies that Vietnam can adopt: risk mitigation, risk transfer, risk acceptance, and risk avoidance. These strategies will be discussed in detail as well as their interdependencies.

First of all, *risk mitigation* entails reducing the risk to an acceptable level. This strategy can be adopted by either defending or attacking the botnet. Since Gamut makes use of command and control centres, these centres could be taken down to prevent infected machines from receiving commands. While currently infected machines will remain infected, they will be unable to take action, which effectively disables them. To defend against Gamut, the Vietnamese government could require mail servers in its country to filter emails that contain the virus, though the ethicality of this approach is questionable. The government could also try to raise awareness of the virus in order to prevent more people from being infected, and it could set up contact points that residents could use to ask for help if they are infected or suspect that they are infected. When adopting risk mitigation, the agency should determine which level of risk is deemed acceptable, and monitor how the threat environment and mitigation results are developing. If the agency observes an acceptable risk level, it can choose to alter its strategy to risk acceptance.

Secondly, *risk transfer* entails transferring the risk to another entity or person, for example in the case of cyber insurance or Service Level Agreements (SLAs). To transfer risk, Vietnam could set up a national cyber insurance scheme where companies that put more effort into protecting themselves against Gamut have to pay smaller premiums. However, it is not easy to quantify the effort companies put into this, making it hard to decide on concrete numbers for the premiums. Risk transfer is a sensible choice if the agency is not able to construct an effective risk mitigation strategy or concludes that the costs of mitigation strategies are too high. However, this strategy does make the agency more dependent on external parties, which may be unwanted from a regulatory perspective[2].

Thirdly, Vietnam can adopt the *risk acceptance* strategy, implying that the current risk level is deemed acceptable. Vietnam can choose to accept the fact that there will be infections and consider the current risk level tolerable. In this case, they should still keep an eye on risks as they evolve over time, but for now, they can choose to do nothing.

Finally, *risk avoidance* would require Vietnam to withdraw from all email services to prevent spam from infecting anyone, but this is infeasible as the Internet is a requirement for many of the country's businesses to operate.

[2] Mitre report on risk mitigation

5. Stakeholder analysis

In this section, the different stakeholders that can influence the security issue will be discussed. Furthermore, their relevant risk strategies will be presented. Since the behaviour of actors is highly interdependent, relationships among stakeholders will also be taken into account in the analysis.

Stakeholder identification

Firstly, the attack strategy, motives and capabilities of cybercriminals strongly influence the severity of the security issue. For example, if cybercriminals decide to invest more resources into enlarging their botnet or increasing its complexity, it becomes significantly more difficult to kill it.

Secondly, a diverse set of companies influence the security issue. In order to provide a more in-depth analysis of their influences, a distinction will be made between three types of companies; Security providers, Security consumers and the security industry.

Security providers are companies who/which produce IT soft- and hardware. For these companies, security is not a core competence. Examples of such companies are Google, IBM and Apple. Security providers are able to influence the strength of control measures in machines being used in Vietnam.
The security consumers are companies which are mostly involved with mature markets and make use of IT either to innovate or increase their operational efficiency. Security consumers influence the security level by allocating a certain fraction of their budget to security.
Finally, The security industry consists of companies which have been able to create a successful business model with security as their core competence. These companies develop security technology which improves the resilience of machines to threats imposed by botnets.

Nextly, citizens own machines which can be targeted by attackers. The security of these machines is dependent on their willingness to invest resources into security technology or more secure machines.

Additionally, law enforcement agencies are responsible for enforcing the legislation regarding threats imposed by botnets and other cyber threats. Increased efforts by law enforcement agencies to such threats enlarge the probability of detection and therefore make it less attractive for cybercriminals to engage in their activities.

Finally, regulatory bodies design the institutional framework in which companies and citizens operate. For example, new regulations might force these actors to invest more resources into security.

Stakeholder relationships

As mentioned before, the identified stakeholders are closely related. In order to properly assess their strategies, it is key to properly identify their interdependencies. The result of this analysis is displayed below.

The analysis shows that security providers, security consumers and citizens are dependent on the security industry to safeguard their systems, devices and software against the botnet threat. Moreover, citizens are highly dependent on the companies for security, especially in case of a low amount of security awareness among citizens. The main conclusion to be drawn from this is that governmental bodies have a crucial role in providing regulations which incentivise businesses to either produce secure technology or provide other businesses with security technology. Furthermore, they should provide the regulatory frameworks for enforcement agencies which are responsible for catching the cybercriminals.

