Business Model of Botnets

C.G.J. Putman
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
c.g.j.putman@student.utwente.nl

ABSTRACT

Botnets continue to be an active threat against institutions and individuals worldwide. Previous research regarding botnets has unveiled information on how the system and their stakeholders operate, but an insight on the economic structure behind these stakeholders is lacking. The objective of this research is to build the business model and determine the structure of the underground botnet economy. This means determining the botnet life-cycle, revenue streams and overall economic impact on institutions and stakeholders. Compared to other botnet related research, this paper focuses on the financial aspects, breaking down the components of the botnet life-cycle and estimating the money flow to the different actors involved. What can be concluded is that building a full scale cyber army from scratch can only be done by large institutions or governments, as it is too costly. In contrast, by outsourcing different tasks and making use of existing malware packages, costs are reduced to a minimum and reachable for the average person. Applying this method to earlier researched botnets, in every case the botnet resulted in being profitable for the botmaster. Initial setup- and monthly costs were minimal compared to total revenue.

Keywords

Botnet, economics, security attacks, life-cycle, cybercrime as-a service, booter, spamming, click fraud, bank fraud.

1. INTRODUCTION

Botnets and malware have shown over the last couple of years to be a serious threat to cybersecurity. A botnet is a network of various computers which can be controlled by attackers. The controller of the network is called the botmaster. He gives commands to the network by making use of various communication channels. The malicious software used to control this structure of computers is known as malware. In current days generally spread over the internet but in the earlier days malware was more commonly spread by using floppy disks or other physical media (which were then mailed to physical addresses). Goals of malware can be various, but in general malware is designed to make its way to the core system files of a device. This can be, for example, to manipulate or damage system processes or files of the infected device.

Botnets can be a valuable source of money in the right hands. It comes as no surprise the main use of botnets is to make money in some kind of way. [7] Table 3.1 shows four cases of in which botnets are being used, and the estimated revenue earned by the botmasters. Although revenue estimates are known, and knowledge regarding the involved actors is improving, it is still unclear what their profit share is and how they are contributing to the botnet assembly chain. This paper tries, by making use of existing literature and case studies of 4 notorious botnet cases, to provide an insight in the scale of involvement of these actors in the actual crimes that are committed. Results as presented by Miller [23] and Bottazzi et al. [7] give an insight on the actors involved, while Miller goes a step further and tries to estimate costs to launch a cyber-attack at the United States. By putting these results in global perspective, as shown in Table 4.1, it however does not seem realistic that an act like this could be performed by a small independent group of unethical computer programmers.

In contrast, “ready to use” botnet packages and spreading costs account for only a fraction of the total costs estimated by Miller. Botnet packages based on popular malware, such as Mirai and ZeuS, are offered for as little as $30,- and $700,- respectively, while spreading costs lie around $0.10 per infection. [12][48][26] These numbers represent a far more realistic view on historical attacks, as shown in Table 4.2 and aggregate Table 5.1. Fees paid to involved actors only make a fraction of the revenue streams generated by botnet operations, which sometimes rise up to several million dollars of revenue each month. However, in realistic perspective, a botmaster is dependent on various actors or services. The business stands by its weakest link, and by relying on many external factors it makes for a rather unstable environment. An overview of the total operation can be found as a Business Model Canvas, in Appendix 1. Disregarding the risk involved, botnets seem to be an interesting alternative to traditional acts of crime. This is especially the case for some of the actors. Malware developers and money handlers can generate significant revenue themselves, while remaining in the shadows of the real villain.

2. BACKGROUND

2.1 History of botnets and malware

Malware has been around for decades. An example of one of the first type of malware, which infected a large number of systems, is the Morris Worm. This type of malware was released by graduate student Robert Tappan Morris, a student at Cornell University, on November 1988 from a computer situated on the campus of the Massachusetts Institute of Technology. The worms purpose was not to damage system or user files: it only slowed down the infected computer. The reasons for Morris to create the worm has remained unclear to date. [42] Unfortunately, the worm featured a bug which made it possible to spread at an unanticipated rate, infecting many machines around the country. The estimated costs of cleaning a computer from the infection ranged from $200 up to $53000. [43]

Although the worm Morris created did not have a clear goal, the goals of malware being used for botnets are various. These consists of, but are not limited to the following:

- Computer frauds and scams, in which typically criminals design malware to gather payment information of victims or a more recent development, install a Bitcoin mining client to

27th Twente Student Conference on IT, July 7th, 2017, Enschede, The Netherlands.

use the computer's power to generate virtual cash. Advertised spamming can also be included as a type of fraud.
- Cyber-attacks, or more common, Distributed Denial-of-Service attacks. These DDoS attacks have the goal of overloading the servers of the target institution by overflowing it with connection requests. This could result in the servers shutting down, and with that consequently the services the targeted server is being used for.
- Cyberwarfare or espionage. More often than not malware designed for this intended purpose collects privacy sensitive information and intellectual property. [6]

Do remind that the use cases mentioned in this Paragraph are only examples, and that botnets can be used for various other purposes. The development of botnets is a still going on progress, as governments and internet security institutions continue to pursue their goal of shutting down and clearing the world of malicious botnets. The result: a continuous process of more and more advanced malware and botnet technology.

2.2 Analysis of the two botnets

A recent development regarding botnets, and the internet in general, is the Internet of Things (IoT). According to K. Rose, IoT refers to "scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention". [36] These new devices with network connectivity and computing capabilities offer a whole new target group for malware and integration of these devices into botnets. This has resulted in new botnets of unheard scales and capacities. Below one can find two notable botnets, of which one is an IoT botnet and the other being a "regular" computer botnet.

ZeuS, a Regular computer botnet - According to Symantec, the ZeuS botnet has been around at least since 2007, and has since continuously been evolving. [12] According to an article in Dutch newspaper "De Volkskrant", published 27th of May 2017, a Russian hacker going by the name of Evgeniy Bogachev is responsible for the development of the malware. [21] The ZeuS botnet package is an all-in-one package that is readily available for sale, and is actively being traded on underground forums. According to a publication released in 2010, the price for this package at that time ranged from $3000 up to $4000, however with Symantec reporting prices as low as $700. [12][48] While the malware powering ZeuS is allowing the attacker to gain full control over a victim's computer, the attackers mainly use the botnet for financial gain. By making use of so called key loggers, programs that can log the keystrokes of the victim, the attackers steal the credentials of online banking tools. Although exact numbers regarding the total amount of infections are unknown, according to security company Dambella around 3.6 million machines had been infected up to the year 2009, mostly in the United States, with up to 1100 infections a day in March 2010. [41][44]

