Economics of Cyber Security Botnet Tracker
Assignment Block 3

M. Kesteloo - 4291158 & R.D. Meeuwissen - 4287150 & P. Remeijsen - 4286243

September 30, 2018

1

INTRODUCTION

In this report we build upon the security issues and metrics that were defined in the previous assignment. This time the focus will be on identifying the actors as well as the risk strategies that could be involved with our scenario. First, we will give some information about the specific problem which will be the center of this report, namely botnets.

A botnet often sends malicious code to other computers and it does so automatically and autonomously. This way, it creates an even bigger network by infecting victim's computers which will then send the malicious code automatically to others. The data that will be used comes from trackers. These trackers monitor the behavior of the malware, such as the status, infected domains/IP-addresses, botnet Command & Control (C & C) servers and the trackers often provide blocklists to allow firms to block malicious network traffic.

For example, one of the trackers concerns ransomware. This particular type of malware serves to hold data for ransom in order to coerce the victims into paying the spreaders of the ransomware. Like with a lot of types of malware, ransomware often spreads with Trojans. These are files that seem legitimate, but are actually the malicious software. Victims download the malware through either a malevolent source or some other type of scheme. Once the ransomware is on the computer of the victim, it activates and consequently encrypts data on that computer. Next, the ransomware notifies the victim that only the attackers have the ability to decrypt the data in order to recover it [1, 2]. Sometimes the victim can decrypt the data themselves, but as these types of criminals have become more advanced, the level of encryption has also improved. The result is that the victims are left with the choice to pay, or consider the data to be lost. Ransomware is a significant problem with a very large number of victims and is certainly at the forefront of cybercrime. This particular tracker differentiates between three types of threats. The first type is C & C servers. These are arguably the most interesting as these are the servers that send commands to other nodes in a botnet. The second type are payment sites and the third are distribution sites. These are distinctions that other trackers often make as well. ZeuS and Feodo are also financial malware. ZeuS can for example be used by criminals to install ransomware, but also to steal information by installing key loggers or using other techniques.

Many researchers have been investigating how to handle botnets. A research paper by Tajalizadehkhoob et al. [3] elaborates on three strategies:

- Access providers taking down the C & C
- Clean up infected machines
- Hosting providers taking down the C & C

In chapter 2 it is stated what the security issue is, who the problem owner is and which other actors are involved in the security issue. In chapter 3 the metrics from the previous assignment is elaborated. In chapter 4 it is discussed what kind of strategies should be used by all actors involved to reduce the risk posed by the security issue. In chapter 5 the rosi model is evaluated for one of the risk strategies. Finally in chapter 6 it is concluded how the metrics and risk strategies help to remedy the security issue.

2

Security Issue

As already stated in the introduction, botnets pose a critical threat in the society. In the ideal case botnets should not exist. Although this is nearly impossible as their will always be ways to get systems affected by malware, botnets can be greatly reduced. If a botnet is small, the potential threat it poses will be reduced. The reduction of botnets to reduce the potential threat is the security issue that is elaborated in this paper. In the next section it is discussed who the actors are and who the problem owner is for this security issue.

2.1. Involved Actors Security Issue

To remedy the security issue posed in this paper, besides the ISP there are more actors that can be analyzed. There are actors who have a critical position in battling botnets and there are actors which are directly or indirectly affected by the issue. In the next section all these possible actors are discussed.

Directly Affected Actors

The direct actors are the actors that are immediately involved with the botnet. Taken the ransomeware botnet as example, all actors of which the data gets encrypted are the direct actors.

Indirectly Affected Actors

The indirect actors are the actors that are affected because the direct actors are affected. For example when the data of a company get encrypted, they may be unable to support their customers. These customers are the indirect actors.

ISP

The ISP is the supplier of internet services to a lot customers. They have an enormous market share on a national level. All packets of data, and thus also malicious data, is transferred between the customers is routing between their modems. Therefore they are involved in the whole security issue.

Hosting Provider

In case the affected system is not owned by the direct actor but by a hosting provider, then the hosting provider is an actor as well. This is in many situation the scenerio as not many people host websites, clouds or other systems on their own servers.

Governmental Institutions

When looking from a national perspective, government institutions take a part in this issue as well. They use law enforcement to make sure companies keep individuals' data private (GDPR[1]. If this data is leaked, this means that the law enforcement did not work efficiently. Besides, if their own data leaks, the results could be disastrous.