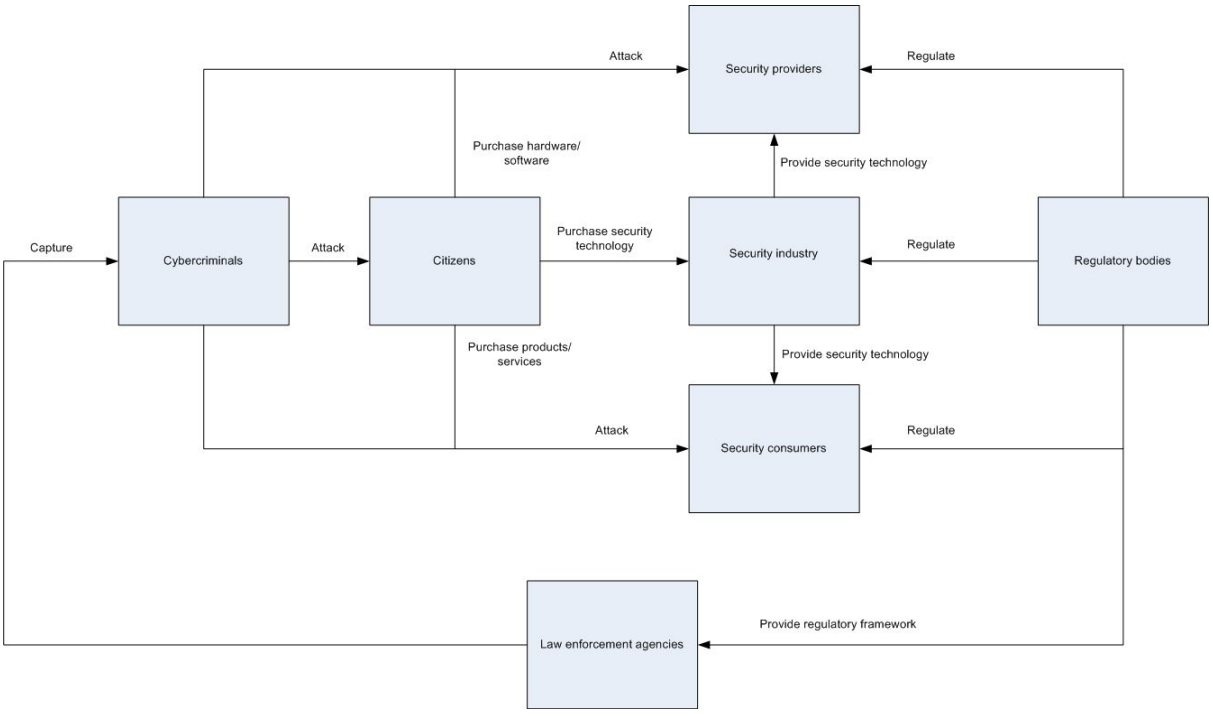


Figure 2: Stakeholder relationships

Stakeholder strategies

Each of these stakeholders can also adopt the four high-level strategies, as described in the previous section. Since the strategies of external parties strongly influence the strategy of the cybersecurity agency, our focal stakeholder, it is crucial to properly address the possible strategies for these stakeholders as well.

To start with, The risk for cybercriminals consists of getting caught and having to pay a fine or serve a jail sentence. They can either avoid this risk by not executing any attacks, mitigate

it by increasing the complexity of their attack or simply accept it. Risk avoidance is generally not a feasible strategy for cybercriminals, since the gain they are after, be it financial or of another type, cannot be attained without executing cyber attacks or other illegal activities. Risk mitigation seems to be the most sensible strategy for cybercriminals, as this strategy allows them to attain the desired utility while mitigating the risk of getting caught. Finally, the feasibility of risk acceptance is highly dependent on the amount of risk that the criminal is taking. When the risk is relatively low, for example in the case of a complex botnet, the cybercriminal can choose to accept the risk because the probability of getting caught is low.

