Thesis no BCS-2016-10

Cybercriminal Organizations

Utilization of Botnets

Bastian Jacobsson

Faculty of Computing
Blekinge Institute of Technology
SE-371 79 Karlskrona Sweden

This thesis is submitted to the Faculty of Computing at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science. The thesis is equivalent to 10 weeks of full time studies.

Contact Information:
Author:
Bastian Jacobsson
E-mail:
Bastian.Jacobsson@gmail.com

University advisor:
Sara Eriksén
Department of Creative Technologies

Faculty of Computing
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

ABSTRACT

Botnets, networks of hundreds to millions of computers, controlled by one or more individuals, increasingly play a part in cybercrimes, with astonishing results. The access of a botnet gives the controller abilities of a large majority of all the cyberattacks over the internet, and with the possibility of buying a complete botnet, this opens the market to nontechnical criminals. The Darknet and the market it provides, enable the buyers to buy and trade everything from botnets and malware to complete schemes.

The increase in cybercriminal activities and organizations has been alarmingly high in recent years, and no wonder, when criminals just need to invest a small amount of money to gain potentially millions of dollars without any advance knowledge of computer science, and with only a slight chance of getting caught due to the anonymity of the internet and botnets.

Based on a literature review combined with a critically reflective analysis of a selection of information about botnets from other sources available on the internet, this paper has identified some of the main types of organizations used in cybercrime and their operations as well as basic information about botnets, the players and stakeholders in this area, the theft and schemes used by botnets and the online money laundering service involved.

Keywords: Botnets, Cybercriminal Organizations, Security, Money Laundering.

Table of Content

1 INTRODUCTION

1.1 Botnets

Botnets, networks of hundreds to millions of computers, controlled by one or few individuals, has been used for over fifteen years, but is still the most effective and profitable way to conduct criminal activates over the internet. The majority of all cybercrime organizations and groups uses the botnets as their base infrastructure of all their operations.

The threats of botnets capabilities and attacks has been increasing exponentially over the last ten years, where only a few people can organize massive large-scale attacks on multiple people and small-large corporations, with only a few clicks. The major threat is not only by the hugeness and widely usage of a botnet, but also how easy it is to build or buy a botnet for only a few hundred dollars as a budget. Due to the infrastructure of most botnets, which contains hundreds to millions of computers, controlled remotely from a secure location, the risk of creating or use one, is relative small, especially in terms of return profit of a successful operation (Wagen & Pieters, 2015).

1.2 Cybercriminals

The pursuit of financial gain has always been one of the main goals of organized criminal groups and due to the anonymity of the internet and the broad victim pool, cybercrime has become the most effective way to conduct illegal activities (Choo, 2008; Hoque, Bhattacharyya, & Kalita, 2015). Due to the increased usage in computers and internet connectivity, all parts of a cybercriminal operation can be conducted over the internet; the recruitment, gathering and communications of the participants, the criminal operation or heist and even the money laundering itself. This is some of the many reasons why this type of criminal activities is the next generation of crimes.

1.3 Organization Structures

Depending on what type of operation, scheme/theft and the user's skills, you can divide cybercriminal organizations into five types, Affiliated, Small, Medium, Large and Collective organizations. Those types can be associated with all of the operations performed by Botnets, but with some seen in a specific group (Martin & Rice, 2011).

1.4 Operations

Due to the variations of attacks done by a botnet, those attacks are the majority of all attacks performed over the internet. Operations such as bank fraud, scams and corporate espionage are very profitable and with a botnet in place, the owner can make hundreds of dollars per hour, pending what type, target and goal they have. Botnets which can collect credentials to bank services such as PayPal, which in turn can be used to sell money laundering services on the internet and the Darknet (Stoyanov, 2015).

1.5 Contribution

This paper will go through all parts of a cybercriminal organizations and the type of attacks possible with a botnet as an infrastructure and will give the readers an overview of the structures and the operations. Most papers focus on either the botnet aspect, cybercriminal organizations, online money laundry or the operations performed by botnets, however this paper will include all aspects on the necessary parts, components and organizations as well as the operation and tasks itself. This can give the readers a complete overview and understanding of this type of growing crimes and groups on the internet.

2 LITERATURE REVIEW & RELATED WORK

2.1 Botnets

A botnet definition is as follows (Fisher, n.d.): Botnet is the generic name given to any collection of compromised PCs controlled by an attacker remotely. Botnets generally are created by a specific attacker or a small group of attackers using one piece of malware to infect a large number of machines. The individual Personal Computers (PCs) that are part of a botnet often are called "bots" or "zombies" and there is no minimum size for a group of PCs to be called a botnet. Smaller botnet can be as few as in the hundreds or thousands of infected machines, while larger ones can run into millions of PCs(Drupal, 2008; Fisher, n.d.; Things, 21, 2008, & Pst, n.d.).

The owner of a botnet can use it for a wide variation of attacks and tactic to gain money or reputation such as; denial of service attacks, spamming, harvesting information from the infected PC, adware installations, hosting phishing sites and much more. Most botnets are the foundation of cybercriminals activities which gives them complete access to infected computers contents, internet bandwidth and the computers resources (Negash & Che, 2015).

The owner, master or the puppeteer of the botnet uses a Command and Control (often referred as C&C) server which sends command to which in turn sends commands through other smaller C&Cs or to all the bots or zombies in its command (Hoque et al., 2015).

2.2 Botnet attacks

There are many possible attacks and operations made from Botnets, most common are the following attacks (Hoque et al., 2015):

2.2.1 Sending Spam

With the help of a botnet, a massive amount of emails can be sent from multiple hosts with various contents to millions of emails, "some of the largest botnets in history were responsible for sending out literally billions of messages a day" (Stoyanov, 2015). Some bots can even harvest its hosts address books and start sending spam to those as well. Most of the emails contains advertisements or phishing attempts, see *Phishing* and *Spam*.

2.2.2 Stealing Credentials & Information

One of the most dangerous usage of botnets and the malware that makes the computer part of a botnet, is the possibility to steal and gather sensitive information from your computer. Depending of what the computer is used for, this type of attack can be devastating. If it used to pay bills, work with sensitive data and information for a company or just to play an online game, the user should really be careful of any kind of malware, viruses or any form of malicious software. Here are some ways infected computers can be targeted with:

2.2.2.1 Sniffing Traffic:

Bots or similar infected computers can have packet sniffers that can read clear-text data passing by the compromised machine or the network it is connected to. The sniffers are mostly used to retrieve sensitive data like usernames with passwords, communication or connections from the computer that can compromise new machines and networks.

2.2.2.2 Keylogging

If a compromised computer uses encrypted communications and feel secure and safe from that reason, should reconsider. Keylogger monitors and saves all the keystrokes before any encryption takes place, thereby all sensitive data and credentials will be in plain-text such as PayPal passwords or VPN/SSH connections to other networks. This is one of the most dangerous features from malicious software in general because there is almost no protection against it, except having an encrypting keyboard or to remove the software.

2.2.3 (Distributed) Denial of Service Attacks

"The intent of a DDoS attack is to direct so much traffic at a web server that it becomes overwhelmed and cannot respond to legitimate requests."(Stoyanov, 2015). Those attacks are not limited to web servers and can be used to overwhelm any kind of servers to deny access. This is the most difficult attack to protect against and is one of the most efficient types of cyberattack in history, see *Famous Botnets Through History*.

2.3 Spreading

There are two main methods of infection which can lead to your computer being part of a botnet, see *Fig. 1. Example of a Botnet overview.*

2.3.1 Drive-by Download

If a user enters a suspicious website or a legitimate website with malicious software, the computer can be infected just be entering the website or by downloading what should be a legitimate file. This file is often the original file but with added malicious code which either contain the code that will make the computer part of a botnet or just the part that enables a download of the real malicious payload.

2.3.2 Email

This is the most traditional and yet most efficient method of botnet infection. This method is by sending large amount of spam that often includes a file, such as PDF or Word with malicious code imbedded within, or the email contains a link that will redirect the user to a website containing infections code.

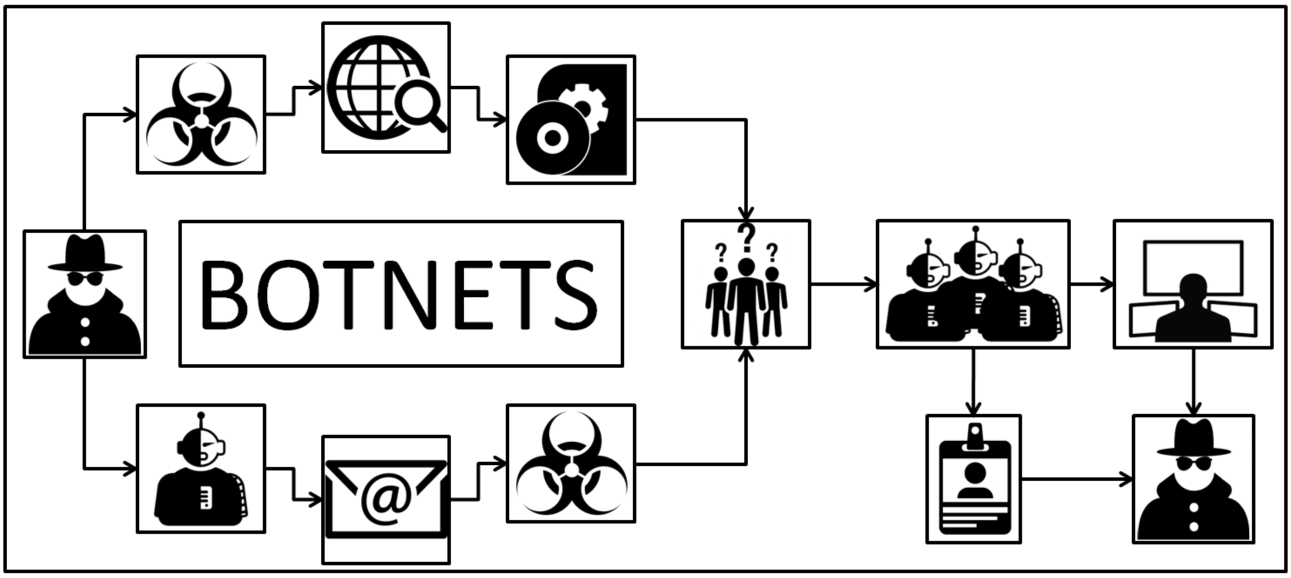

Fig. 1. Example of a Botnet overview.