Mirai, an Internet of Things botnet - On September 20, 2016, the website of internet security journalist Brian Krebs was hit by a DDoS attack of unusual large proportions. According to the company that protects his website from attacks like these, Akamai, his website was attacked with approximately 620 Gbps of traffic per second. In comparison, the largest attack Akamai had encountered before was recorded to put through a mere 363 Gbps of traffic. As Krebs quickly remarked in one of his own articles: "There are some indications that this attack was launched with the help of a botnet that has enslaved a large number of hacked so-called "Internet of Things," (IoT) devices". [20] Ten days later, on September 30th, the presumed creator of the malware used for this botnet published the source code of his creation on the American based website HackForums.net. The malware was dubbed "Mirai" which translates to "Future" in Japanese. Furthermore, it was confirmed the attack on Krebs' website had been conducted by a Mirai based botnet. [39] The release of this source code made it possible for internet security firm Imperva to analyse if any attacks to their infrastructure could be identified as being caused by the Mirai botnet. This seemed to be the case; an attack which peaked at 280 Gbps of traffic per second and made use of 49657 unique IP addresses which hosted devices could be identified as being infected with the Mirai malware. Further research indicated that the infected devices were mostly security cameras, digital video recorders and routers and could be found in 164 countries. [8][14]

On October 21, 2016, internet performance monitoring company Dyn was subject of a large-scale DDoS attack, specifically aimed at their DNS service providing services. This attack caused major internet service platforms to be unavailable for several hours. Affected institutions included major web services like PayPal, Netflix, CNN and many more. A statement regarding the attack and downtime of these services was made a few days later, on October 26, which confirmed that the Mirai botnet was behind the attack. Recorded peak traffic was reported at 1.2 Tbps of traffic per second, an all-time high. Accurate numbers regarding monetary damages towards Dyn and other affected companies are unknown, however John van Siclen, CEO at IT company Dynatrace, has estimated it could have lost companies up to $110 million. [11][40] Furthermore, before the attack, Dyn was the most favoured Managed DNS provider, with 137 customer ranked within the top 1000 Alexa websites in 2015. After the attack, Dyn lost many customers to competitors which resulted in offering their services to only 90 websites in the Alexa top 1000 in February 2017. [4]

Other notable attacks caused by IoT botnets are attacks on Deutsche Telekom (German internet service provider, September 27, 2016) and OVH (A French cloud computing company, September 22, 2016) of which both attacks were presumably conducted by (a variant) of the Mirai botnet. [4]

2.3 Building a business model

To be able to determine the business model of a botnet it is important to understand what a business model is. In this paper I will be using the Osterwalder Business Model Canvas as a basis. This canvas was first spoken about in the "Business Model Generation", authored by Alex Osterwalder and Yves Pigneur. [29] The authors define a business model as "the rationale of how an organization creates, delivers and captures value". Since its publication the theory they propose has been adopted and tested in various organizations, including IBM, Deloitte and Ericsson.

Osterwalder and Pigneur propose nine building blocks as the basis of a business model, the logic of how a company intends to generate profit. These nine building blocks are on its own covering the four core areas of business, being: customers, offer, infrastructure and financial viability. The nine building blocks, customer segments, value propositions, channels, customer relationships, revenue streams, key resources, key activities, key partnerships and cost structure each have their own core question which every notable business should be able to answer. An example of such a question, in this case for the first building block "customer segments", can be "Who are our most important customers?".

These nine building blocks form the basis for the Business Model Canvas. Each of the nine building blocks are represented on this canvas. To make use of the BMC, one can fill in the business activities which apply to a certain building block in the assigned

segment on the canvas. One of the main benefits of this canvas is that this gives the user an organized overview of the business areas that are undeveloped and therefore need attention. Furthermore, it highlights aspects which can be marked as core business activities that have to be maintained to assure the continuity of one's business practices. [34] To be able to make use of the BMC in the case of a botnet business, I determined and categorized the different activities which occur in the different stages of the life-cycle of a botnet. This way it should be possible to apply the theory proposed by Osterwalder to the "business" of developing, starting and using a botnet.

3. FROM DEVELOPMENT TO USE

In Paragraph 1.1 the uses of botnets have been discussed shortly. Unfortunately, the short description given does not do right to the complexity of this subject. Reasons to create malware, setup a botnet or use a botnet are various. As explained in Rodriguez-Gomez et al. [35] botnets go through a certain life-cycle, of which the end is the attack success, which is reached only after all the previous stages have been carried out successfully. Proposed are six stages a botnet goes through in its life-cycle: conception, recruitment, interaction, marketing, attack execution and attack success. These stages are divided into several phases or processes, in which different actors are involved. Understanding the phases of the botnet life-cycle is important to estimate the costs involved.

3.1 The botnet life-cycle

The first phase, conception, is all about motivation: why does one want to setup a botnet? What should the purpose be? On this subject, Rodriguez-Gomez et al. [35] argues there are five types of motivation on why a botmaster would want to setup a botnet. These are money, entertainment, ego, cause, entrance to social groups, and finally status. Of these six it is argued that the major motivations are those which involve financial gain. This is usually reached by selling the source code of the botnet malware, which has been discussed shortly in Paragraph 2.2. More common is renting out the botnet code or its services. The latter is the case when talking about booters. Booters are people, or institutions, which offer to stress web services by making use of botnets. The advertised purpose is to test the stability and integrity of the targeted web service. Using booters, or marketing these services, is not illegal. Booters can therefore be found pretty easily by making use of any search engine. Unfortunately, the services of booters are often used to attack institutions instead of stressing the client's own servers. Stress testing has changed to DDoS attacks, with the client of the booter remaining anonymous.

The second stage is the recruitment phase; infecting computers (or paying others to infect computers for you) with botnet malware resulting in the botmaster being able to control the computer. Usually a larger botnet is better, as the power of a botnet is highly dependent on its size. Especially for booters this is the case. Depending on the size of the botnet, renting a botnet from a booter for DDoS attacks can cost up to several thousands of dollars a day. However, smaller botnets with limited attack power can only cost around $50,- a day.

Next, the botmaster can decide to use the botnet himself, this would be the interaction stage. Bank fraud, spamming or click fraud are among popular botnet uses. If this is not the case, and the botmasters decides to rent out the botnet services or code, it has to be marketed. This often takes place by making use of underground online marketplaces or forums, which can be found and accessed via the dark web. To be able to access these websites one has to make use of software which allows the user to connect to these hidden dark web websites. The software anonymizes the user's digital identity (IP address, hostname) when browsing this network. This is necessary as operating a botnet is illegal in most countries; to setup a botnet it is necessary to hack into and install a piece of malware onto someone's computer to add it to the network of bots. [5] In the U.S., the law that prohibits the user to create a botnet (amongst other fraudulent computer activities) is known as the Computer Fraud and Abuse Act. [1] Other countries have similar laws in regard to fraudulent computer use, which include botnet use and ownership.

Enforcing the correct use of the services that booters offer is much more difficult. An article published on May 16, 2013 by internet security expert Brian Krebs investigates the legality of such booter services. He explains how he got in contact with the moderator of the website Ragebooter.net, one of the more popular booting service providers. Unsurprisingly, the moderator claims his business is completely legit. Later on Krebs confirmed this statement by consulting security expert and former attorney for the U.S. Department of Justice, Mark Rasch. He states that providing booter services is legal, as long as the customer provides a notarized letter stating they requested the service provider to break into the security and stability of their servers. [32] Of course, in the digital world, falsifying these documents can be done with ease. This results in a situation where the customer is hard to identify, and booter is hard to be held accountable for his actions.