Secondly, companies can avoid risks by not engaging in risky business activities, accept risks, mitigate them by investing in security or transfer them by buying cyber insurance or incorporating cyber risks in Service Level Agreements. Completely avoiding the botnet threat seems to be ineffective for companies, since this would force them to (partly) execute business processes without internet access, resulting in losses in productivity losses. Investing in security technology, awareness campaigns and other mitigation methods allows companies to lower the risk to an acceptable level. However, it might be complex for companies to identify how high the current botnet threat is and what level of risk is deemed acceptable.

Thirdly, citizens are able to mitigate the risk by making use of secure hard- and software, transfer it by ensuring that the producers of the hard- and software they buy are responsible for losses, accept it, or avoid it by not making use of certain services. For citizens, mitigating the risk can be costly, since it requires investments in security technology. Moreover, citizens can effectively mitigate their risk by increasing their knowledge with regard to protection against the botnet threat. Avoidance of the risk would cause a significant loss in productivity and ease of life and can, therefore, be seen as infeasible for this actor. Furthermore, risk acceptance can seem like a logical choice from the perspective of citizens, because of the fact that in some cases, being part of a botnet does not directly cause any losses. In addition to this, an underestimation of the risk level, probably caused by a lack of awareness, can cause citizens to accept the risk rather than mitigating it.

Additionally, law enforcement agencies are able to mitigate the risk by investing resources in the detection of botnets. By doing so, they mitigate the risk of losses for the stakeholders for which they are responsible, such as citizens and companies.

Finally**,** regulatory bodies can mitigate the risk by creating awareness regarding cybersecurity for citizens and providing new regulations which determine mandatory security technologies or policies. Taking this approach to risk treatment provides regulatory bodies with a means of decreasing the risk for citizens and companies. At the same time, its effectiveness is highly dependent on the response of these stakeholders to the policy.

With regard to the dynamics of these strategies, they are expected not to change significantly within the available data points, since the timeframe of the dataset is one month. However, certain changes in the threat environment might significantly change the likelihood of stakeholders adopting a certain strategy. For example, if the complexity of the botnets increases and losses for companies and citizens are on the rise, it is expected that

regulatory bodies will invest more into the mitigation of these risks, citizens and companies will look for possibilities to transfer it and cybercriminals to further mitigate the risk by limiting their chances of getting caught.

6. Analysis

We have decided to analyse the cost-effectiveness of enforcing the installation of spam filters on mail servers in Vietnam. The effectiveness is calculated over the period of one year and will be expressed as the *Return on Security Investment* (ROSI), which is calculated according to the following formula:

$$ROSI = \frac{(Risk\ Exposure \times Risk\ Mitigated) - Solution\ Cost}{Solution\ Cost}$$

Furthermore, the risk exposure is expressed as the product of the *likelihood* and the *impact*.

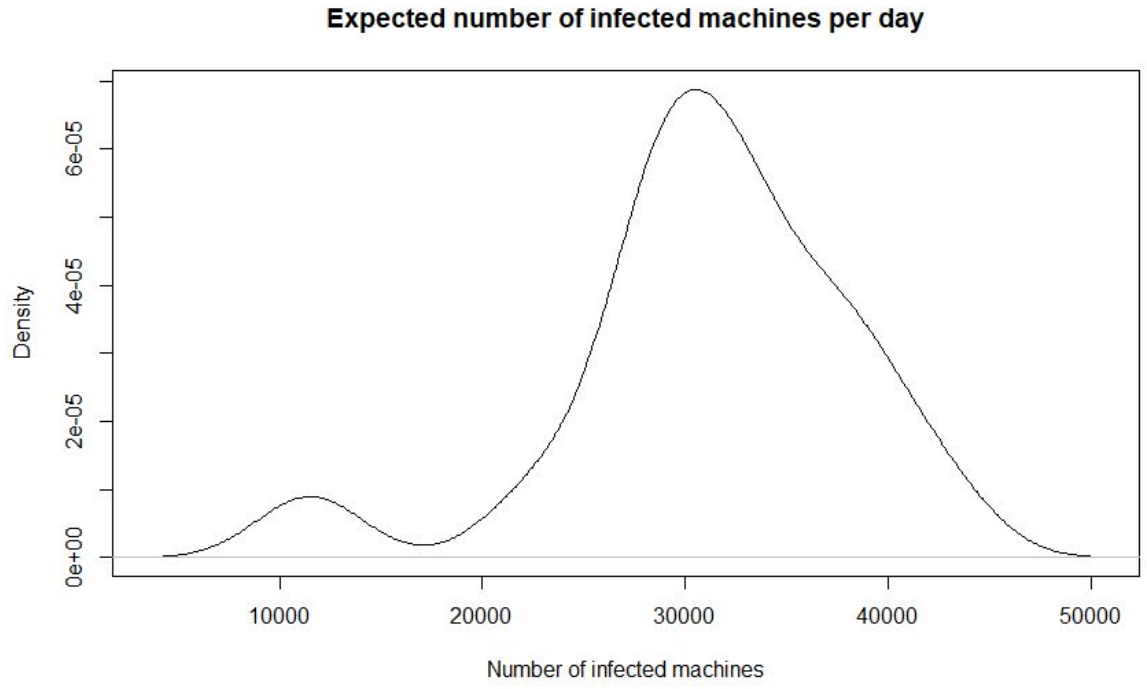
This means that we need to find four values:

1. Likelihood
2. Impact
3. Risk mitigated
4. Solution cost

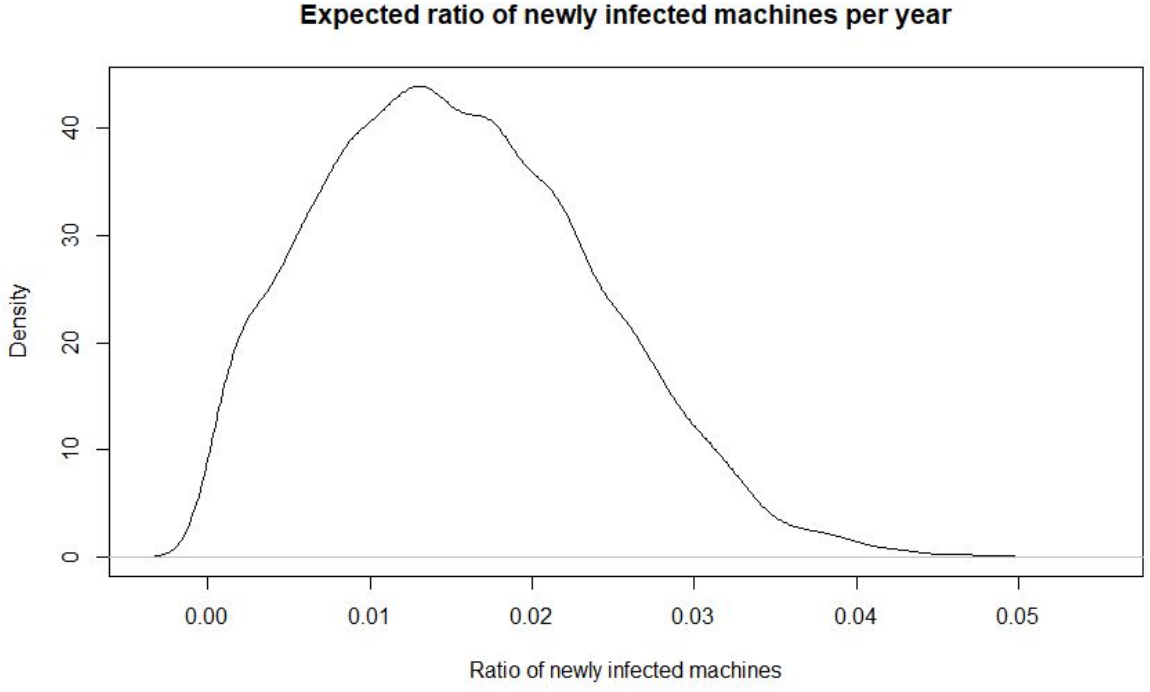
To improve the quality of our risk analysis, ROSI will be expressed as a distribution. This is because the exact ROSI cannot be determined because of uncertainties in our measurements and because the risk environment itself is unpredictable.
Expressing ROSI as a distribution requires that the four values mentioned above should also be expressed as distributions. However, for simplicity, we have decided to express *risk mitigated* and *solution cost* as constants.