Make note that after a computer has been infected there is a high risk of the malicious code to spread on to other computers in the same network.

2.4 Infection

After the first part of the infectious code has been downloaded, it begins installing itself and opening a backdoor to be able to start communicating and download the complete payload of the code enabling the bot to be controlled by the botnet master. After the bot is completely installed, it attempts to contact the C&C asking to be added to the fold, with this handshake it is often sending a complete package with information about the host such as IP address (gives a geographic location), computer name, operating system, etc. What comes next can vary from the bot hibernating and waiting for orders, start collecting credentials or receiving commands from the C&C (Fisher, n.d.; Stoyanov, 2015).

2.4.1 Infection Prevention

On "FBI"s blog that warns about botnets and what they can do, they stated following tips how to prevent your computer to be part of a botnet ("Botnets 101," n.d.):

- Make sure you have updated antivirus software on your computer.
- Enable automated patches for your operating system.
- Have strong passwords, and don't use the same one or two passwords for everything.
- Download free software only from sites you know and trust.
- Don't open e-mail attachments in unsolicited e-mails. Even if it comes from people in your contact list, and never click on a URL contained in an e-mail, even if you think it looks safe. Instead, close out the e-mail and go to the organization's website directly.

- Use antivirus software on your smartphone. Criminals are already stealing personally identifiable information from smartphones after owners unknowingly download malware, and it won't be long before we see the emergence of mobile botnets undertaking DDoS attacks and other criminal activities.

2.4.2 Signs of Infection

There are simple ways to determine if a computer is actively participating in a botnet, however, it is almost impossible to notice a dormant bot without anti malicious scans (Stoyanov, 2015).

- System isn't behaving normally, perhaps running slower than usual.
- The firewall or anti-virus software has been disabled.
- The CPU, hard drive or your network usage is used more than usual.
- Files or folders have changed or been removed.
- Messages has been sent without the user's knowledge.

2.5 Famous Botnets Through History

There are several famous successful botnets worth mentioning, Zeus with keylogging abilities, the spambot Lethic, Mariposa as a DDoS and scam bot and last ZeroAccess which mines Bitcoins ("Botnet," 2016), see below.

2.5.1 2007 – Zeus

One of the most financially lucrative bots in history. First discovered in 2007, Zeus was designed to secretly monitor a victim's PC and steal banking information. The FBI estimates that to date, the Zeus botnet may have stolen hundreds of millions of dollars. In 2010, it was reported the creator of Zeus was retired and gave the source code to the creator of the SpyEye botnet. In 2011, the source code to Zeus was leaked online, which has led to an explosion of Zeus variants. Because of this, Zeus infections and botnets continue to account for a large number of global botnet installations.

2.5.2 2008 - Lethic

At one time, Lethic was one of the most prolific spambots in existence. At its peak, the botnet had 300,000 computers under its control and was responsible for sending out tens of billions of messages per day, which accounted for a whopping eight to 10% of global spam. While the botnet was partially dismantled in January 2010 by Neustar, Inc., its owners were able to regain full control two months later. Lethic is still in business, and it's estimated that the botnet is now sending out about 2 billion messages daily.

2.5.3 2008 - Mariposa

Primarily used for cyber scams and DDoS attacks. In 2009, Spanish authorities were able to take the botnet down, which, at the time, was responsible for an estimated 12 million infections that were capable of generating at least 250,000 Euros a month in revenue for the owners.

2.5.4 2011 - ZeroAccess

Known to have infected between one and two million computers, and it is belived that the zombie network is still generating millions of dollar per year in bitcoin mining and click fraud, *see Adware Pay per-Click Service*.

2.6 Successful take downs of Botnets

Of all the major botnets, there have only been a few arrests and successful extermination of botnets in the history (“Botnet,” 2016), here are three worth mentioning:

2.6.1 2006 - Rustock:

First identified in 2006, the Rustock botnet was a major spam generator, capable of sending up to 20,000 spam emails per hour from a single infected PC. In 2011 Microsoft, in coordination with US Marshalls, FireEye, Pfizer, Dutch authorities and others were successful in shutting down the Rustock botnet, generally seen as the largest source of spam at the time. Microsoft was successful in quietly petitioning the courts in the US to pounce on Rustock's infrastructure before its owners had the chance to move its control servers elsewhere.

2.6.2 2009 - Bredolab:

This botnet was based out of Armenia and first identified in 2009. Dutch authorities were able to seize control over 140 servers related to the management and operation of the botnet. After the botnet was taken over, its new benevolent owners were able to redirect infected hosts to a webpage notifying them of the infection and how to remove it. An Armenian citizen was arrested by authorities, and the author was sentenced to 4 years in prison in 2012.

2.6.3 2009 - Bamital:

In existence since 2009, Bamital was used primarily for click fraud and disseminating additional malware such as fake antivirus. In February 2013, Microsoft, working with Symantec, using the same court actions they used against Rustock, raided two server facilities in the United States and shut the botnet down. Bamital, according to Microsoft's lawsuit, was a multi-million-dollar operation and infected hundreds of thousands of computers.

3 METHODOLOGY

3.1 Research Method

The literature reviews and research to provide information and knowledge to answer the research questions and to write this paper, has been done by several database searches regarding papers containing relevant information. However, due to the topic genre, most information older than a year after their research, could have been changed, been inconclusive or now incorrect. IT and especially in IT-Security is in a constant change where researches and anti-malicious companies are playing cat and mouse with the cybercriminals, and are always one step behind.

Due to this, most litterateurs, such as articles and published books, are therefore not enough to state the current situation. Therefor this paper has also focused on articles and blogs from legitimate sources. To legitimate a source that is somewhat questionable, the information was compared to other sources, legitimated or non-legitimated, and thereby confirmed the state and correctness of their content. This legitimization followed Harvard's "Evaluating Sources" guidelines ("Evaluating Sources § Harvard Guide to Using Sources," n.d.).

The databases used for literature searches were Google Scholar and Summon, with the search words such as: "Botnet", "Cybercriminals", "Money Laundering", "Organizations", etc. Most of the articles, blogs and other sources, was found by searches by the Google Search Engine and by references in relevant articles found. The same type of search words were used as in those searches in the database.

3.2 Research Questions

The research questions can be sorted into three main questions categories, that contains subquestions in regard to those questions that needs to be answered.

3.2.1 How does Botnets work?

- What can a botnet perform?
- What kind of attacks can be done with a botnet?
- How does the malicious code spread?
- Prevention methods?
- How to notice an infection?

3.2.2 What does a cybercriminal organization look like and how do they work?

- What types of organizations exist?
- What kinds of attacks do they perform?
- What type of employees?
- How do they sell their products and services?

3.2.3 How can you transfer illegal funds over the internet?

- How can they transfer illegally obtained money without having it seized?
- How do they avoid leaving a money trace which could lead to an arrest?

4 ANALYSIS & RESULTS

The analysis and result have been added together and divided into five categories in order to get the correct understanding of all the separate parts of a criminal organization.

4.1 The Darknet

Darknet is an internet beneath the internet which is used every day, cloaked from search engines and obvious domain names. Like a war zone, this is not a place most common people visit and in this case, even knows about. But for the knowing, such as hackers, criminals or people in search for illegal or embarrassing content, this is the place they would visit. The Darknet is like any other websites or forums on the internet, but where users will walk in a labyrinth instead of flying from A to B. When users type normally just type in where you want to go, the Darknet, or what some people call the Deep Web, only has references to other places, linked by the website or referred to by other people. Most part of the Darknet is not accessible for the "non-invited" where you will need a specific link, name or a way to connect.

There is no specific genre of people accessing the Darknet, but a majority of them have criminal intent or actions in mind. Cybercriminals, hackers and programmers, which this paper will focus on, is no different. Here they can sell their products, services or illegal content for a specific sum of money or to the highest bidder, as any other physical or black markets. Payments are generally made by Paypal, WebMoney, Bitcoins or other electronic payment systems, which can be close to anonymous.

Kaspersky's investigation in Russian-language cybercriminal market (Stoyanov, 2015), shows a list on some products and services made and sold on the Darknet:

4.1.1 Products

- Software designed to gain unauthorized access to a computer or a mobile device, in order to steal data from an infected device or money from a victim's account (the Trojans);
- Software designed to take advantage of vulnerabilities in software installed on a victim's computer (exploits);
- Databases of stolen credit card data and other valuable information;
- Internet traffic (a certain number of visits to a customer-selected site by users with a specific profile.

4.1.2 Services

- Spam distribution;
- Organization of DDoS Attacks;
- Testing malware for antivirus detection;
- Renting out dedicated servers;
- Renting out exploit packs;
- Renting out botnets.

Another service sold in the Darknet, is money laundering services. They provide cleaning of your illegally obtained money (often at a high price), see *Mules*.

4.2 Collective Organizations

There are many hacktivist and hacking collectives, but the most notable and recognized are Anonymous and will thereby be the collective organization mentioned henceforth. Newspapers and commentators have often refereed Anonymous as activists, hackers, vigilantes, etc. (Serracino-Inglott, 2013). But Anonymous describes themselves as an "internet gathering" rather than a group or an organization. They state that they have a very loose and decentralized command structure that operates on ideas rather than profit or directives. In August 2011, an Anonymous member gave out a press release regarding their deciding process:

"*With any given operation there are always some who agree and some who disagree... Anonymous allows each person to individually vote on each operation, a yes vote means they will participate, a no vote means they do not. Anyone is allowed to create an operation and if other votes yes it will get traction and something may be accomplished. If a member of Anonymous are interested in executing a cyberattack, they will, even if they consist of only a small fraction of the group's overall membership.".*

Prior to 2008, Anonymous would be defined as an unorganized group or as they choose to be recognized as, "an internet gathering", where members can work together or not, may participate or not, may agree with the majority of the groups philosophy and motivation or disagree.