Brunt et al. [9] goes deeper into the profitability of DDOS services. An in depth analysis of shutdown booter service vDos, at its peak one of the largest DDOS-for-hire services in the market, gives an insight in the revenue generating process. Over a period of a year, over 800.000 attacks were launched directly from the vDos servers. Transactions were done via Bitcoin and PayPal, of which the latter eventually got scrapped, likely because of privacy reasons. Over a 24 month period, vDos generated a median monthly revenue stream of nearly $26k, maxing out at nearly $43k. Although not useful for this research, an average of 970 customers per month made use of the service over this 24 month period. Exact profit margins are unknown, it is however concluded that even after the removal of the PayPal payment option, which in August 2015 resulted in a decrease of around $12.5k revenue from an average of $28.5k in the previous months, vDos was still profitable. Major costs for vDos were estimated to be hosting and customer support, minor costs being (amongst others) payment processing charges.

Authors do, however, not agree on the most profitable use for botnets. Bottazzi et al. [7] states that spamming and DDoS-attacks can be considered least profitable, since the operation is too noisy, which stands in great contrast to the findings in Kanich et al. [18] and the in Brunt et al. discussed vDos case. A summary of previous findings on these cases can be found in Table 3.1.

3.2 Actors in the life-cycle

Through the several stages which became clear in the previous Paragraph, many actors are involved in the process. Bottazzi et al. [7] has defined a botnet assembly chain, which contains six different blocks regarding activities varying from development to utilization. Furthermore, this assembly chain is coupled with the level of skill necessary to be able to successfully complete the activity mentioned in the brick, and the "darkness" of the market it is operating in. The latter indicates the level of illegalness the actions a user has to perform are. In general it is concluded that in advanced stages of development actions turn more to the illegal spectrum while more skill is necessary in the earlier stages of development of a botnet. Gosler et al. proposes

Paper	Activity	Malware	Context	Finances
Kanich et al.	Spam advertised pharmaceutic als	Unknown	360 Million emails per hour, 10.000 bots	$100 per sale, $3.5 mil. annually
Bottazzi et al.	Robbing bank credentials	Eurograb-ber, ZeuS based	30.000 Targets across Europe	$47 mil. over 2.5 months
Brunt et al.	Booter, botnet-for-hire	Unknown	800.000 Attacks over a 1 year period	$26k monthly revenue, median of 24 months
Bottazzi et al.	Advertise-ment click fraud	Zero-Access	140.000 hosts	$900k of daily ad revenue losses

Table 3.1: Overview of botnet case studies

a similar division, however more based on the involved actors, which he calls tiers. [13] This model can be found in Table 3.2.

The hierarchy consists of four different tiers, which show some similarities to the supply chain as proposed in Bottazzi et al.. To compare both models I will look at the different stages and indicate similarities as well as differences. It is, however, already clear to see that the tier model is focused more on the technical development of a botnet. Tiers two to four all contain actors which are involved in developing or discovery of malicious code, which makes it necessary for the involved actors to have at least some technical programming knowledge. Tier one, on the other hand, is at first sight comparable with the actors involved in the last three stages of the Bottazzi et al. model.

The first stages of the botnet supply chain, R&D and Money Transfers are arguably legal businesses. Research and development involves the continuous search for exploits in software, the development of new malicious software and selling knowledge of computer systems and software. The actors behind this process are mostly IT professionals, and can (for all we know) have a normal job at an IT firm aside of their malware development activities. These same people offer support, customize the software to the wishes of the customer and operate alone or in groups. If the first is the case, supporting the software can be troublesome. A piece of malware may have been sold to many customers, and giving support to all these customers on your own is nearly impossible. This applies even more when one assumes the person behind these so called Software as a Service provider practices a normal IT job in daily life. The actors in this stage of development can be linked to tiers two, three and four in the hierarchy proposed by Gosler et al.. [43] The latter, Money Transfers, regards providing anonymous payment methods to, for example, the people behind the R&D activities. It is no surprise buyers of malicious software want to remain anonymous as installing this software on someone's computer without authorization, which is necessary to create a botnet, is illegal. Furthermore, the people who get payed for their services would also prefer remaining anonymous as they could possibly (depending of the laws and regulation of the country of prosecution) be convicted of an accessory charge. The discussed two stages in the botnet supply chain are, however, not illegal. This therefore makes for quite a safe business model. However providing customer service to the end user of botnets might, depending of the law, determined as complicity to the crimes committed by the end user.

Tier	Description
1.	Practitioners who rely on others to develop malicious code, delivery mechanism and execution strategy.
2.	Practitioners with a greater depth of experience, with the ability to develop their own tools.
3.	Practitioners who focus on the discovery and use of unknown malicious code.
4.	Criminal or state actors who are organized, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits.

Table 3.2: Tier model of botnet practitioners [13]

The third and fourth brick, C&C Bulletproof Hosting and PPI Distribution operate in a more grey area regarding legality. The first aspect regards services to market and sell the malicious software or goods. Furthermore, it includes offering web-based storage for the botnet end-user to store stolen information like banking credentials or passwords on. The hosting service can also serve as the server for the command and control centre of the botnet master. The command and control centre of a botnet sends out commands to the computers involved in the botnet. This control centre can consist of one or multiple computers, in the last case typically for redundancy purposes. [46] Regarding PPI Distribution; many malware developers do not have the resources to spread the malware they have written to various computers across the world. At least not on a significant scale. To solve this problem they make use of the so called PPI (pay-per-install) Distribution model. In essence this involves the owner of the malware paying affiliates to spread the malware, providing a commission to these malware spreaders per infected device. The client making use of PPI distribution to spread the malware usually collects the funds to be able to afford this by selling regular botnet related services, which are mentioned in Paragraph 1.1. Taking a look at the tier-based hierarchy, it is likely that the practitioners which are mentioned in tier 1 make use of the PPI Distribution model. As is mentioned, these practitioners rely on others regarding the delivery mechanism, which is exactly what the PPI model is about. To give an indication of the usage of the PPI model: Caballero et al. [10] indicates the PPI model is one of the most used ways of distributing malware. Estimates are that of the twenty most prevalent families of malware twelve made use of the PPI distribution model. [26]

Lastly, bricks five and six enter the indefinite illegal spectrum. Actors involved in this stage are the owners of botnets, the ones who actually perform the attacks. As mentioned before, the botmaster can have its own reasons to conduct an attack, but more often than not the owner gets payed by a third party to