6.1 Likelihood

The likelihood expresses the expected ratio of newly infected machines in the coming year if no action is taken. Before this likelihood can be calculated, we first need to find the expected number of infected machines per day. This value can be obtained from the Spamhaus dataset by counting the number of newly detected infections per day; the density of this data is shown in the figure below.



To simplify further calculations, a normal distribution can be fitted around the expected number of daily infections. By multiplying the distribution of the daily number of infections by 365, the expected number of infected machines per year can be obtained. By then dividing the curve by the number of Vietnamese citizens with Internet access, an estimate of the ratio of infected machines per year is found, which is shown below.



It must be noted that this approach is overly simplistic because it assumes that the numbers can be approximated by a normal distribution, even though we have no evidence for this. Furthermore, the number of new infections per day would increase over time because

network effects allow each computer to infect multiple other computers; but after some more time the botnet will slow down again because there aren't many machines left to infect.
All this is ignored in our analysis for simplicity.

6.2 Impact

The impact describes the expected costs under the condition that loss occurs. Therefore, the impact calculation is not concerned with the probability that a loss may occur.

To create the impact distribution, several assumptions must be made since it is either totally unfeasible to find the correct data or some of the variables do not have a deterministic value. We are looking at how much an infection of the Gamut virus is going to cost the individual on average, hence the finding the distribution of costs related to the infection.

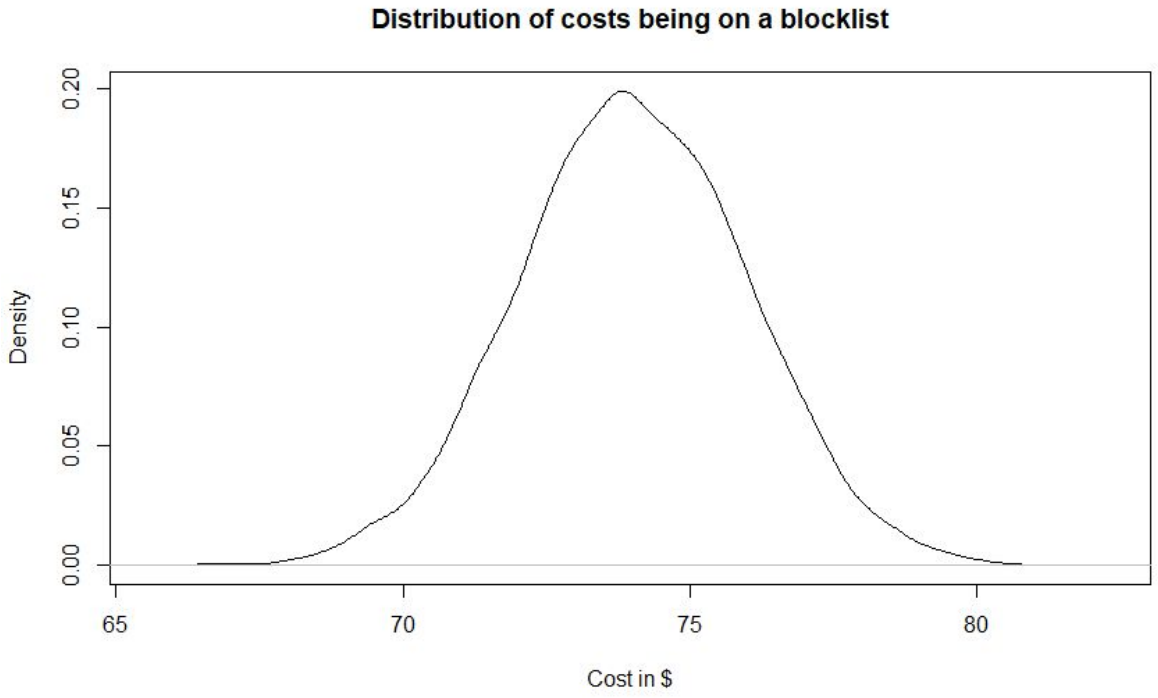
The average person in Vietnam has a monthly salary of $150 a month[3]. This makes for ca. $1 per hour, considering normal workload (35–40 hours a week). We are interested in estimating how much money is lost by the average person when their mail service is put on a blocklist. This number will vary, as not all people are dependent on sending mail for conducting their work. To make the calculation a bit easier, we assume 10% of the people working in Vietnam cannot properly work without their mail server functioning.
Furthermore, we have to make an assumption on how long a specific domain will be on a blocklist before it is removed. For this calculation, we assume that on average it takes 15 days to find out you are on the blocklist, 3 days to implement features that fix the spam issues, then another 2 days for it to be removed from the blocklist.