[1] General Data Protection Regulation. Found on: gdpr-info.eu/

2.1.1. EDUCATIONAL INSTITUTIONS

Many educational institutions have their own network. For example a famous and large network in Europe is Eduroam. Also this is like any other ISP a possible internet supplier that could contain parts of a botnet. Though the networks of educational institutions have much less customers than large ISPs

2.2. PROBLEM OWNER

Often it is not enough to clean up infected machines. According to Van Eeten et al. [4], ISPs have a critical position in battling botnets: only 50 ISPs account for 50% of all infected machines. This means that only a small number of actors can have a tremendous impact on botnet mitigation. Furthermore, it is easier for governments to intervene because ISPs often have their target on national levels instead of a global level. Besides, ISPs are the largest internet suppliers in comparison with governments or educational suppliers. In addition, in many cases they also provide internet to host providers. In the last case, this means that packets that are routed to services hosted by the host provider, are also routed over the ISPs network. Because of the enormous responsibility that the ISP has, it is concluded that the ISP is the problem owner.

3

METRICS

In this section we use one of the metrics that was defined in the previous report to investigate a relevant difference in security performance. We have chosen to focus on the metric describing which registrars are relatively often associated with malicious behavior. The metric is defined as the percentage of infected domains of the top 20 most commonly used domain registrars in the ransomware dataset. If one would just count the top 20 most occurring registrars, you are not actually taking the amount of possible domains into account. It would make sense that a larger registrar has more malicious behavior in their network because the chance of infection is simply bigger when there are more possible victims. That is why we have to check percentage of infected domains per registrar instead of just counting the total amount of infected domains per registrar. From the dataset, we only included the registrars with more than 100 infected domains in the dataset.

Next, Registrarowl[1] was used to find the domain count for each domain registrar which is used to calculate the percentage. It should be noted that such a public source for the data is not ideal considering the data is always several months old and the collection is not completely accurate. Furthermore, the entries in the dataset are mostly from 2016 and 2017 and we retrieved the data from Registrarowl in September 2018. However, due to there not being other convenient sources, we have chosen to settle for this.

The relevant difference in security performance that this metric shows is that not all registrars are equally involved with malicious sources. If a dataset such as the one we are using can reveal that a larger fraction of the domains under a certain domain registrar is linked to malicious behavior, it allows decision makers such as the problem owners to better manage their risks. For example, network traffic coming from certain domains registered by a certain domain registrar could be blocked completely if it turns out certain domain registrars are closely linked with malicious behavior. In Figure 3.1, the percentage of infected domains is shown based on the data from Registrarowl and the ransomware dataset. Be aware that the x-axis is shown in log-scale. It is clear that the domain registrar Paknic (private) limited, based in Pakistan, is the domain registrar which is linked to malicious domains most often in terms of percentage: almost 8 percent of the total domains using this particular domain registrar are malicious. It is interesting to note that Paknic (private) limited has a very small market share: only around 4000 domains are registered by this domain registrar. In comparison, GoDaddy.com has the biggest market share with 60 million registered domains but only 0.002 percent of the domains registered via GoDaddy.com are malicious.