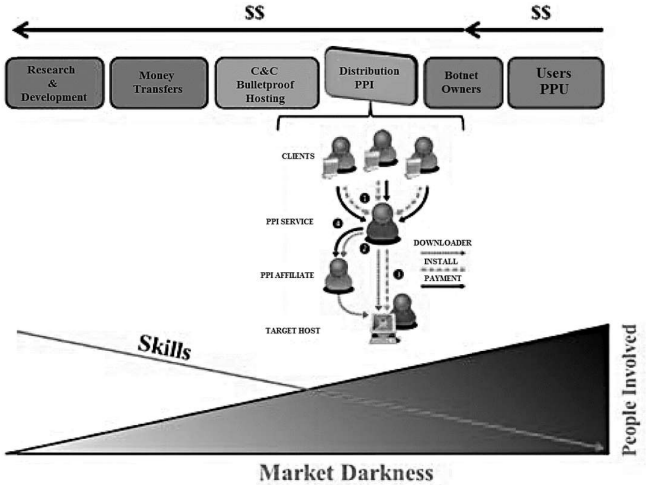

Figure 3.1: Botnet Assembly Chain [7]

conduct an attack. This third party is the sixth brick, persons who make use of the "Pay-Per-Use-Model". In which the botmaster gets paid to execute some kind of plan involving the botnet. [7]

4. LIFE-CYCLE COSTS ANALYSIS

By identifying the various phases which occur in the botnet life-cycle, it should now be possible to estimate the costs involved in each step. In the following Chapter the life-cycle has been split up in three phases, estimating the costs the botmaster has to make to successfully set up a botnet. These steps, acquiring malware, spreading and performing maintenance, form the basis of building the botnet business.

4.1 Acquiring malware

For this calculation, a 2010 research of American computer security researcher Charlie Miller is taken as the baseline. [23] According to his analysis a full scale act of cybercrime aimed to break down great parts of digital infrastructure of the U.S. will set the attacker back an annual amount of tens of millions of dollars. This is therefore indicates such an attack is only really viable for large companies or government like institutions. Furthermore, Miller estimates that planning the attack and developing the malware takes at least a couple of years before it is actually usable. To be able to apply the data he collected into the perspective of other countries I propose the following:

- Weigh in the active amount of internet connections of a certain country - (defined as n) [38]
- Weigh in the ITU ICT Development Index (IDI), which is (according to ITU) "used to monitor and compare developments in information and communication technology (ICT) between countries and over time" - (defined as i) [17]
- Set the active amount of internet connections and IDI base level at the level of the United States.

This has resulted in the following calculation:

$$\frac{n}{n_{us}} * \frac{i}{i_{us}} * Miller's\ estimated\ costs$$

To be able to apply this formula correctly, it is important that at least the number of active internet connections and the IDI are estimated in the same year. The costs estimated by Miller have been released in 2010. Unfortunately, I have not been able to find conclusive data regarding the IDI and the number of connections from this year. Therefore, In this case, I will make use of data collected in 2015. As an example, we can now apply the calculation as mentioned above on a country like the Netherlands. In 2015, the number of active internet connections was estimated to be 15.757.109, while the IDI was 8.53. In the U.S., the number of connections was estimated at 239.882.242, while the IDI was 8.19. [38][44] The total costs as estimated by Miller were $45,5 million:

$$\frac{15757109}{239882242} * \frac{8,53}{8,19} * 45,4 = \$3,11\ million$$

The above calculation would result in an estimate of annual costs of $3,11 million to launch a full scale attack on the internet infrastructure of the Netherlands. This calculation is, however, a very rough and unreliable estimate. Fixed costs apply, and manager costs are being defined differently by Miller. For example, spreading costs will most likely be a lot less when compared to the U.S., simply because the amount of devices is significantly lower. Other aspects, like development, maintenance and tester costs will, according to the formula, most likely be around the same or even higher level in the case of the Netherlands (as the country's IDI lies slightly higher than that of the U.S. but disregarding wage levels). Therefore, I propose to apply the calculation above only on certain aspects of malware development. Doing so has resulted in the results as presented in Table 4.1. As can be seen, when applying the factors only to the aspects which are impacted by the number of internet connections the story changes. Total estimated costs rise with a factor of over 700%. For comparison purposes, the most right column estimates the costs for an average European country (with an IDI of 7.35 [17]) per 10 million connections. This information will be used as a benchmark for a country situated in the Western world.

Actor	IDI	Conn.	US - $ million	NL - $ million	EU – 10 million connect.
Vulnerability analysts	Y	N	2,9	3,0	1,96
Exploit developers	Y	N	7,3	7,6	6,55
Bot collectors	N	Y	4,15	0,27	0,18
Bot maintainers	Y	Y	12,9	0,88	0,48
Operators	Y	Y	5,4	0,37	0,20
Remote personnel	Y	N	0,4	0,42	0,36
Developers	Y	N	2,85	3,0	2,56
Testers	Y	N	0,8	0,83	0,72
Technical Consultants	Y	N	2	2,1	1,79
Sysadmins	Y	Y	0,5	0,03	0,19
Managers[1]	N/A	N/A	6,2	3,0	2,4
TOTAL			**45,5**	**21,5**	**17,4**

Table 4.1: Miller's conceptual cyber army [23]

Why is this information interesting? For a botmaster there are two options to acquire a piece of malware to create a botnet. One option is by making use of readily available malware packages, available for buy on the dark web. Prices range from several tens of dollars up to thousands of dollars. This can be done by nearly everyone and does not require any extreme special technical knowledge. Secondly, one can develop its own malware. The breakdown mentioned above includes Bot Collectors, Bot Maintainers, Operators and Remote Personnel, which are not necessary for the stage of development of malware. Removing these costs from the most right calculation, one would still need around $16 million to launch an attack on an average European country. According to Miller, smaller attacks aimed at single institutions like banks or the stock market can be executed much more economically. Adding to this, Khosrowpour mentions that malware development can take only a few hours up to several months, depending on the complexity of the malware. [19] This would mean less complex malware could indeed be developed by a small group of tech experts, or more complex malware over a longer period of time. For example, the developers of ZeuS, Evgeniy Bogachev and associates, have presumably worked over three years on the development of the ZeuS malware. [21]

The numbers proposed by Miller are certainly very interesting, but not very reliable. They give an indication of how large scale cyber-attacks work, but are not by any means guaranteed an indication of practices of the average botmaster. As mentioned in Chapter 1, premade ZeuS or Mirai malware packages are much cheaper, at only several tens to hundreds of dollars. Comparing

[1] Miller estimates a total of 540 employees is necessary. One junior manager per ten employees, one senior manager per ten managers. Annual wages are set at $100k respectively $200k.

packages with developing from scratch, the contrast could not have been bigger. In the case of Mirai, for $30,- one gets a basic package with two servers and 10 pre-infected bots. A more complete package which includes six servers and 500 pre-infected devices can be bought for $100,-. [24] In comparison, the ZeuS package is available starting at $700,- for the basic package, up to over $10k for more advanced packages. Additional modules can raise the price significantly. [12][48] As discussed earlier, Miller's case would cost around $16 million a year, excluding the lower management costs because of the personnel cut-back. Development costs in the case of the ZeuS botnet, assuming Bogachev is a lone wolf, and assigning him the level 1 pay scale ($125k a year) defined by Miller, this would account for a total of $375k over a period of three years. [21][23] Still only a fraction when compared to Miller.