But with the start of their "Project Chanology" against the Church of Scientology in January that year when more than 600 members of the group protested in the streets of over 18 cities worldwide from America, Europe and Australia the prior group definition of Anonymous was changed as well as their attacks which got more aggressive and without any provocations (Barkham, 2008; "Project Chanology," 2016).

Most notable was the project in 2011, when a Tunisian merchant's goods were seized without reason from the government which resulted in him setting himself on fire and got recorded by an unknown bystander. Anonymous then launched massive cyberattacks on Tunisian government websites and infrastructure, which helped to start the riot against President Zine El Abidine Ben Ali, the Tunisian president, who fled the country only a month after of the first attacks (Abouzeid, 2011).

Most of those organizations are anonymous it is difficult to understand their layout, since not even themselves knows everyone in such an open collective such as Anonymous. However, there are layers or ranks that can give a hint on how the organization such as this looks like. Make note that this is an example of a possible layout, also make note that a chain of command is not necessary, needed or wanted, but reputation, status and acknowledged deeds puts them in their category explained below and shown in *Fig. 2.*

Layer I consists of one or more leaders or people with the highest status. Those people are often known to most of the group and the people within and are those who start the most votes and collect tribute or acknowledgment from within the collective or from without. Those people are responsible for the collective's services such as communication and the dividends of group labor.

Layer II consist of people with various skills and areas, such as public relations, social engineering or economy as well as their skill in IT and computer science. Most of the public statements done by Anonymous has been done from this layer, with or without the layer I's approval. Those people are more noted due to their communications with a larger amount than the higher layer and are the ones being caught by law enforcement agencies and posted as "the leaderships of...", which often is not true since layer I is not often known to even those people or may not even have been in contact with them.

Layer III are the project or region "leaders", often in charge of a "mission" with a large yes votes from the collective. Those are often seen as mission or project leaders, which fills the same roles as project leaders in legal organizations. They rally their friends from the layers below due to geographical placement, knowledge or status, to perform their task.

Layer IV consist of people with computer skills or similar expertise. These group members are often sympathizers of the cause and may be known to other members and participate in specific missions, but are mostly working alone with common goals of the organizations or for reasons of their own.

Layer V are people that sympathize and agree with Anonymous goals and visions. Those people have often included themselves in the group and may not even know anyone from another layer within, but states to be a member. The major content of previous protests and public activities done by Anonymous members, has been from this layer with only a few others. Layer V have not done anything notable or acknowledged by a level higher up.

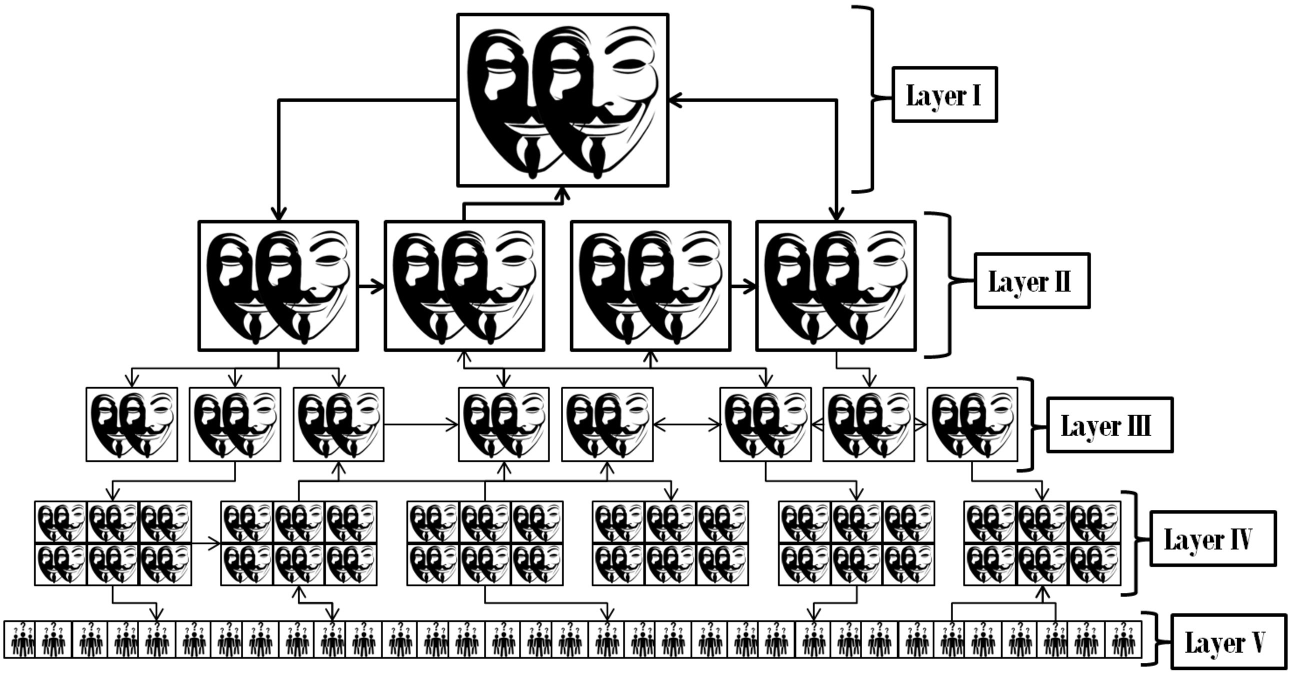

Fig. 2. Example overview of a Collective Organization

As you can see in the example in *Fig. 2*, communications between or within layers can be down sided, up sided or in a mutual relationship. Please note that member of a layer can have communications with another member that is higher or lower than one layer, but are often very rare considering that the relationship per say almost gives them status to get on a higher layer. Note that votes are often closed within a layer, or started by one layer and voted in one layer below, very few votes transcend over more or over all layers.

Due to the "loose" structure of an organization such as Anonymous, it is difficult to know if and how many of their member's deeds that are profitable and are indeed a group heist. If there are such actions, often a member or members of a higher rank, decide and organize the attack. Due to the sensitivity of criminal activities (mostly those with economical gain) these kinds of votes or plans are often done within a small group of members within the same layer, and are thereby those who become the operation leaders. Depending on the collective's knowledge and in what layer this attack is done, a tribute is often given to their contact with the layer above which often results in the leadership gets a cut, to provide the community and the services that requires to keep it going.

4.3 Business Organizations

There are two types of cybercriminal Business structures, which are medium and large organizations and two types of small operations, such as Affiliated and small size organizations, which can consist of one person or a few people. For the continued understanding of figures and overviews, a few icons will be introduced below. They will be described since they are necessary to understand the overviews correctly.

This icon represents malicious software/code, this code will enable the sender control of the targets system. This icon represents the first part of the code, which installs a backdoor as well as the botnet code which is downloaded as the second payload, see *Spreading*.

This icon represents the Command-and-Control authorization, which gives the person access and control of the botnet it commands, see *Infection*.

This icon represents a website, often part of the *Drive-by Download*, which spread and expand the botnet by having infected a file or a website that is being downloaded on false pretenses.

This icon represents the "email" infection method in the part *Email*. Where spam emails containing malicious code is being sent to a massive amount of email addresses in hopes that they will click on the attached file and become infected.

This icon represents a third party and can mean a contact or a contract has been made with another party, in this cases it is often websites or forums on the dark web, see *The Darknet, Products* or *Services*.

This icon represents an operation which enables the users to obtain money or valued information. The icon is marked red due to the variation of operation it can represent, see *Cybercriminal Operations* for more information.

This icon represents a mule operation which can contain one or more mules depending on what operation it is and is marked red due to the variation of mule operations it can represent, see *Mules*.

4.3.1 Affiliated Organizations

This type of organization is one of the easiest and least expensive methods of getting involved in cybercrime activities. The idea is that you buy all the necessary parts that you need to start a cybercrime activity, which are sold on the dark web by large cybercrime organizations, see *Large Sized Organization*. For an amount of money, you can buy botnets, malicious code or pay for an amount of email spam or per downloaded file which were infected, etc.

After "The guy" have payed and received the product, starts the operation and gains access to money or items of value. Then he contacts a Mule Service the same way he contacted the hacker to be able to start his operation, and buy their service. The Mule service often has a startup fee which is payed upfront and during the process they will take a cut of the money or items stolen, see *Mules*. Then they will send what's left of the money or the value of the items stolen, now as "cleaned".

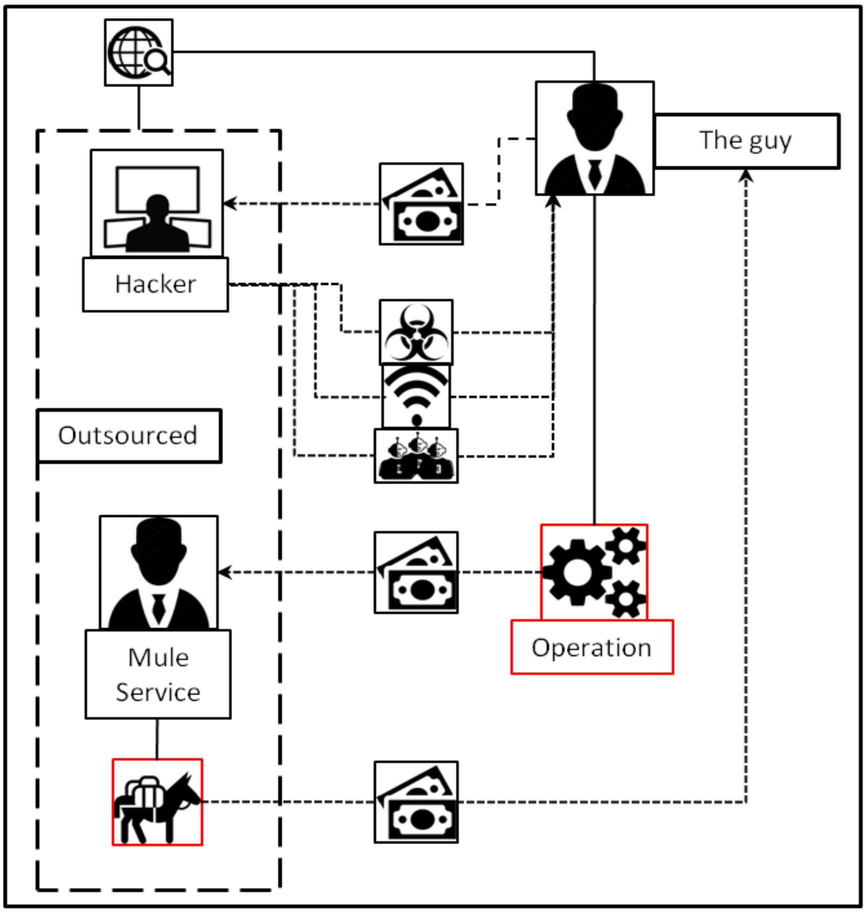

Fig. 3. An overview of an Affiliated Organization

4.3.2 Small Sized Organization

The differences between Affiliated organization and Small sized organizations are few, but have the essential difference skill wise, they are able to execute some parts without help, however the majority is still bought on the black market. This type of organization may contain up to five people and their skill in the area can variate from self-learned from published guides or as high as a degree in computer science, but their knowledge of hacking is of basic proportion.