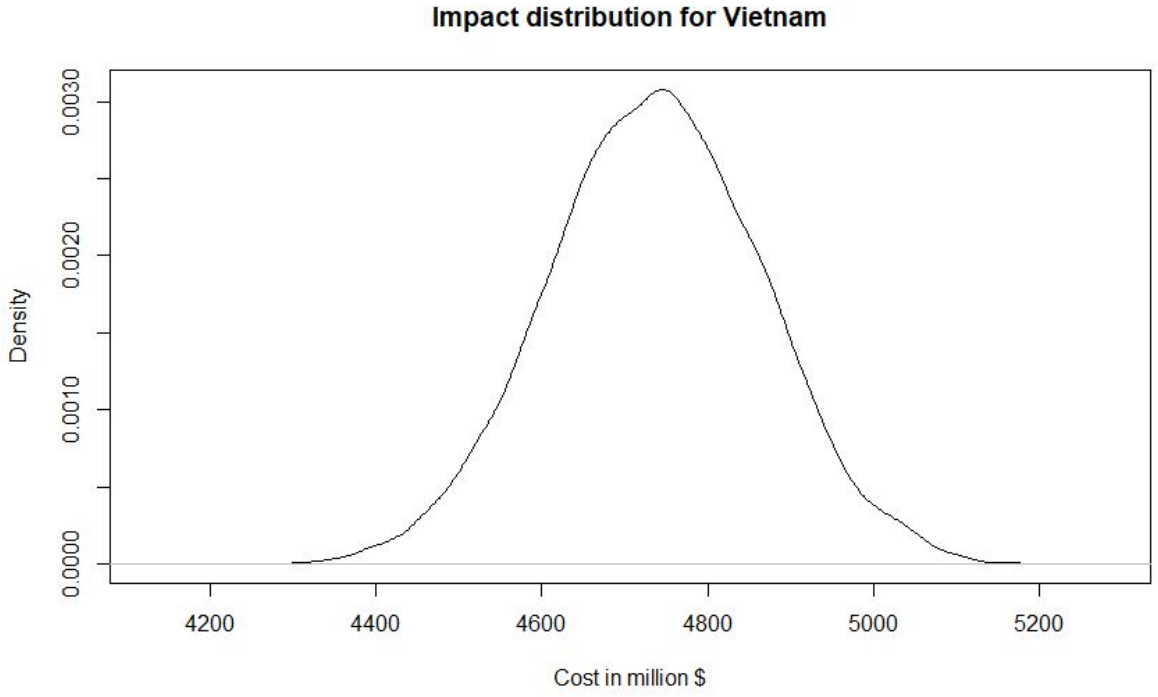
To find the average loss of a citizen in Vietnam we must use the law of total probability:

$$10\% * (37h * 20days) * \$1 + 0.9\%(0) * \$1 = \$74$$

We choose a standard deviation of 2. We must emphasize that these are highly artificial numbers which we created in order to find the impact distribution and that they are in no way representable for the actual scenario, but we consider it sufficient for this assignment. Furthermore, we assume a normal distribution, with independent variables. In reality, the chance of an infection occurring is not independent between multiple machines, because machines in the same network are more likely to infect each other.

[3] https://www.vietnamonline.com/az/average-salary.html





6.3 Risk Mitigated

The risk mitigated represents the percentage of infections that are prevented by implementing our chosen measure, in this case, a spam filter. According to an online

whitepaper by Spamhaus, the source of our dataset, the effectiveness rate of a properly set-up spam filter using only free, open-source software can already reach 99.6%.[4]
Since the Gamut botnet propagates using trojan downloaders that are sent through spam messages[5], we assume that this spam filtering effectiveness rate can also be used for the percentage of infections that are mitigated.