The costs regarding botnet packages estimated above are in line with other publications. Harris et al. [15] argues that for "the true do it yourself type" there are botnet malware how to guides and necessary tools available for less than $600 in start-up costs. This seems logical: the mentioned ZeuS and Mirai botnet packages are already set up, but still need some configuration to get them running. The more expensive ZeuS packages offer easier and more complete functionality. As in many cases, the more DIY a product is provided, the cheaper it is. However, this only goes as long as you choose from a range of readily available products; creating an entirely new piece of software is a costly project.

4.2 Spreading the malware

Malware is useless without spreading it to various computers. In Miller's case, if one would want to calculate the total costs of malware, including spreading but excluding the use and maintenance of the botnet, it should be possible to add up $160k to the $16 million which is already accounted for. In other cases, the average botmaster will most likely make use of the earlier describe payed per install model. According to Brian Krebs, making use of the PPI distribution model, costs are estimated to vary from $7,- to $180,- per 1000 installations. [26] As both researches have been conducted around the year 2011, it should be possible to compare these costs. Taking the average of $93,5 per 1000 installations ($0,0935 per installation), and comparing this to the estimated $160k spreading costs for an average EU country, with the PPI distribution model it would be possible to infect over 1.7 million devices. The spreading costs in Miller's report appear to be more economical, at around $0,016 per infected device. However, general costs allocated to the managers, system administrators and equipment are not included in this calculation, which could increase the costs significantly.

Miller aims to reach the 100 million infected devices mark after 1.5 years followed up by 500 million after 2 years. He does, however, doubt how realistic these estimates are. These doubts might be grounded: the Dyn attack which disrupted a significant part of the US internet infrastructure was executed with a mere 100.000 devices. This makes the need for 500 million devices seem to be a bit overestimated, if even attainable.

4.3 Botnet maintenance

Botnet malware has to be maintained to ensure effectiveness and to resolve any bugs that might occur in the software. In the case the owner of the botnet is also the author of the malware code, he can resolve these issues himself and release new revisions of his malware if necessary. In case the botmaster has bought the botnet package and does not have the knowledge to maintain the code he has to hire someone else to do this. Usually this is the developer/seller of the malware. According to a Mirai based case study, maintenance costs of desktop botnets exceeds the revenue generated by DDoS attacks. [22] With the rise of IoT, a new target group consisting of less secure devices like CCTV cameras has risen. A botnet composed of these less secure devices may be a lot cheaper to maintain even though it is ten times bigger. A botmaster will always want to grow, or at least maintain, the strength of his botnet. Every disinfection of a device requires the botmaster to infect another device. Software on desktops, laptop and other more advanced devices gets updated on a near daily basis. This makes it possible to patch security holes in software targeted by malware. Consequently this means re-infecting these kind of devices is a time consuming and costly practice. New security holes have to be discovered, and in nearly all cases the disinfected device cannot be re-infected with the same version of the malware. Less secured devices which are not equipped with advanced update features, like CCTV cameras, are therefore an easier target. The Mirai botnet makes use of these devices. Although the malware can be cleared off an infected device by simply rebooting it (as the malware is only stored on the device's RAM, which gets erased when rebooting) the same device can most likely be re-infected almost immediately. [25] This makes it much easier for the botmaster to maintain the botnet strength. He only has to keep a list of IP-addresses which have been infected in the past, and scan if these IP-addresses are still connected to the botnet.

Now that this is clear maintenance costs can be estimated. Re-infection costs have been estimated at $0,0935 per device. For each disinfection a new device has to be infected. Furthermore, the malware creator has to constantly innovate, as security updates are rolled out every day. Lastly, in some cases the malware creator provides customer service to his customers, which bought a malware package from him. According to Miller, a level 1 malware developer earns around $125k a year. Assuming the specific malware is being developed and maintained by a level 1 developer, maintaining the botnet costs the developer around $59 per hour. (Based on 22 working days a month, working 8 hours a day). Let's apply these costs to the two previously investigated botnet malware types:

ZeuS - As re-infection is impossible, the botmaster has to rely on unpatched devices. If this is the case each infection costs the estimated $0,0935. According to ZeuS tracker, the average ZeuS binary antivirus detection rate lies around 40%. [49] Therefore, finding unpatched devices should not be a problem. If the problem should arise new malware has to be developed, or the ZeuS malware has to be altered, this would cost the developer the estimated $59,- per hour. Assuming the developer has a normal tax-paying 8 hour a day job besides malware developing, 8 hours of sleep a day and some spare time, the developer can spend around 4 hours a day on developing and/or maintenance. Over a year's period, instead of maintaining the botnet, the developer could have worked a job which would have provided him around $62k. This will be regarded as maintenance costs per year.

Mirai - As the owner of the infected device has very little influence in making sure his/her device gets patched, or requires at least some advanced computing knowledge to do so, one can assume successful re-infection is more likely to occur than not. Assuming the 2 year warranty period as the minimum lifespan of the product, chances of the device being replaced by a newer non vulnerable device (assuming the device owner does not know his device has been infected) seems negligible. This makes maintaining a Mirai botnet much easier and cost efficient, as each re-infection (if done by making use of the PPI model) only costs the estimated $0,0935. This is, however, all speculation as conclusive data regarding the maintenance of Internet of Things botnets is currently unavailable.

Depending on the intended use of the botnet, it can now be used or marketed to rent it out. In both cases the botnet is being run

from one or multiple command and control centres, which are basically computers which run the software used to control the botnet. Controlling the botnet costs time, of which the costs per hour have been set at $59,- in the previous section. Marketing and selling the botnet costs little to no money. Botnets are generally being marketed on various underground hacker forums, or put up for sale on dark web marketplaces like the Alphabay or the Silk Road. No costs are bound to this process. In the case of a booter, which usually markets his service out in the open, some expenditures regarding hosting and building a website have to be made. Website and hosting, in the vDos case, accounted for around $2400,- in monthly costs. [9]

	ZeuS	Mirai	Miller (10 million EU connections)
Malware package	$700,- up to < $10k	< $30,-	N/A
Malware dev.	$125k	Unknown	$16 million
Spreading per device	$0,0935	$0,0935	$0,016
Maintenance[2]	$62k,-	Unknown	$48k
Marketing	$28,8k	$28,8k	N/A

Table 4.2: Estimated botnet setup costs

Summarizing, the total setup costs for a ZeuS or Mirai based botnet can be found in Table 4.2. For comparison, Miller's estimates have also been added. All numbers are on annual basis, except of malware package and spreading costs. Do these results mean a ZeuS based botnet is useless? Most definitely not. As Mirai can only be used for DDoS attacks, since no one is banking or sending emails from a security camera, the activities conducted by this botnet are much less profitable. This should definitely be taken into consideration.

5. BOTNET ECONOMICS

The information given in Chapter 3 provides for an adequate basis to estimate money that flows to the various actors that occur in the life-cycle. Furthermore, case studies of the various botnets give an indication a botnet can have on institutions. With the information available it now should be possible to compare the expenses of botmasters with the damages suffered by the victims.