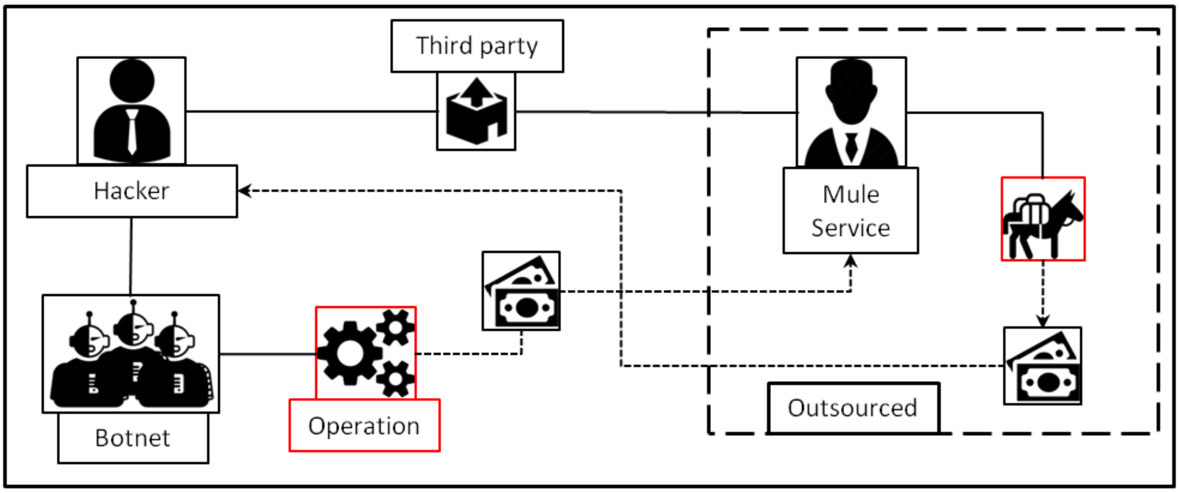

Fig. 4. An overview of a Small Sized Organization

4.3.3 Medium Sized Organization

What distinguishes this form of cybercriminal organizations from affiliated and small sized organizations is that they construct everything themselves, in need for their operation to be able to succeed. The leader or administrator is handling the workflow from the malicious programmer who creates all the necessary code to create zombies or to infect the targeted computer or system to be able to perform what they want them to do, to the distributor who specializes in spreading the code. Both the leader, malicious programmer and the distributor share the access to the infected computers, while the leader makes the final calls. After the operation is successfully initiated, they use their leader's connection to a third party mule service, which receives the assets stolen and by various means, tunnels and wash the money. Then they take a cut of the money and transfer the rest of the money to the leader, which in turn pays his subordinates which often are a percentage of the money obtained.

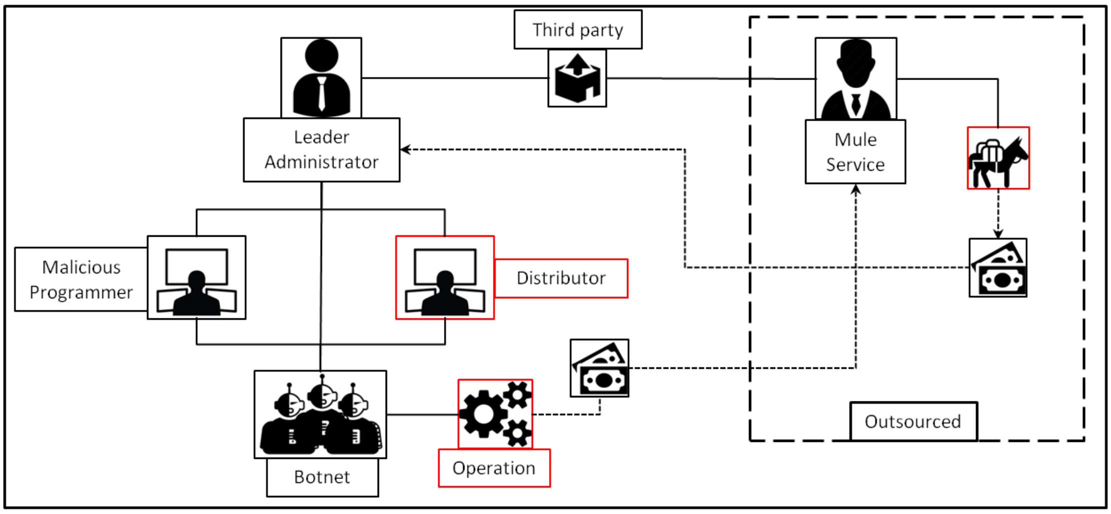

Fig. 5. An overview of a Medium Sized Organization

4.3.4 Large Sized Organization

The large sized businesses targets are very different from the other organizations. They target banks, small and medium-sized companies or engage in large scale frauds. To a certain extent, the structure reflects on an ordinary, medium-sized computer company (Stoyanov, 2015).

The Administrator performs almost identical tasks as in a legitimate business, they maintain the IT infrastructure and maintain the working condition. They buy equipment such as servers and ensure tools for anonymity such as VPN tunnels. They also have the role as a project leader for the Programmers and Malicious programmers.

Malicious Programmer are responsible for the creation of malicious code which allows them to gain a foothold in corporate networks. They work towards more efficient and stealthier code and are always adding new repacking of the code to make it harder for security systems to notice them.

The Programmers responsibilities are the Command-and-control systems (C&C) and the communication between the C&C and the infected computers under its control. The programmers can also work as testers for all the new code and upgrades to the botnet and malicious code created by the other programmers and if needed work with web design for the distributors.

The Distributors goal is to make sure the downloads and the increase of infected computers. They work with the Leader who gives them specific profiles on what targets they want to infect. The distributors can also consist of hackers that can target specific systems to place the code and infect. Those hackers are often paid on a fee-for-service basis and does not need to be part of the team.

The Money Flow Manager (MFM) takes position when all preparations of the tasks are done and the team is ready for the theft. The MFM are the one who withdraws money or valued information from the compromised computers and often have a thorough understanding of the targets proceedings and internal rules. The stolen goods are then sent to their mules account with cooperation from the Mule manager, see *Mule Manager below*. The Money Flow Manager is one of the few roles in this type of organization that often receive a percentage of the obtained money, rather than a fixed salary as all other receive.

Mule Manager is the organizations representative and works closely with the people involved in the process of stealing the goods. The Mule Manager has built their own infrastructure of mules to optimize the success rate of the laundering. It is assumed that around half of the value stolen is divided between the people in this branch, due to the higher risk of getting caught.

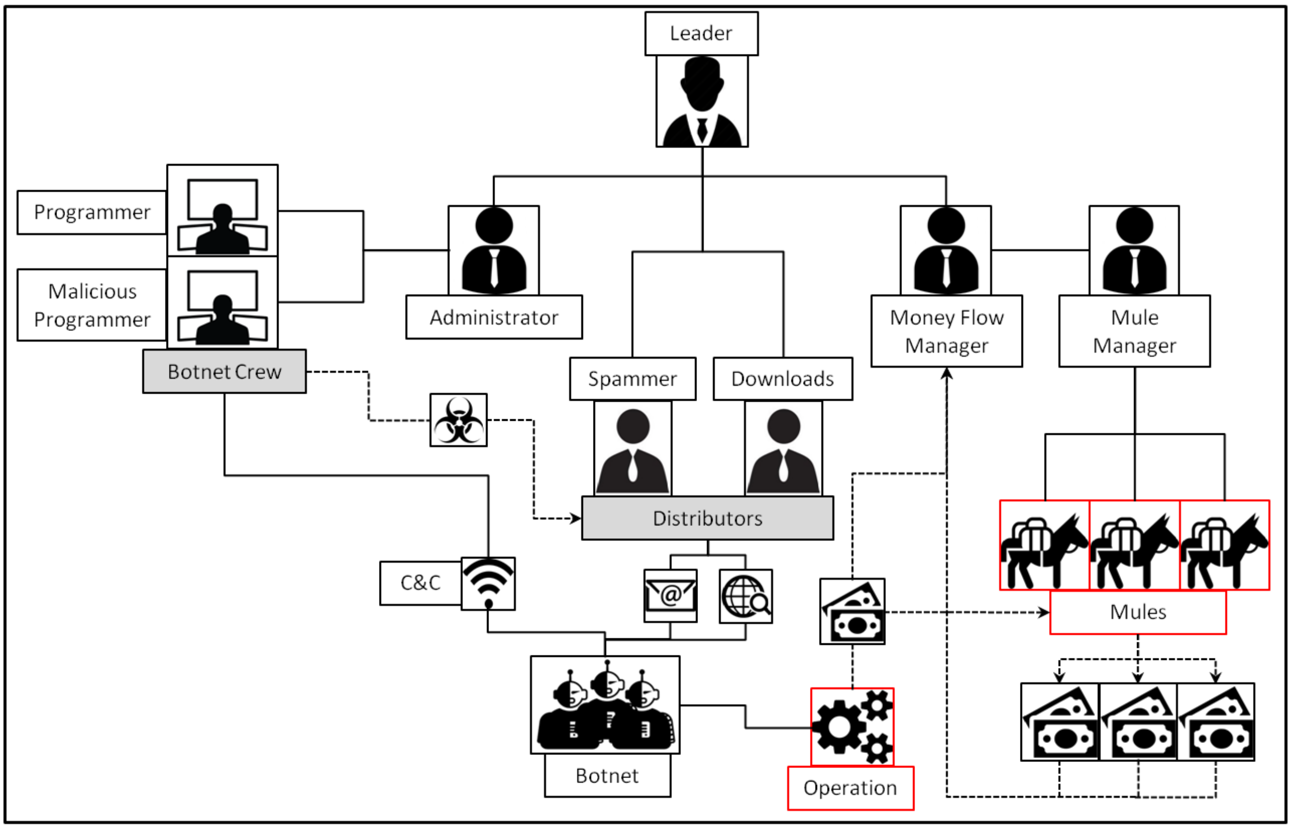

Fig. 6. An overview of a Large Organization

4.4 Cybercriminal Operations

There are a lot of operations, hacks or plans to extract valuable information or to steal money from people as well as organizations. Hereby follows some examples on some operations, but due to the illegality of those operations, most of the recent or operations used today, are unknown. Therefore, those examples will be a general explanation rather than detailed.