[1] http://www.registrarowl.com/index.php

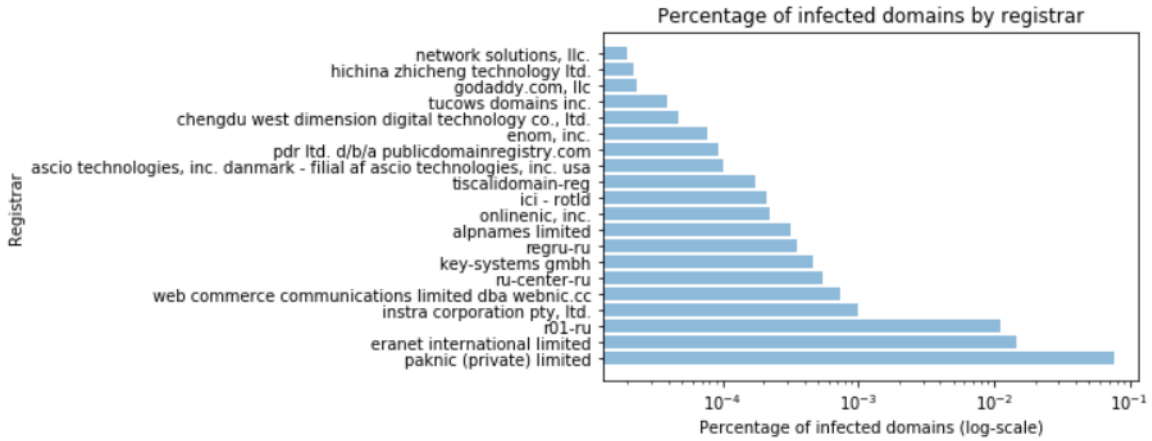

Figure 3.1: Percentage of domains infected per registrar (log-scale)

4

Risk Strategies

In this chapter we will discuss the risks involved in our particular scenario that affect the chosen problem owners. First, we need to define risk. Risk is the probability of an impact, for instance a damage or loss on the expected performance of a system or product. This definition suggest that the problem or security issue can be described in 4 different ways:

- Threat: What is it that can actually happen to the system or actor in general?
- Impact: What are the financial or operational consequences of the threat and how bad is it actually?
- Frequency: How often can or does the threat actually happen.
- Certainty: How accurate are the estimates for the cost and frequency?

Next, we will explore what this means for the problem owners and other actors.

4.1. Global strategies

There are a number of global strategies that enable decision maker to manage the risks that are relevant to their particular scenario.

- Risk mitigation: This would mean actually doing something to take away the risk. In case of an ISP or Registrar this would mean mitigating the risk of being used to host a botnet. One possible strategy could be investing in advancing the monitoring capabilities of the network that they operate. Being able to better detect botnets could result in reduced risk.
- Risk acceptance: Sometimes the actors do not have a tool or policy to deal with the threat, or at least not an economical one. In this case, the ISP or registrars would just say that the botnets are part of reality and the potential victims of attacks by those botnets should take their own precautions.
- Risk Avoidance: When the actors cannot mitigate or accept they could avoid the risk altogether. However, because the hosting of domains is one of the cornerstones of their activities, it will be almost impossible to avoid the threats that we discussed. Only drastic decisions like blocking all traffic from a certain registrars or country might lower the risk.
- Risk transfer: This entails an agreement with a third party to take over the risk. In our particular scenario, this will not be an option, considering there are few insurers that are willing to deal with a threat as unpredictable as cyber crime.

4.2. Risk Strategies For The Problem Owner

As stated earlier, the owner of the problem discussed in this paper are the Internet Service Providers (ISPs). To reduce the risk posed by the problem at hand, the ISPs can use multiple strategies. An ISP should make sure their customers will not get infected systems and will not be a part of a botnet. The major strategy discussed in this paper is making use of trackers. ISPs can use the information retrieved from the trackers. For example the

Zeus Tracker provides domain- and IP-blocklists. The ISP should be responsible to provide this information to the customer. Possible strategies to do this are making use of a firewall, awareness training, and as a last resort nullrouting the DNS or even shutting down the ISP.

4.2.1. FIREWALL

In general ISPs provide a modem to the customer. Most ISPs provide a firewall integrated in the modem (from own experience the Dutch ISP KPN does provide this). A good practise would be if the modem should contain an up to date firewall system. The domain- and IP-blocklists retrieved from trackers should be added automatically to all customers' firewall whenever they are available. This adds layer 3 security to the customers' network. Layer 3 security means that security is on the third level of the OSI-Model (see Figure 4.1) which is the network layer. This means that packets are filtered before they are routed from the modem to the destination system in the network.