6.4 Solution Cost

In this section, we look at costs for Vietnam to implement these risk-mitigating controls. The main cost is going to be installing spam filters on all Vietnamese mail servers.
To derive some estimates for the total cost of installing spam filters on all mailboxes in Vietnam, we must start with the number of people in the world (in 2016), which is 7.3 Billion[6]. The percentage of internet users in 2016 was 47%, and the number for Vietnam in the same year is 43.97 million. Finding the percentage of internet users being located in Vietnam:

$$43.97 \div (7300 \times 47\%) = 1.282\%$$

To find the number of mailboxes in Vietnam, we must also start with the amount of mailboxes globally (in 2015)[7]. This leads us to approximately:

$$4353 \times 1.282\% = 55.78 \text{ million mailboxes}$$

Let's assume Vietnam will use SaaS-style spam filter providers. According to Spamtitan, the costs are roughly around $3 per mailbox[8], but since this price is based on just 5000 mailboxes, Vietnam, with roughly 56 million mailboxes, can probably get this for a lower price, assuming economies of scale. This leads us to our estimate of $1 per mailbox per year.

For a price of $1 per mailbox per year and 55.78 million mailboxes, the cost of a spam filter for all of them would be *$56 per year*.

6.4 ROSI

Now that all necessary values have been obtained, the ROSI can be calculated. As noted above, this is done using the following formula:

$$ROSI = \frac{(Risk\ Exposure \times Risk\ Mitigated) - Solution\ Cost}{Solution\ Cost}$$

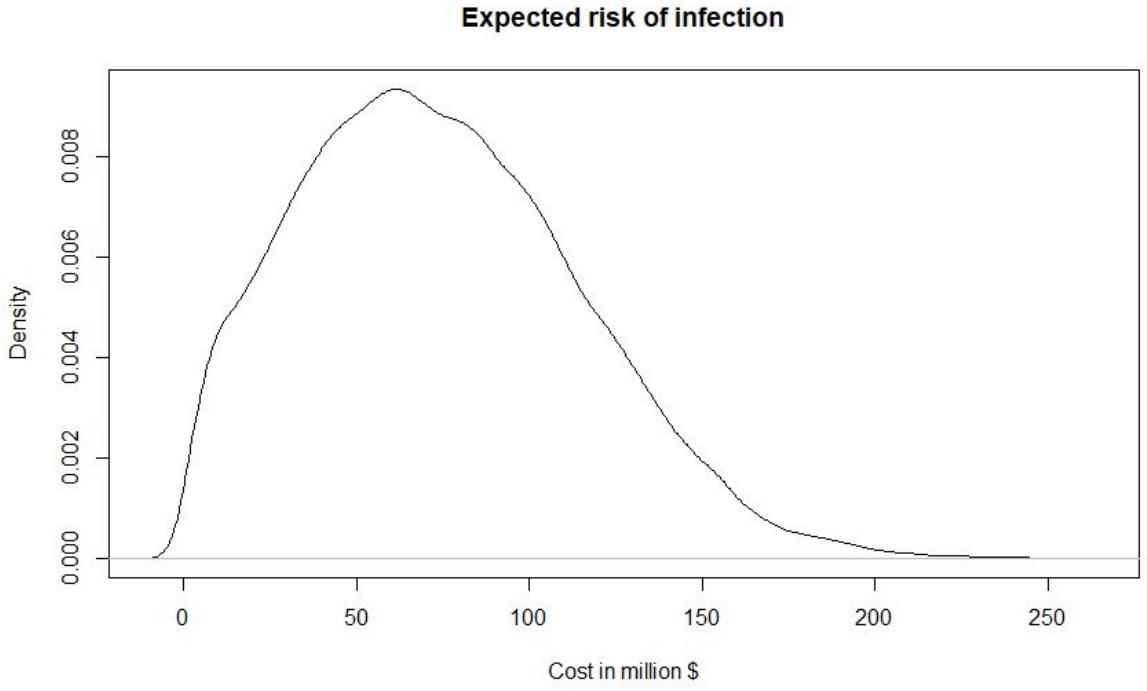
[4] https://www.spamhaus.org/whitepapers/effective_filtering/
[5] https://www.trustwave.com/Resources/SpiderLabs-Blog/Gamut-Spambot-Analysis/
[6] https://www.statista.com/statistics/456519/

[7] https://www.statista.com/statistics/456519/

[8] http://spamtitan.com/

6.4.1 Risk Exposure

First of all, *likelihood* and *impact* should be combined into the *risk exposure*. This is done by sampling the respective distributions 10 thousand times and multiplying their values until a new distribution is obtained. The density of this distribution is shown below. The expected risk is notably lower than the impact described before because the impact described the worst-case scenario without considering the expected success of attacks.