5.1 Cost-benefit analysis

While the analysis in Chapter 4 focuses on ZeuS and Mirai, the analysis that follows is activity based. The four main botnet related activities, DDoS attacks, spamming, bank fraud and click fraud are linked to a certain type of malware. For example, as explained before, Mirai is only suitable for DDoS attacks. [27] A detailed overview of the researched cases can be found in Table 5.1.

Several side notes have to be made. The specific types of malware that were used in the DDoS and spamming case are unknown. To provide some kind of indication, the popular DDoS malwares Mirai and ZeuS have been chosen to base calculations on. Furthermore, the spammers made use of a fraudulent web shop claiming to sell pharmaceuticals. [18] This is similar to the researched DDoS case, in which popular booter vDos sold their services via some kind of web shop. [9] Because of these similarities, one can assume hosting costs for the spammers were at least as high as in the vDos case. Lastly, the spreading costs are calculated such that all bots have to be re-infected each month. As this most likely is not the case, botnet profit will be even higher after the initial investment. Miller's estimates have not been included in this table, a detailed overview of this can be found in Table 4.1.

At a glance one's initial thought would be that the botmasters are the real winners. Neither of the researched cases of botnet use were not profitable, and three out of four operated for a period longer than 6 months. In the scenario this was not the case, the bank fraud case, this was not necessary. Over a period of 2.5 months a revenue of $47 million was made, the highest of the researched cases. [7] But what is interesting to see is that the actor which performs one of the more legal activities, performing bank transfers, overall places 2nd in terms of financial gain. According to the vDos case, Bitcoin transaction fees lie at 3%. [9] As Bitcoin is an anonymous way of transferring money, it is a widely preferred currency when dealing with illegal money streams. Furthermore, developing malware shows three clear identifiable tactics. Sell malware on a large scale, for a very high price or bind services to a monthly fee. ZeroAccess is a perfect example of how a malware developer should operate: a high price with a recurring monthly payment plan. The contrasting low price of Mirai can be explained as the source code has been made publicly available by the developer. ZeuS is a very flexible package, with the more simple packages providing less options at an appealing price, and the more expensive packages providing more advanced options like bank fraud, be it at a significantly higher price.

Since initial costs vary little between each case compared to the potential profits, it is no wonder spreaders and hosting providers take a significant part of DDoS revenue. Around 25% of total revenue per month to be precise, assuming every bot has to be re-infected every month. A significant part, especially when compared to the maximum of 1.1% of hosting and spreading costs of the other three cases. Hosting could be seen as a viable business, as it brings relatively low risk with it. Spreading, however, brings large risks as it is demonstrable punishable by law. But most importantly, in the end, what remains as profit for

	DDOS - 30000 bots[3]	Bank Fraud - 30000 bots	Spamming - 10000 bots	Click fraud - 140000 bots	
N/A	Unknown	ZeuS	Unknown	ZeroAccess	**Malware type**
1. Developer	Mirai: $30,- Zeus: $700,-	$700,- up to < $10k	Unknown	$5000,- up to $10k[4]	**Malware package costs**
2. Money handler	$780,-	$564000,-	$9000,-	$750000,-	**Transaction fees at 3%**
3. (Bulletproof) web hosting provider	$2400,-	< $70,-	< $2400,-	< $70,-	**Web- and C&C bulletproof hosting costs**
4. Distributor	$2805,-	$2805,-	$935,-	$13090,-	**Distribution costs by the PPI model**
5. Botmaster/user	$26000,-	$18,8 million	$300000,-	<$25 million	**Monthly revenue**
MONTHLY PROFIT	ZeuS: $19315,- Mirai: $19985,-	> $18,2 million	> $287665,-	< $24,2 million	

Table 5.1: Aggregated botnet costs/benefits based on case studies

[2] In the case of both ZeuS and Mirai excluding the costs of re-infecting an unknown amount of devices. ($0,0935 per device)

[3] vDos claimed attacks with power up to 216Gbps. Average internet speed around the world lies at 7.2Mbps. [50][45]

[4] Monthly recurring costs, price varies between packages. [28]

the botmasters? Even though these are very rough estimates, a successful botnet business can provide up to millions of dollars in profit each month. The costs that have to be made to setup a botnet are, as indicated, in most cases nearly insignificant. It seems, however, the real winners are the money handlers. An act that can potentially be defended in court, while collecting great amounts of money.

5.2 Economic impact on institutions

But at what price does this mentioned profit come? Information regarding the overall economic impact of botnet attacks on various institutions is scarce. A possible cause for this could be that it is hard to estimate the economic impact: it is not always known which institutions are affected, and economic impact is more often than not an indirect impact (think of customers not extending their contract at a certain service provider because of botnet attack related downtime) than a direct impact. Furthermore, institutions that have been affected by an attack may be reluctant to release any information regarding this subject. A 2011 report of intelligence provider Detica on the impact of cybercrime on U.K. based institutions defines four types of costs associated with cybercrime: costs in anticipation of, costs as a consequence of, costs in response to and indirect costs associated with cybercrime. [34] Regarding direct and indirect impact, Anderson et al. elaborates on the aspects mentioned above, and give a few examples, based on bank fraud. [3] Some of these aspects are more abstract, like distress suffered by victims and loss of trust in online banking. Because of the abstractness of these aspects, estimating direct impact can be difficult. To provide clarity on this subject. A dedicated research regarding this should be conducted. This research can only be accurate if it started a while after an attack was committed. This is necessary to be able to estimate the long term effects, like non-extension of contracts. Such a research would heavily rely on internal data. This would make it nearly impossible for a third party, like news institutions, to report on this. In existing literature, Anderson et al. features an estimate of overall cybercrime costs in several fields. Unfortunately important botnet related cybercrime activities like booting, spamming and click-fraud are not investigated.

An ongoing research by the Ponemon institute on the costs of cybercrime has, in opposition to Anderson et al., included the costs of DDoS and botnet attacks. Ponemon includes 237 separate companies in their study, and determined the average annual costs weighted by attack frequency. During their observation period nearly 2 attacks per company per week were detected. Of the eight types of detected acts of cybercrime, they found the weighted cost of an "undefined" botnet attack to be the lowest. At around $995,- dollar per attack on average. DDoS attacks, however, rank as one of the most costly types of cybercrime, at $133,5k costs on average. Finally, nearly all of the companies have experienced infections of devices with malware on their network (this includes ransomware, a type of malware which locks up the data on the device after which the blackmailers demand a fee to unlock the computer). Even though malware is being ranked as the second least costly types of cybercrime, at $5110,-, due to its frequency of attacks it makes for the costliest of all researched types of cybercrime. Furthermore it is known that the time it takes to resolve a certain act of cybercrime significantly changes the impact factor of that particular act of cybercrime. Ponemon has estimated that if it takes less than 30 days to contain a cybercrime attack the average costs lie at $7,7 million. If it takes much longer, greater than 90 days, the costs rise to around $12,2 million on average.