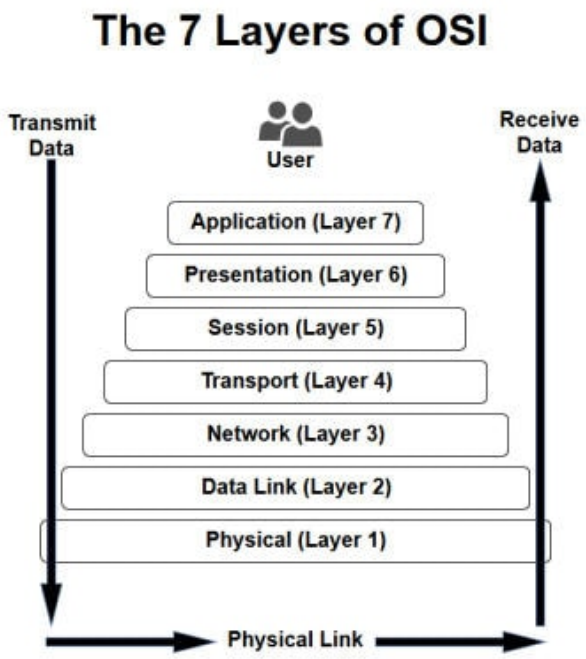

Figure 4.1: The OSI-Model. Layer 3 security means security on the third level of the OSI model. Source: www.webopedia.com/quick_ref/OSI_Layers.asp

4.2.2. AWARENESS TRAINING

Another strategy for the problem owner to reduce the risk is making customers aware of the risks of certain actions on their systems. Unfortunately not all intrusions can be prevented by tools. Social Engineering attack can in many cases bypass any security tools that are in place. Social engineering is making use of malware disguised as something familiar to a user. Whenever the user interacts with it, the system in use can get infected. Making users aware of the social engineering and help them recognize them, reduces the risk.

4.2.3. LAST RESORT

If prevention from getting infected failed, and a botnet is carrying out an attack, there are limited options left. At this moment the ISP can do two things. The first is null-routing the DNS, which means that all domain names are translated to zero. Therefore no IP addresses can be reached from the infected system. A last option is shutting down the ISP and cut off all internet to the devices. This however can be disastrous as exactly all ISP customers' have no internet.[5]

4.3. Risk Strategies For other Actors

In addition to the problem owner, there are other actors in this scenario that could take actions to limited the negative impact of the threat.

4.3.1. Home Users

Home users are not only the most numerous, but arguably the most vulnerable targets. This is mainly due to the fact that there are countless individuals who are not up-to-date on the technical side of things and can't determine for themselves that something is off.

Backup

One of the things that these individuals can do is making regular back-ups. Doing this often enough will ensure that the is as little data lost when the encryption happens. When the data is very little there is little incentive to pay the attackers.

Anti-virus

Another option is to use anti-virus software. Even when an individual makes a mistake of clicking on an email link that they should not have , anti-virus software might be able to detect the malware in time before it can do damage.

Up-to-date Software

Similarly, keeping ones software up-to-date ensures that there are as little vulnerabilities as there have to be. In addition to the software vulnerabilities, new updates might also add newer known malicious parties to white- or black-lists, which in term decreases the probability of exposure to malware sources.

4.3.2. Enterprises

Another type of actor that could be targeted by botnets are enterprises. These might be the preferred targets of cyber criminals, considering that there is often more money to be made compared to targeting individuals. This also means however that the security often is better as well, making it harder for the criminals to actually get the target to pay.

White-listing Applications

One of drawbacks of the enterprise is that there are often many people working on the same network. It is hard to check whether any of those individuals are using applications that they shouldn't be using. One solutions could be the white-listing of applications, so that you can have one person responsible for approving the use of a certain application on the network.

Enhanced Mitigation Experience Toolkit

The EMET is a tool which is used to prevent that unpatched vulnerabilities are used in the Windows operating system. It can mitigate the vast majority of the attacks from exploit kits by protecting against software vulnerabilities that are not patched yet or for which no patch exists at the moment. These are knows as zero-day exploits.

Email Filtering

Nowadays, there are more and more ways to make emails look as legitimate as possible. Cyber criminals can use emails to send malware via the attachments in an email or by simply misleading people to click on a link which is in the content of the email. Because of the many ways of misleading, there are so many people that could accidentally open malware, it is a smart idea to filter or block emails that have certain file types attached, such as: .js, .bat, .exe etc. or which contain a link to known malicious domains.