Please note that every operation is using a specific botnet type or function, which is made for the specific operation. However, a botnet can have more than one or all the functions necessary for some or all operations stated below, question is how the owner is utilizing it.

4.4.1 Bank fraud or theft

This type of operation uses the botnet keylogging ability and are often used by medium to large-sized criminal organizations. The target can be a specific bank or company, but thanks to the wide spread targets of most botnets, they can choose an infected target in relation to an organization relevant to this operation. It can start with an infected employees home computer, who uses the same password from personal use as work or have remote access to the company network. From there they penetrate and gain a foothold in the network, infecting relevant computers belonging to employees with access to money or bank accounts. After gaining all the access they need, the organization plans the next stage of the attack, the theft itself. When all parts needed for the heist, they start transferring, as an example the money to their account or the account created or owned by the money laundering department or service.

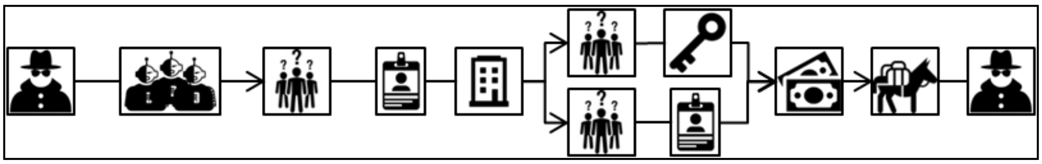

Fig. 7. An overview of a Bank Fraud operation.

4.4.2 Information theft

4.4.2.1 Holding information for ransom

Some malicious software start searching for important files after infecting a computer such as Word or PDF documents. Those files are secretly encrypted with a key only known to the owner of the malware, those file content cannot be read or understood without the key. The malware notifies the user that the files has been encrypted and cannot be used unless they pay a fee and receive the key. If the user tries to scan and remove the software, they will never be able to get that information back. The solution is to send the money to the criminal’s account which in turn be gives the key. Most of the time, this business is legit and the key is sent, in some few cases, they never send or don't even have a key and have just scrambled the data in those files, never to be recovered, an example of this kind malware is the CryptoLocker which appeared in 2013. CryptoLocker infected documents as well as photos revealed that over forty percent of the victims payed the fee (“CryptoLocker,” 2016).

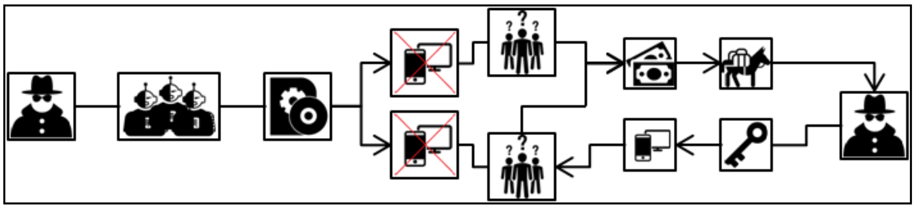

Fig. 8. An overview of a Ransom operation.

4.4.2.2 Corporate espionage

This operation can also be sold as a service from cybercriminals to large businesses that can gain economical or technological knowledge by the information from their competitors. Just like in *Bank fraud or theft*, they for example can gain access to an employee's personal computer with a remote connection to their work, which in turn give them a foothold and access to the company's network and servers. They search and extract valued information for that company or a competitive company, either to be sold or to blackmail the company.

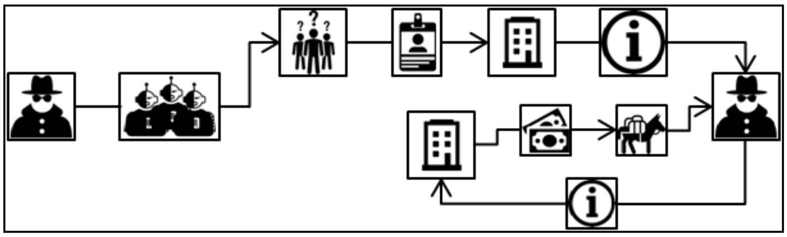

Fig. 9. An overview of a Corporate Espionage operation.

4.4.2.3 Phishing

Phishing attacks are the most common way to use spam, where they try to trick the receiver into doing something they want. It can be a money laundering scam or a fake email from the users bank, where they are required to submit their credentials. This operation does not have a high success rate, but thanks to large botnets, they can send millions of emails and with a success rate on for example, 1%, they will still receive a high amount of valued information.

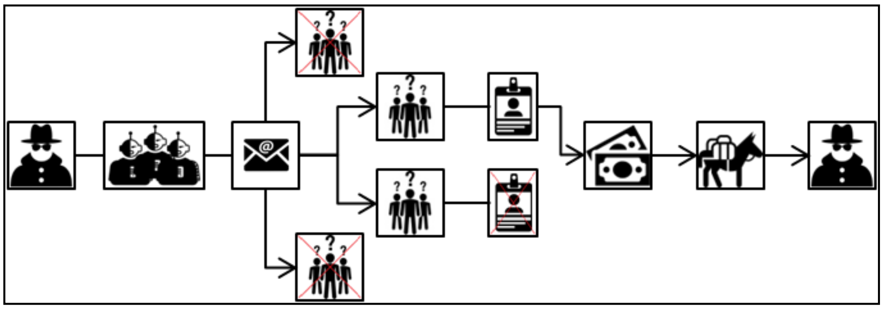

Fig. 10. An overview of a Phishing operation.

4.4.3 Computer Utilization

4.4.3.1 Distributed Denial of Service Attack

This is one of the most used, notorious and destructive operations done by a botnet. This can be done for economical gain, reputation or personal grudge. They use their botnets broadband to send enormous traffic from the botnet computers to overflow the target servers and by that deny the legit requests or put the servers offline. If the purpose is economical gain, a message is often sent to the company with a ransom fee to stop the attacks. Commercial companies often losses a large amount of money not being able to sell or have their services online. Such fees can be around $10.000-50.000, which is often payed due to the losses that can be over millions per day.

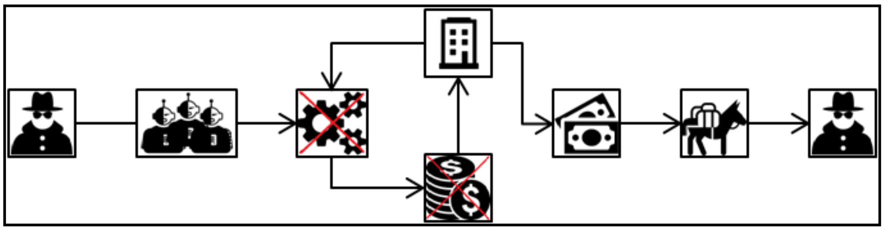

Fig. 11. An overview of Distributed Denial of Service Attack operation

4.4.3.2 Bitcoin Mining

This type of operation is very unusual and only a few botnets have utilized this in history, for example *2011 - ZeroAccess*. This generates low money per computer, but are a very safe way to use a botnet. The malware waits for the owner of the computer to be inactive and then starts to process calculations, which bitcoin mining is based upon, and stops using the computer when the owner is back. With a large amount of bots, this can give the best earnings/risk of all operations, since the computer owners have a hard time noticing they are infected and due to the fact that bitcoin mining and bitcoins are based on anonymity.

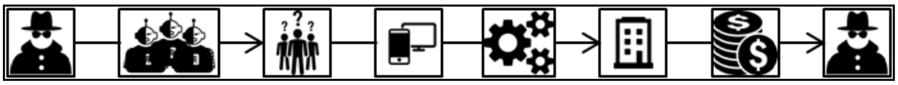

Fig. 12. An overview of Bitcoin mining operation.

4.4.4 Service Sale

4.4.4.1 Adware Pay-per-Click Service

This service is mostly used on Google AdSense, which are advertisements on websites or commercials such as YouTube. Cybercriminals use their botnet to watch and click those ads showed on the buyer's website, which gives the buyer of this service an amount from Google for the "impressions". This may generate only a few hundreds of dollars depending on the amount and value of the adverts, but often generates more attraction from legit viewers, which in turn can give them a higher viewership on their account or website.

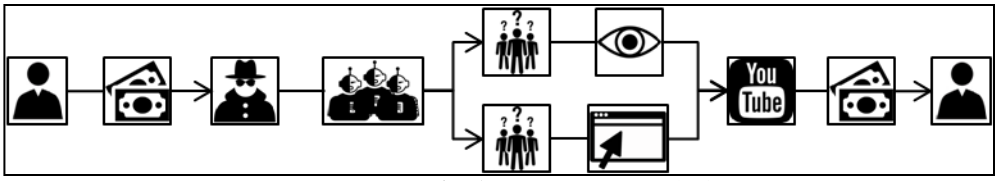

Fig. 13. An overview of Adware Pay-per-Click operation

4.4.4.2 Spam Service

This operation is almost the same as *Phishing*, when they send out a massive amount of emails with some kind of scam or phishing attempt that will fool the reader into revealing useful information. This service is sold by the botnet owners on the Darknet for a period of time or a specific amount of emails sent. Even if the ratio can be as low as 1:500000 emails per successful scam and the scam gives them one dollar, it is a big return of money considering botnets such as *2008 - Lethic* sent out billions of emails per day.