Further analysis on the breakdown of these costs regarding external consequences caused by cybercrime indicate that information loss has the greatest impact, followed by information- and revenue losses. Of course, external consequences do not single-handedly account for all of a company's expenses regarding cybercrime. Detection, recovery and investigation costs are, among other costs, also take a significant part of total damages. Unfortunately, Ponemon does not provide absolute financial data regarding this, whilst the division of percentage of costs between those is also unknown. Therefore this data provides not to be useful. [31] Summarizing what is known, Table 5.2 describes per type of attack the subsequent costs of the target company.

Cybercrime type	Percentage of costs	Annual costs (in million $)	Attack costs (in $ x1000)
Malware	16.5%	1,57	5,11
Phishing / SE	13%	1,24	95,8
Web-based attacks	16.7%	1,59	88,1
Malicious code	12.5%	1,19	92,3
Botnets	2.8%	0,27	0,995
Stolen devices	8.8%	0,84	31,9
DDoS	17.5%	1,66	133,5
Mal. insiders	12.2%	1,16	167,9

Table 5.2: Financial impact of botnets on institutions [31]

It is clearly visible that DDoS attacks are amongst the most expensive attacks, accounting for 17.5% of total annual costs. However, DDoS attacks do not occur very often, but when they occur they are not easy to resolve. On average, each DDoS attack costs around $133.5k in damages and larger organizations were more often victim than smaller ones. This is in line with an estimate of Overvest et al. which mentions $52k for smaller companies, up to $444k for larger enterprises. [30] Furthermore, phishing is most likely the result of spamming, one of the various uses of botnets. Spamming is also a possible cause for infection with malware, although malware can also be found on various sketchy websites which may be visited by company employees. Lastly, the undefined botnet attacks only have marginal impact on the total costs of cyber-attacks.

Web-based attacks include various ways of manipulating software by making use of taking advantage of poor parameter checking, or instruction spoofing. One could state DDoS attacks can also be defined as a type of web-based attack, but since it has its own category in this research Web-based attacks will be disregarded in the calculation of botnet attack costs. [37] Malicious code must not be confused with malware; according to Kaspersky malicious code is "an auto-executable application that can activate itself and take on various forms" and different from malware, it identifies as scripts placed on websites which can exploit code weaknesses in order to upload malware. [47] The remaining two types of malware which cannot be associated with botnets are stolen devices and malicious insiders. This makes sense as they both require physical presence of some kind, which of course a botnet does not.

It's time to draw up the numbers. Several sources indicate that in 2009, around 80% of total spam volume was generated by botnets. Original source seems to be a Symantec MessageLabs report, however this is unreachable. [33] Assuming this, it's safe to say at least 80% of phishing e-mails is being sent by botnets as well. This accounts for $992k in damages, which phishing can be hold accountable for, to the average researched company. Secondly, according to a 2017 Verizon report, 66% of all malware was installed by malicious email attachments. [2] Assuming nearly all malware sent by email is sent by a botnet, this would account to a little more than $1 million in damages.

Adding up these figures up to the DDoS and undefined botnet attack costs, estimated annual botnet damages total to at least $3.95 million. Of course, it is possible that some of the other mentioned acts of cybercrime are related to botnets as well, so it could be very much possible the actual total lies slightly higher. Holding on to this calculation, however, indication is that nearly 42% of all costs related to cybercrime are being caused by botnets in some form or another.

5.3 Business model

So what does a botnet business look like? As explained earlier, Osterwalder's Business Model Canvas is a great tool to display the organization of a business. With the gathered knowledge it's now possible to fill in the business model canvas. In this case the canvas has been filled in from the point of view of a botmaster, and includes the aspects discussed in the various chapters of this paper. Of course, there are more possibilities to utilize a botnet which have not been treated (in depth) in this paper. This should, however not matter. For each botnet activity the basis should remain the same. The canvas has been added as Appendix 1.

6. CONCLUSIONS

Other studies have contributed to research by identifying the actors, assembly chain and revenue streams of botnets. This has provided the possibility of determining the business model of botnets, which at first seems a difficult one, but does not differ from many other supply chains. When tapping into various resources from the actors involved in the assembly chain, as described in Bottazzi et al., setting up a botnet is relatively easy and does not require extraordinary knowledge or investments. By making use of readily available malware packages and outsourcing malware infection it is possible to set-up a profitable botnet business within several days.

Previous case studies have shown botnets can be very profitable, with revenue streams varying from several thousand up to millions of dollars each month. The initial investment costs of malware and spreading, combined with the recurring hosting and transaction fees are of such insignificance that they should not form a barrier for a potential botmaster to start up a business. In three out of four researched cases initial set-up costs accounted for a maximum of a mere 1.1% of monthly revenue. Furthermore it is interesting to see the differences between profitability. For example, based on the case studies, a DDoS botnet should be nearly 35 times bigger to achieve the same monthly profit as spamming. Of course, it is likely the prominent case studies focus on the more successful cases in botnet history, as they drew attention. But it seems highly unlikely that a botmaster, which has at least some technical knowledge, following all the correct steps of the botnet life-cycle assembly chain and taking appropriate identity hiding measures is not making any profit over the long term.

This profit is generated by attacking, misleading or stealing from institutions. According to my analysis, around 42% of all cybercrime related costs can be traced back to botnets, with DDoS attacks firmly on top, accounting for 17.5% of total costs caused by cyber-attacks. With the gathered knowledge regarding botnet actors and their revenue streams, future research should focus on how these streams can be intercepted. This should result in total disruption of the botnet business, as each step is in the assembly chain is crucial for the correct operation of a botnet, and with that reduced damages done to institutions. Huang et al [16] offers a good start in this direction, and furthermore indicates the solutions in his article do not only apply to DDoS attacks. Therefore, applying their proposed solutions to the broader scale of botnet activities could be the next step in dismantling botnets.

7. REFERENCES

[1] 18 U.S. Code § 1030 - Fraud and related activity in connection with computers | US Law | LII / Legal Information Institute: *https://www.law.cornell.edu /uscode/text/18/1030*. Accessed: 2017-06-13.

[2] 61 Percent of Data Breaches Affect Small Businesses: Verizon Report - ChannelE2E: 2017. *https://www.channele2e.com/2017/04/28/verizon-report-61-percent-of-data-breaches-affect-small-businesses/*. Accessed: 2017-06-13.

[3] Anderson, R. et al. 2013. Measuring the cost of cybercrime. *The Economics of Information Security and Privacy*. 265–300.

[4] Angrishi, K. 2017. Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV): IoT Botnets. (2017), 1–17.

[5] Botnet Facts | Washington State:*http://www.atg.wa.gov /botnet-facts*. Accessed: 2017-06-13.

[6] Botnets, how do they work? Architectures and case studies – Part 2: 2013. *http://resources.infosecinstitute .com/botnets-how-do-they-work-architectures-and-case-studies-part-2/#gref*. Accessed: 2017-06-13.

[7] Bottazzi, G. and Me, G. 2014. The Botnet Revenue Model. *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14*. (2014), 459–465.