5

ROSI

To give an example of a return on security investment (ROSI) calculation, we will focus on the actor "end-user": your average Joe who's computer might get infected with ransomware. This person might work for a big enterprise, has his own little company for which he has a website or is a full-time student. The first and foremost risk strategy that this actor can use is making a back-up of the data [1]. There are several options when making a back-up. People can buy a physical hard-drive for making back-ups or they can use an online service like Microsoft's Azure. The downside of making manual back-ups by using physical hard-drives is that when you are working on an important project, you are inclined to create a back-up every now and then. It is however tedious work to manually do this often because you have to plug in the physical hard-drive every time you make a back-up. After making the back-up, the hard-drive should be disconnected because when your computer is infected, there is a chance that the physical hard-drive might get infected too. Furthermore, if you do not do this regularly, you might lose a big part of your important project which is of course an issue. A big enterprise might have some additional servers which are solely used for making back-ups. However, we will focus on the risk strategy where actors will be backing up data using an online service because these services make it very easy to sync your files automatically.

5.1. What the data tells us

When looking at the Ransomware dataset, we can see that the most prevalent ransomware in the dataset is Locky, see Figure 5.1. Locky is a specific ransomware variant that was released in 2016. It was often delivered by email and claimed to be an invoice for a payment. Then, through social engineering, it would get the victim to download the actual malware that encrypts the data of the victim. It gained notoriety through a massive attack on a hospital[2]. Due to this malware type being the most common in the dataset as well as being an example of malware with well documented statistics, we have chosen to use this malware as the focus of the risk analysis.

5.2. ROSI equation

It is difficult for security decision makers to make a decision on where to invest. A good way of making a decision is by using the return of security investment (ROSI) calculation [6]. ROSI can be estimated with the following formula:

$$\text{ROSI} = \frac{RiskExposure * \%RiskMitigated - SolutionCost}{SolutionCost}$$

Risk exposure is the risk that is posed whether a system gets exposed to malicious software. In the case of the security issue of this paper, this could be malware that can encrypt files of the system at any time.

Percentage of risk mitigated is the percentage of the risk that can be solved by means of proper interference. This can be calculated by comparing statistics before and after a mitigation. Using the proper metrics the

[1] See https://ransomwaretracker.abuse.ch/mitigation/
[2] https://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176

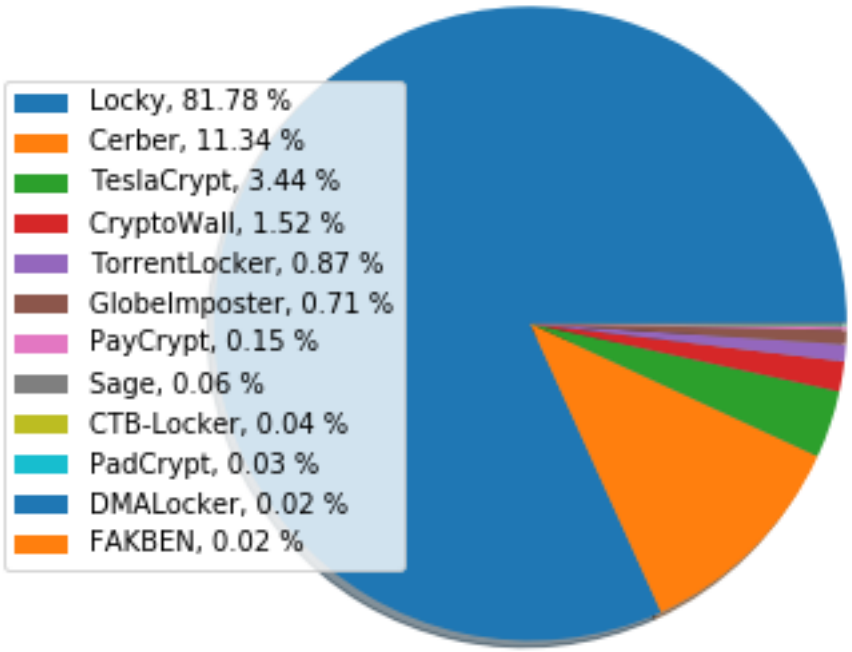

Figure 5.1: Percentage of type of malware

results before and after can be quantified.

Solution Cost consists of all costs of implementing the mitigation. All costs means not only the direct costs of implementing the mitigation, but also the indirect costs that come with the implementation.

When calculating ROSI it should be clear that having a mitigation in place can also bring additional costs. For example, if a new security control is put in place (think of two-factor authentication), it can cause a loss in productivity. However, if this loss is lower than the expected loss when not having the security control in place it can still be considered a decent security investment.

$$\text{ROSI} = \frac{ALE_0 - ALE_S - C}{c}$$

This equation gives us the same result but is easier for calculation. Here we use ALE which means Annualized Expected losses. It is the impact x probability. Where Ale_0 is without the security measures in place and ALE_S is with the security measures in place.