The hiring cost is around $100 per hour for a small to medium sized botnet that can send out hundreds millions of emails per hour, the return of hiring such a botnet could be as high as $200-500 per hour. In this case valued information such as credit card information or PayPal credentials is highly valued and profitable on the black market (Décary-Hétu & Dupont, 2012).

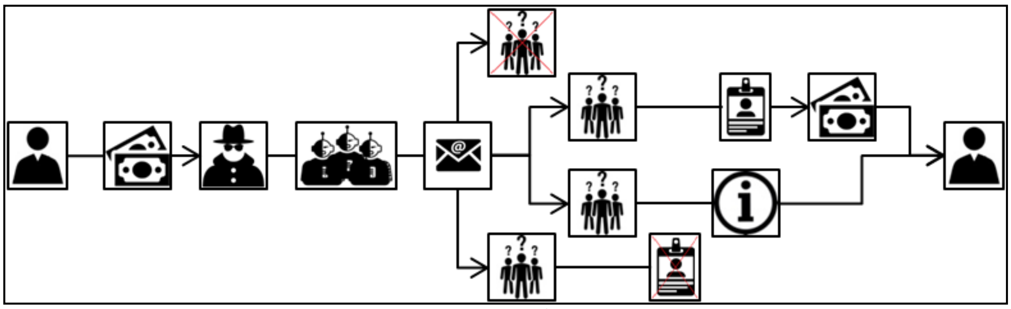

Fig. 14. An overview of Spam operation.

4.4.4.3 DDoS Attacks Service

This service provides a shutdown or latency spike of websites, online games or services on the target of the buyers choosing. In some cases, this service is bought for the buyer's competition that will help their business, but in many cases, the reasons are grudges or paybacks for the buyers. This service is known to be sold by one of the largest collectives, LulzSec, who often target online games such as Heroes of Newerth or League of Legends, and can be used on targeted game servers to make a game round invalid due to high latency.

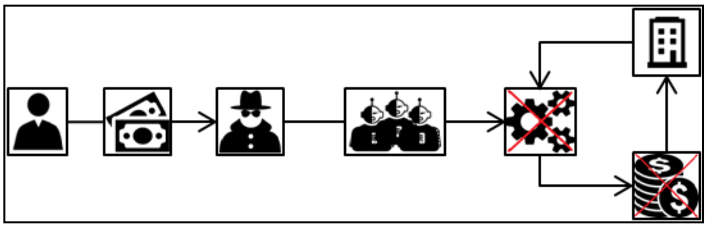

Fig. 15. An overview of DDoS Attacks operation.

4.4.4.4 Hosting Illegal Websites

The Darknet is a perfect place to sell illegal products and services anonymously, however, due to the difficulty and low audience, sellers for illegal goods that need a higher volume of visitors and buyers, this is the service for them. Botnet owners can sell an upkeep of an illegal website for a period of time by having one of the bots hosting it for a short period of time before letting another bot host it, to make it nearly impossible for authorities to shut the sellers down.

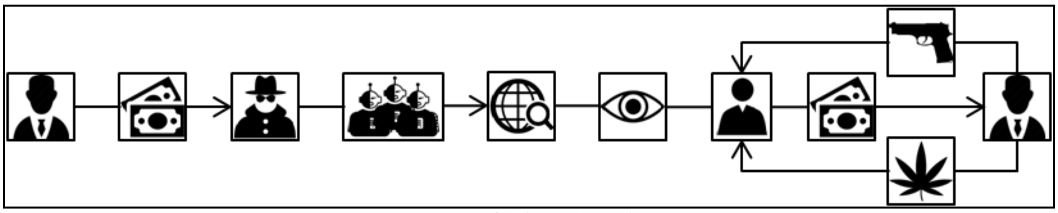

Fig. 16. An overview of Illegal Website Hosting.

4.4.4.5 Renting out or selling botnets

This service is often sold by small to medium sized organizations, which consists of one or more programmers of malicious software. They create a specific malware for every customer or for every botnet to rent out and create a unique C&C for every sold or leased botnet. The botnet is created for many different operations, or sold depending on the type. The renting period can be for hours to days while the sold botnet often has a duration of some weeks depending on the anti-malicious companies response. The code is not very often very sophisticated in comparison to ordinary botnets and is often based on the same code with slight differences for each botnet.

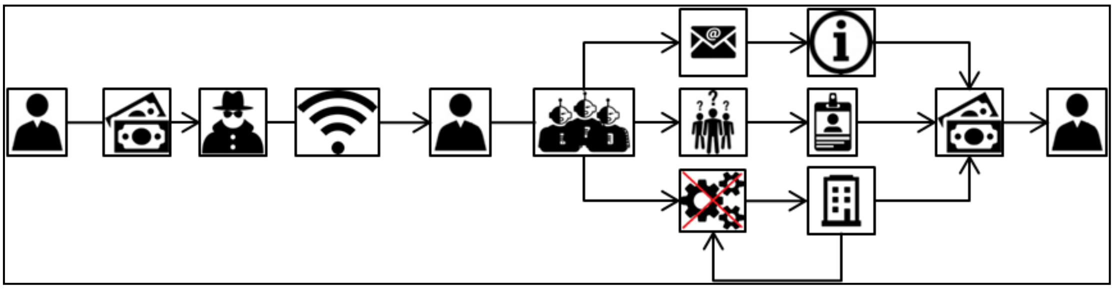

Fig. 17. An overview of selling a botnet operation.

4.4.4.6 Manipulating Online Polls/Games

This operation is one of the least used, due to the low and advanced economical gain. Companies can pay for this service to manipulate or give false results on surveys or polls done by other companies or governments. The reasons can be for economical gain because competitors get the wrong results and information and can lose money, but often this service is used in online voting which change the results to the buyer's advantage.

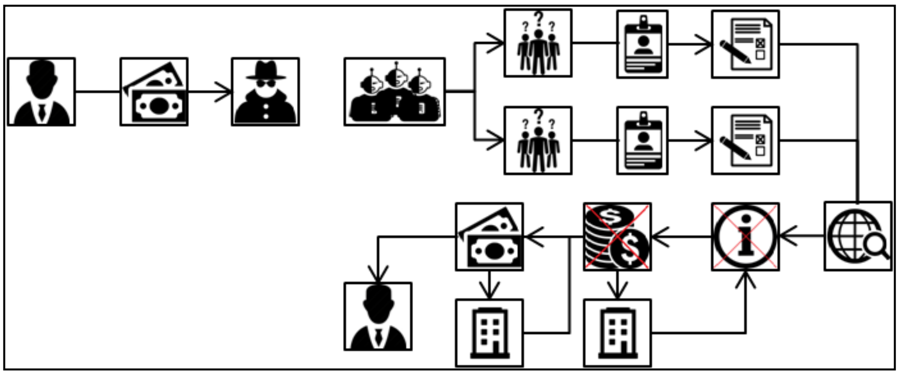

Fig. 18. An overview of Manipulating Online polls operation.

4.5 Mules

"If it sounds too good to be true, it probably is!"

4.5.1 Duped Mules

Duped mules, the people who are (at the start at least) unaware of the scheme or that they have become mules. There are many types of schemes to create duped mules, (Richet, 2013) see some examples below:

4.5.1.1 Work-From-Home Schemes (WFH):

WFH schemes are fake jobs that are offered in various forms, such as: Email spam, Job Search Sites, Social Network sites. At the start of the employment they are required to submit their banking credentials "for the purpose of receiving the payment or as part of the job". Their task will often be to receive money or checks that they will need to accept to their bank account, then after they take a cut, relocates the money to another account given by the company. Those schemes can easily be spotted by the job ad, if the company is located in another country, they offer significant earnings for little effort, the job involved transferring goods or money.

4.5.1.2 Email Spam:

In comparison to more normal email scams and fraud, these kinds of emails try to make the receiver a mole, but this spam will give them a profit. Mule frauds from emails will often require the same thing as WFH Schemes, such as receiving money and being asked to transfer and relocate the money. Those kind of mules often fall prey to normal email scams, such as:

- **Romance Mules**, when the person they have been online dating for a while asks them to receive money or send money due to reasons such as "they claim to be military personnel stationed overseas who need assistance accessing their funds due to being in a war zone" or some kind of issue with foreign bank account transactions.
- **Lottery and inheritance Mules**, who falls prey to a lottery or inheritance scam were they either won money or inherit money but need to transfer a small sum of money for the transaction fee they will have before sending the money. Those scams can be used to create mules with a portion of the money they are promised actually being transferred which in turn, will make the person more willing to pay a larger fee.

4.5.2 Non Duped Mules

Non Duped mules are trickier but have a better success rate and a larger amount of cleaning capabilities. The most common mules of this kind, are people with access to foreign accounts or a number of accounts on internet banks, such as Liberty Reserve, Paypal or MoneyGram (myiq2xu, 2008; Richet, 2013). They use those accounts to transfer illegally obtained money from one account to another anonymously to be later be sent to the real receiver after taking a cut or a payment from the criminals.

In the world of cybercriminals, such accounts are easily obtained and used for such money laundering which has a low chance of getting caught due to the amounts and variations of people and their geographical locations. It has been known for criminals to use other more conventional methods of laundering money such as the Gallery Scam (myiq2xu, 2008): *"Open an art gallery, and hang up a bunch of homemade art with high prices on it. Anonymous buyers come in and purchase the art with cash…"* or by other methods, and can thereby be reported, taxed and thereby become clean.

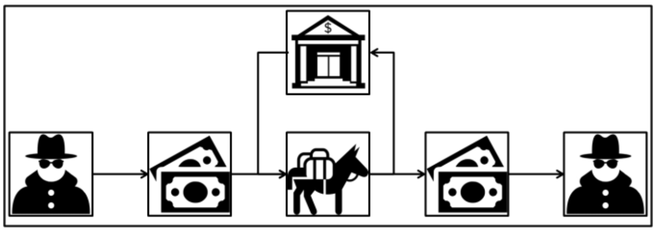

Fig. 19. An overview of a Mule operation.