6.4.2 ROSI

The ROSI is calculated by multiplying the *risk exposure* by the *risk mitigation*—which we defined as a value rather than a distribution—and then subtracting and dividing by the *cost solution*—which is also defined as a value.
As shown in the cumulative distribution below, the mean ROSI value is 31.8%.

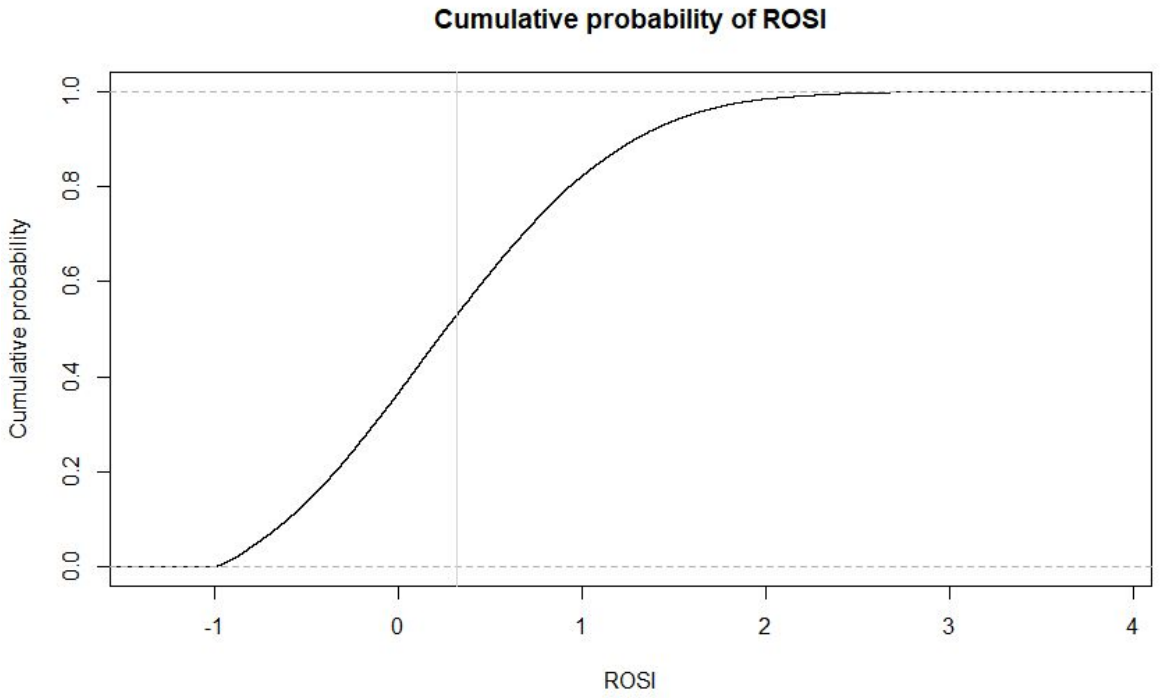


Figure 3: ROSI calculation for spam filters (1 on the X axis is equal to a ROSI of 100%)

Conclusion

To conclude, the cybersecurity agency of Vietnam has multiple options when choosing a strategy for the treatment of the risk caused by the Gamut botnet. Risk mitigation seems to be the most sensible strategy, since this would allow for an effective risk treatment without severely damaging the productivity of businesses and citizens. Furthermore, the stakeholder analysis has shown that the agency should take into account the threat environment as well as the risk strategies of other stakeholders. For example, if cybercriminals choose to invest more resources into risk mitigation by increasing the complexity of their attacks, the agency might choose to alter its strategy to risk transfer, since the efforts of the cybercriminals make detection of the botnet infeasible. The calculation of the Return on Security Investment (ROSI) for the mitigation strategy, specifically the implementation of a spam filter, has shown that a ROSI is expected of 31.8%. Although this calculation is based upon rough assumptions, spam filters seem to be a sensible strategy for Vietnam. Further research should be focused upon determining more accurate values for the costs and losses and comparison of the risk mitigation strategy with the other possible strategies for Vietnam.