5.2.1. CALCULATING ROSI

AVERAGE JOE

For this calculation the focus is on average Joe who is a freelancer in web development. He works with an average of 8 hours a day. For his work he gets a salary of €25,- an hour, which is €200,- a day. Before Joe heard about the ransomware Locky he did not backup anything. It is assumed that Joe has between 250 and 500 gigabyte of data. There are multiple suppliers for storing your backup data. For the scope of this calculation we use two well known suppliers: Microsoft Azure and Apple ICloud. The prices for at least 250GB data are shown below:

- Price a month Microsoft Azure: €8,433, thus €101,196 a year[3]

[3]Source: https://azure.microsoft.com/nl-nl/pricing/details/backup/

- Price a month Apple ICloud: €9,99, thus €119,88 a year.[4]

As Azure is the cheapest option, it forms the Solution costs. As a backup mitigation Joe backs up his data every day on 22:00. So if his data would get encrypted he can at most miss one day of data.

The top month in 2016 has 90000 devices infected per day[5] There are $17.68 * 10^9$ total connected devices in 2016[6] The risk exposure in this situation is $\frac{90000*365}{17{,}68*10^9} = 4.277 * 10^{-3}$

The percentage of risk mitigated is dependent on how often you would backup. We assume two different scenario's:

1. Joe never uses a backup service. Though after he finishes a job he transfers the data to the customer. We assume in this case that with making a backup every day his percentage of risk mitigated would be approximately 20%.

2. Joe makes a backup once a week. His expected loss if he is a victim of ransomware is then at most one week of produced data. With the mitigation this is reduced with 6 days. The percentage of risk mitigated is then $\frac{6}{7} * 100\% \approx 86\%$

ROSI can now be calculated for the two scenario's.
Secured Scenario:
Unitary Impact: 500-1000 euros per incident, bigger amounts for large corporations or governments [7]. Other costs include loss of data because the victim's files are sometimes not decrypted after paying and the costs when deciding not to pay.
Annual frequency: 25.000.000 - 35.000.000 incidents per year, so for one person the probability of infection is approximately $4 \cdot 10^{-3}$.

Secured Scenario:
Unitary Impact: 0 - 100 euro incident, depending on how often you let your computer sync with the online back-up service. Furthermore, you have to pay around 100 euros every year for the online back-up service. There is also a slight chance that your online back-up service gets compromised in which case you are not able to recover your data.
Annual frequency: 25.000.000 - 35.000.000 incidents per year, so for one person the probability of infection is approximately $4 \cdot 10^{-3}$.

TODO ACTUAL CALCULATION

[4] Source: https://support.apple.com/nl-nl/HT201238
[5] Source: https://www.smartdatacollective.com/locky-ransomware-statistics-geos-targeted-amounts-paid-spread-volumes-and-much/
[6] Source: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
[7] Locky ransomware asks for 0.5-1 bitcoin which is around 500-1000 euros on average over 2016-2017

6

Conclusion

BIBLIOGRAPHY

[1] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, *Cutting the gordian knot: A look under the hood of ransomware attacks,* in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (Springer, 2015) pp. 3–24.

[2] X. Luo and Q. Liao, *Awareness education as the key to ransomware prevention,* Information Systems Security **16**, 195 (2007).

[3] S. Tajalizadehkhoob, C. Gañán, A. Noroozian, and M. v. Eeten, *The role of hosting providers in fighting command and control infrastructure of financial malware,* in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (ACM, 2017) pp. 575–586.

[4] M. Van Eeten, J. Bauer, H. Asghari, S. Tabatabaie, and D. Rand, *The role of internet service providers in botnet mitigation an empirical analysis based on spam data,* (2010).

[5] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, *Botnet: classification, attacks, detection, tracing, and preventive measures,* EURASIP journal on wireless communications and networking **2009**, 692654 (2009).

[6] W. Sonnenreich, J. Albanese, B. Stout, *et al.*, *Return on security investment (rosi)-a practical quantitative model,* Journal of Research and practice in Information Technology **38**, 45 (2006).