5 FUTURE WORK

5.1 Further Investigations & Reports

Due to the constant change in IT-Security and related threats which are often based on flaws in the security shield guarding computers and systems, this topic is always in need of further investigations and research.

5.1.1 Cybercriminal Organizations

To secure and minimize the risk of cybercriminals success rate, infiltration in successful hacking organization is the quickest way to secure and safeguard against new threats. Cybercriminals has had a high rate of success in infiltrating systems and computers which has led to this explosion in cybercriminality. Investigation is not only needed to notice flaws, security breaches and holes, but also to get a better understating on those organizations as well. Kaspersky and other companies in the security business, have been working hard to infiltrate such organizations which this paper is based upon, but either the full extent of the information is not shared or just not obtained in the volume which is needed to make a turning point against those criminals (Stoyanov, 2015).

5.1.2 Botnets

Botnets and the general infrastructure it creates, is not an unknown or undocumented topic, however most malware contains the same base code as many known botnets use, but slight changes in the infiltration and spreading procedure makes it hard to secure against it. A more sophisticated tool against the usage of botnets and related malware is needed. Anti-malware tools are often based on signatures of code and are therefore in need of a signature to notice the code as a threat.

5.1.3 Mules & Money laundering

Most countries are in an agreement and have cooperation to prevent money laundering over borders, this type of laws applies only if both countries are in cooperation with those laws that receives or transfers the money. Websites such as PayPal or MoneyGram have cooperation with those countries, mostly because they have no choice to be able to operate in that country, but as long as some countries is not in agreement, transfers across those countries makes it hard to prevent the transfer. Most of the transfers need to be identified with criminal intent for PayPal or MoneyGram to stop the transfer before it happens. Since the usage of botnets gives the criminal credentials to such web based banks and transfer services, the criminals doesn’t care if that account is getting banned or frozen after the transfer has been made. They are not in need of that account anymore and can just use another one.

6 CONCLUSION

6.1 Botnets

This paper starts with the most basic information about botnets, *how they spread*, how to notice an *infection* and some examples of *successful botnets*. This gives the knowledge to understand the botnet as the base infrastructure of cybercriminal activities, it can perform the most common and effective *operations*, and with the widely spread usage such as *keylogging* and *Distributed Denial of Service attacks*, botnets can be part of, and used in a majority of all cyberattacks.

Thanks to the *Darknet*, everyone can buy botnet and related services and software, and due to the simplicity of the usage of botnets, this type of malware is the most dangerous and the most used one. The increase usage and the number of botnets has been growing over the years and are getting more attention than ever before.

6.2 Organizations

This paper has introduced five types of *cybercriminal organizations*, which are, with some variations, the majority of the structures used based on their knowledge, contacts, targets and goals. Due to the illegal genre, it is hard to know what kind of structures are the most common and effective ones, however the larger and more specific knowledge base of the group, the more money and information is stolen. For the understanding of this paper, those five categorized groups have not specified the member's goals and operations. The structure and members vary a lot, the majority of the structures mentioned in this paper are correct.

6.3 Operations

This paper has mentioned the most common and effective *operations* possible with the usage of botnets, however for the simplicity and understanding for the readers, non-specific attacks and operations in those *categories* has been mentioned. All operations may vary due to the specific target and goals with the operation, but the majority of the operations stakeholders and related tasks, are correct.

6.4 Summarization

This paper can help the readers to understand the structure of organizations and structures used by cybercriminals and can be used to get a clear picture of an existing or nonexistent criminal organization. By choosing an *operation* and placing it in an overview of an *organization* type, the readers can get an understanding of all the tasks and stakeholders, see examples *Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6.*

6.4.1 Affiliated Organization with Ransom Operation

The *Affiliated Organizations* with a single or few members without any related knowledge, hiring a Botnet to perform a *Holding information for ransom* operation.

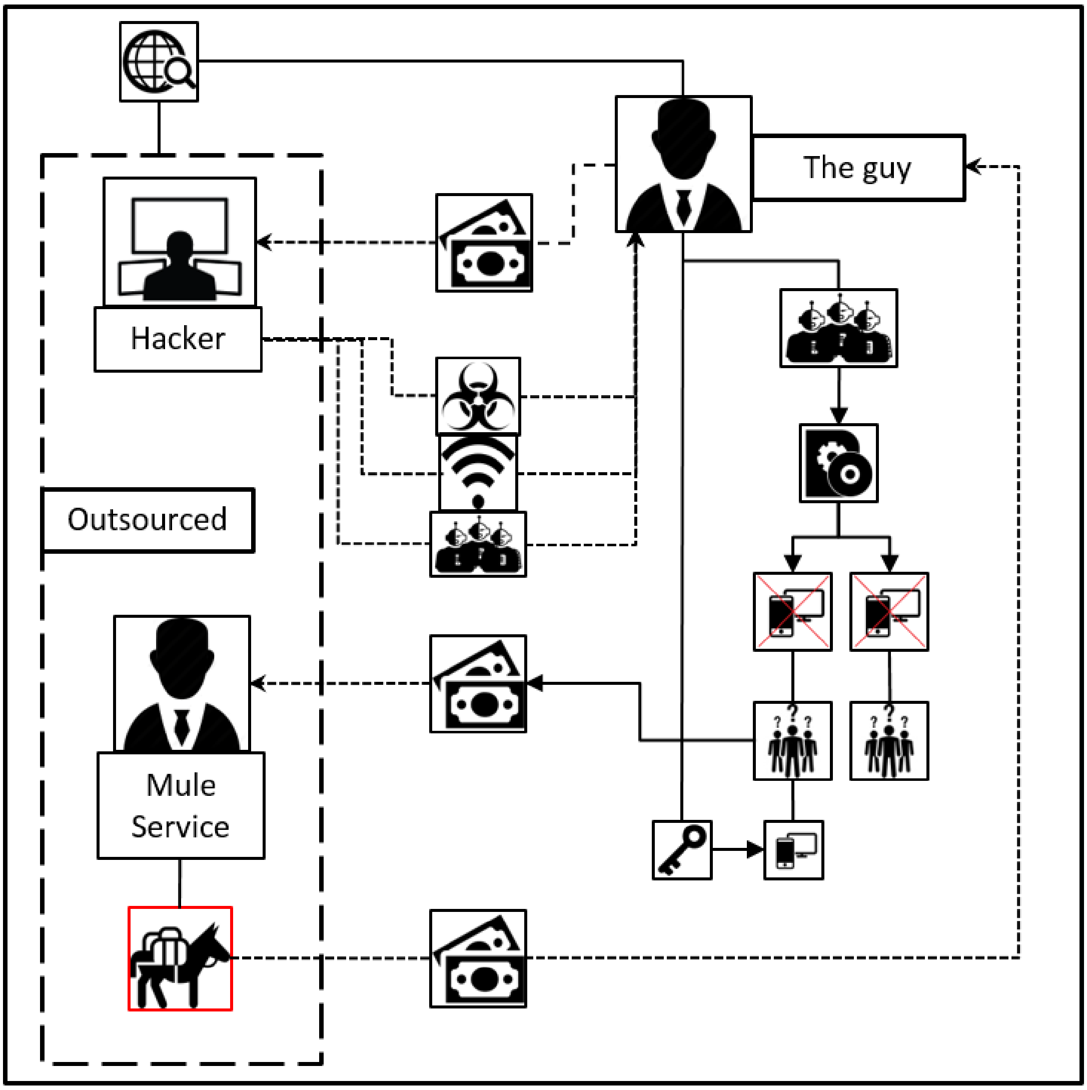

Fig. 20. A summarization of an Affiliated Organization type with a Ransom Operation.

6.4.2 Small Sized Organization with Bank Fraud Operation

The *Small Sized Organization* with a single or few members with some knowledge and their own Botnet performing a *Bank fraud or theft* operation.

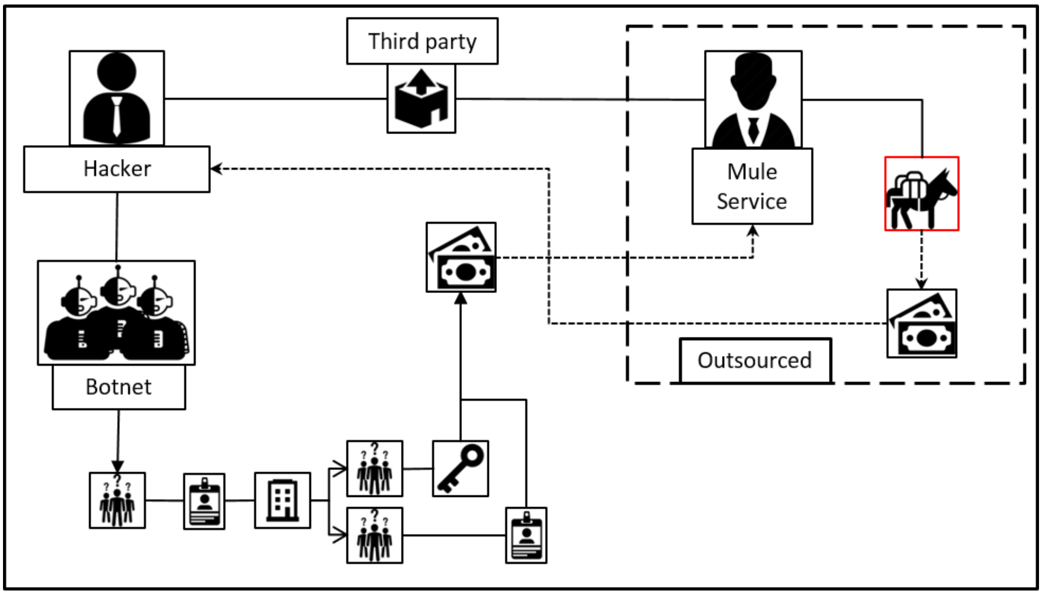

Fig. 21. A summarization of a Small Sized Organization type with a Bank Fraud Operation.