[8] Breaking Down Mirai: An IoT DDoS Botnet Analysis: 2016. *https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html*. Accessed: 2017-06-13.

[9] Brunt, R. and Mccoy, D. Booted: An Analysis of a Payment Intervention on a DDoS-for-hire Service.

[10] Caballero, J. et al. 2011. Measuring Pay-per-Install : The Commoditization of Malware Distribution. *USENIX Security Symposium*. (2011), 13–13.

[11] Dyn Analysis Summary Of Friday October 21 Attack | Dyn Blog: 2016. *http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/*. Accessed: 2017-06-13.

[12] Falliere, N. and Chien, E. 2009. Zeus: King of the Bots. *Symantec Security Response (http://bit. ly/ …*. November (2009), 1–14.

[13] Gosler, J. and Von Thaer, L. 2013. Resilient Military Systems and the Advanced Cyber Threat. January (2013), 1–146.

[14] Hacked Cameras, DVRs Powered Today's Massive Internet Outage — Krebs on Security: 2016. *https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/*. Accessed: 2017-06-13.

[15] Harris, B. et al. 2013. Breaking the DDoS Attack Chain. *Institute for Software Research*. August (2013).

[16] Huang, Y. et al. 2007. Defeating DDoS attacks by fixing the incentive chain. *ACM Transactions on Internet Technology*. 7, 1 (2007), 5–es.

[17] ITU | 2015 Global ICT Development Index: *http://www.itu.int/net4/ITU-D/idi/2015/*. Accessed: 2017-06-13.

[18] Kanich, C. et al. 2011. Show Me the Money: Characterizing Spam-advertised Revenue. *Usenix Security*. (2011), 15.

[19] Khosrowpour, M. 2014. Cyber behavior: concepts, methodologies, tools, and applications. *Cyber behavior: concepts, methodologies, tools, and applications*. Hershey. 263.

[20] KrebsOnSecurity Hit With Record DDoS — Krebs on Security: 2016.

https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. Accessed: 2017-06-13.
[21] Kreing, T. and Modderkolk, H. 2017. Ongrijpbaar aan de Zwarte Zee. *De Volkskrant*.
[22] Mapping Mirai: A Botnet Case Study | MalwareTech: 2016. *https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html*. Accessed: 2017-06-13.
[23] Miller, C. 2010. Kim Jong-il and me: How to build a cyber army to attack the U.S. *DEF CON 18*. (2010).
[24] Mirai Botnet: The Rapid Evolution of DDoS Attacks | Radware Security: 2016. *https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/mirai-rapid-evolution/*. Accessed: 2017-06-13.
[25] Mirai Scanner: Are Your IoT Devices for Vulnerable? 2016. *https://www.incapsula.com/blog/mirai-scanner-unwitting-mirai-botnet-recruit.html*. Accessed: 2017-06-13.
[26] Most Malware Tied to "Pay-Per-Install" Market - MIT Technology Review: 2011.*https://www.technology review.com/s/424241/most-malware-tied-to-pay-per-install-market/*. Accessed: 2017-06-13.
[27] N.A 2007. Akamai's State of the Internet / Threat Advisory - ZeuS Crimeware kit. 9, 2 (2007), 1–20.
[28] Neville, A. and Gibb, R. 2013. ZeroAccess Indepth. *Symantec Security Response*. (2013), 40.
[29] Osterwalder, A. and Pigneur, Y. 2010. *Business Model Generation*.
[30] Overvest, B. and Straathof, B. 2015. What drives cybercrime? Empirical evidence from DDoS attacks. *CPB Netherlands Bureau for Economic Policy Analysis*. 7, 11 (2015), 956–963.
[31] Ponemon Insitute 2016. 2016 Cost of Cyber Crime Study; the Risk of Business Innovation. (2016).
[32] Ragebooter: "Legit" DDoS Service, or Fed Backdoor? — Krebs on Security: 2013. *https://krebsonsecurity.com/2013/05/ragebooter-legit-ddos-service-or-fed-backdoor/*. Accessed: 2017-06-13.
[33] Report: botnets sent over 80% of all June spam | Ars Technica: 2009.*https://arstechnica.com/security/ 2009/06/report-botnets-send-over-80-of-all-spam-in-june/*. Accessed: 2017-06-13.
[34] Report, A.D. and Partnership, I.N. 2011. the Cost of With the Office of Cyber. (2011), 1–8.
[35] Rodrıguez-Gómez, R. 2011. Analysis of Botnets Through Life-Cycle. *Ceres.Ugr.Es*. (2011), 257–262.
[36] Rose, K. et al. 2015. The internet of things: an overview. *Internet Society*. October (2015), 53.
[37] Ruvalcaba, C. and Langin, C. 2009. SANS Insitute InfoSec Reading Room - Web Based Attacks. *System*. 1 (2009), 19.
[38] SANOU, B. 2015. ICT Facts & Figures. The world in 2015. *Itu 150 Años (1865 - 2015)*. (2015), 6.
[39] Source Code for IoT Botnet "Mirai" Released — Krebs on Security: 2016. *https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/*. Accessed: 2017-06-13.
[40] Tens of Millions of IP Addresses Used to Take Down Twitter, Netflix in "Unprecedented" Cyberattack | KTLA: 2016. *http://ktla.com/2016/10/22/ unprecedented-cyberattack-involved-tens-of-millions-of-ip-addresses/*. Accessed: 2017-06-13.
[41] The Hunt for the Financial Industry's Most-Wanted Hacker - Bloomberg: 2015. *https://www.bloomberg.com/news/features/2015-06-18/the-hunt-for-the-financial-industry-s-most-wanted-hacker*. Accessed: 2017-06-13.
[42] The Morris Worm | Limn: *http://limn.it/the-morris-worm/?doing_wp_cron=1493212119.7306540012359 619140625*. Accessed: 2017-06-13.
[43] The Robert Morris Internet Worm: 1992. *http://groups.csail.mit.edu/mac/classes/6.805/articles/ morris-worm.html*. Accessed: 2017-06-13.
[44] Trojan.Zbot | Symantec: 2016. *https://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99*. Accessed: 2017-06-13.
[45] vDos Stresser Peak Power: 2014. *https://twitter.com /vDosStresser/status/519496081592156160*.
[46] What is command-and-control servers (C&C center)? - Definition from WhatIs.com: 2017. *http://whatis.techtarget.com/definition/command-and-control-server-CC-server*. Accessed: 2017-06-13.
[47] What is Malicious Code? | Definition | Kaspersky Lab US: *https://usa.kaspersky.com/resource-center /definitions/malicious-code*. Accessed: 2017-06-13.
[48] ZeuS Banking Trojan Report | SecureWorks: 2010. *https://www.secureworks.com/research/zeus*. Accessed: 2017-06-16.
[49] ZeuS Tracker :: Home: *https://zeustracker.abuse.ch/*. Accessed: 2017-06-13.
[50] Q1 2017 State of the Internet – Connectivity Executive Review | Akamai. 1–6.

APPENDIX 1 - BMC