6.4.3 Medium Sized Organization with Bitcoin Mining Operation

The *Medium Sized Organization* with member with divided knowledge and tasks, performing a *Bitcoin Mining* operation.

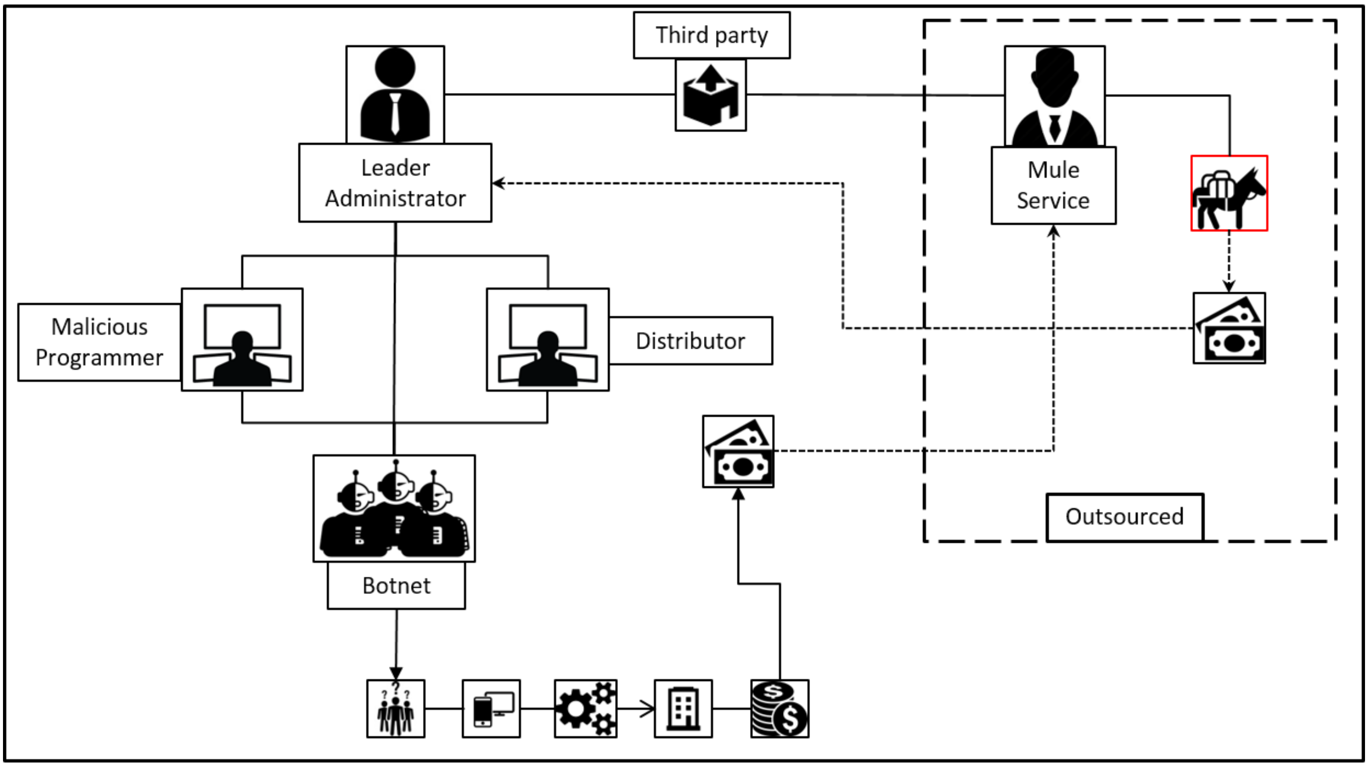

Fig. 22. A summarization of a Medium Sized Operation type with a Bitcoin Mining Operation.

6.4.4 Large Sized Organization with Corporate Espionage Operation

The *Large Sized Organization* with members with many divided knowledge and divided tasks, performing a *Corporate espionage* operation.

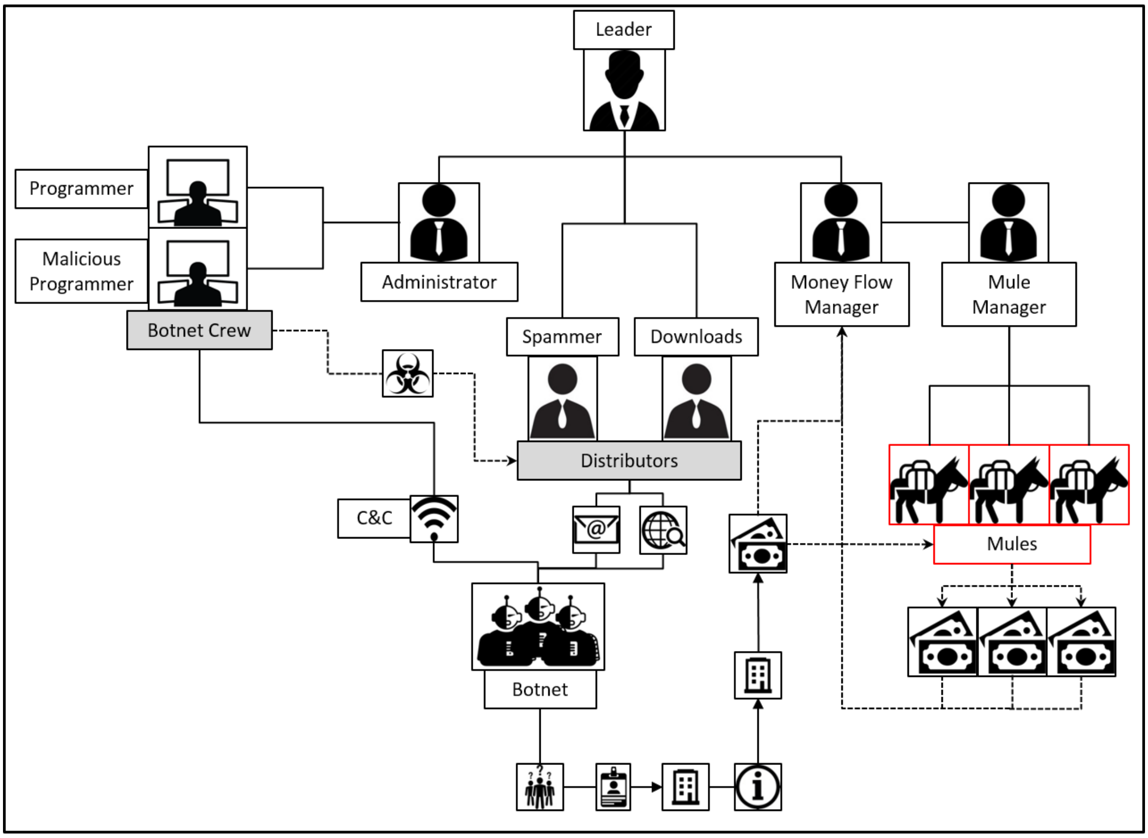

Fig. 23. A summarization of a Large Sized Organization type with a Corporate Espionage Operation.

REFERENCES

Abouzeid, R. (2011, January 21). Bouazizi: The Man Who Set Himself and Tunisia on Fire. *Time*. Retrieved from http://content.time.com/time/magazine/article/0,9171,2044723,00.html

Barkham, P. (2008, February 4). Hackers declare war on Scientologists amid claims of heavy-handed Cruise control. Retrieved May 12, 2016, from http://www.theguardian.com/technology/2008/feb/04/news

Botnet. (2016, May 1). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Botnet&oldid=718158082

Botnets 101: What They Are and How to Avoid Them. (n.d.). Retrieved May 8, 2016, from https://www.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them

Choo, K.-K. R. (2008). Organised crime groups in cyberspace: a typology. *Trends in Organized Crime*, *11*(3), 270–295. http://doi.org/10.1007/s12117-008-9038-9

CryptoLocker. (2016, April 6). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=CryptoLocker&oldid=713805864

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160–175. http://doi.org/10.1080/17440572.2012.702523

Drupal. (2008, August 10). Uses of botnets | The Honeynet Project. Retrieved May 8, 2016, from https://www.honeynet.org/node/52

Evaluating Sources § Harvard Guide to Using Sources. (n.d.). Retrieved May 12, 2016, from http://isites.harvard.edu/icb/icb.do?keyword=k70847&tabgroupid=icb.tabgroup107786

Fisher, D. (n.d.). What is a Botnet? -Kaspersky Daily. Retrieved May 8, 2016, from https://blog.kaspersky.com/botnet/1742/

Hoque, N., Bhattacharyya, D. K., & Kalita, J. K. (2015). Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys Tutorials*, *17*(4), 2242–2270. http://doi.org/10.1109/COMST.2015.2457491

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, *30*(8), 803–814. http://doi.org/10.1016/j.cose.2011.07.003

myiq2xu. (2008, May 23). How to Launder Money 101. Retrieved May 8, 2016, from http://www.correntewire.com/how_to_launder_money_101

Negash, N., & Che, X. (2015). An Overview of Modern Botnets. *Information Security Journal: A Global Perspective*, *24*(4–6), 127–132. http://doi.org/10.1080/19393555.2015.1075629

Project Chanology. (2016, April 25). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Project_Chanology&oldid=716978163

Richet, J.-L. (2013). Laundering Money Online: a review of cybercriminals methods. *arXiv:1310.2368 [Cs]*. Retrieved from http://arxiv.org/abs/1310.2368

Serracino-Inglott, P. (2013). Is it OK to be an Anonymous? *Ethics & Global Politics*, *6*(4). http://doi.org/10.3402/egp.v6i4.22527

Stoyanov, R. (2015, November 19). Russian financial cybercrime: how it works - Securelist. Retrieved May 8, 2016, from https://securelist.com/analysis/publications/72782/russian-financial-cybercrime-how-it-works/

Things, M. K. | in 10, 21, N., 2008, & Pst, 5:08 Am. (n.d.). 10 answers to your questions about botnets. Retrieved May 8, 2016, from http://www.techrepublic.com/blog/10-things/10-answers-to-your-questions-about-botnets/

Wagen, W. van der, & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *British Journal of Criminology*, *55*(3), 578–595. http://doi.org/10.1093/bjc/azv009