# Analysis and detection of a Botnet

*Thesis submitted in partial fulfillment of the requirements for the award of degree of*

**Master of Engineering**

In

**Information Security**

*Submitted By*

**Navdeep Kaur**

**(Roll No. 801433017)**

Under the supervision of:

**Dr. Maninder Singh**

Associate Professor

Thapar University, Patiala

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

**June 2016**

## Certificate

I hereby certify that the work which is being presented in the thesis entitled, "*Analysis and Detection of a Botnet*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security/ Computer Science and Engineering* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Maninder Singh* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Navdeep Kaur
(Navdeep Kaur)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Maninder Singh)
Associate Professor, CSED

**Countersigned by**

**(Dr. Maninder Singh)**
Head
Computer Science and Engineering Department
Thapar University
Patiala

**(Dr. S. S. Bhatia)**
Dean (Academic Affairs)
Thapar University
Patiala

# Acknowledgement

First of all I would like to thank the Almighty, who has always guided me to work on the right path of the life. It is a great privilege to express my gratitude and admiration towards my respected supervisor **Dr. Maninder Singh,** Head and Associate Professor of Computer Science & Engineering Department. He has been an esteemed guide and great support behind achieving this task. This work would not have been possible without the encouragement and able guidance of him. I also thank my supervisor for his time, patience, discussions and valuable comments. His enthusiasm and optimism made this experience both rewarding and enjoyable. I am truly grateful to him for extending his total co-operation and understanding whenever I needed help and guidance from him. I am also heartily thankful to **Rupali Bhardwaj**, PG coordinator, for motivation and providing uncanny guidance and support throughout the preparation of the thesis report.

I will be failing in my duty if I do not express my gratitude to **Dr. S. S. Bhatia**, Senior Professor and Dean of Academic Affairs, for making provisions of infrastructure such as library facilities, computer labs equipped with net facilities, immensely useful for the learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation, love and affection, which made my stay at Thapar University memorable. Last but not least, I would like to thank my family for their wonderful love and encouragement, without their blessings none of this would have been possible.

Navdeep Kaur

(**801433017)**

# Abstract

Due to an increasing growth of Internet usage, cybercrimes has been increasing at an Alarming rate and has become most profitable criminal activity. Botnet is an emerging threat to the cyber security and existence of Command and Control Server(C&C Server) makes it very dangerous attack as compare to all other malware attacks. Botnet is a network of compromised machines which are remotely controlled by bot master to do various malicious activities with the help of command and control server and n-number of slave machines called bots. The reason behind choosing botnet as a famous weapon for cybercrimes is that, it easily hides attacker's identity, difficult to find command and control server, encryption of malicious traffic and hide itself with normal traffic. The main motive behind botnet is Identity theft, Denial of Service attack, Click fraud, Phishing and many other malware activities. Like many other Malware, botnet is one of the dangerous attacks on cyber security. But it becomes more harmful with its autonomous behavior and longer activeness. It can also encrypt itself to hide with Normal Traffic and generate very low traffic. Botnets rely on different protocols such as IRC, HTTP and P2P for transmission. Complexity of Internet and its encrypted command and control server makes the Botnet very difficult to trace. Command and control server can work properly until it gets detected. Different botnet detection techniques have been proposed in recent years. There is a big need to design an accurate techniques or model to detect the botnet in efficient way.

# Table of Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

Internet is a global system of interconnected computers in a network which connect millions of devices all around the world. A network of networks that is having a millions of public, private, business, academic and government networks of local to globe extent, connected by a wide array of wireless, electronic and optical networking technologies. The Internet takes a wide range of information services and resources, like interlinked hypertext documents and World Wide Web (WWW) applications, telephony, electronic mail, and peer-to-peer networks for sharing files.

Now a day, the Internet facility is accessible to hundreds of millions of people in public, cooperative and self-sustaining all around the world. The Internet uses a part of the total resources of the existing public telecommunication networks. Two latest adaptions are the Intranet and the Extranet they also make use of the TCP/IP protocol.

## 1.1 Overview of Botnet

The Threat of Botnet has become one of the most dangerous attacks to internet security. As web based applications are used in every field thus, each Organization, IT industries, schools and individual needs to protect their systems from this kind of network based attacks. Botnet is known as most dangerous among all malware because of it's some very serious features as hiding its presence, download script without owner knowledge and defending itself from detection. The common Command and Control server is center from where botmaster send command to all bots. Botnet is very dangerous attack because of its longer activeness and it also generates very low traffic. Botnet is responsible for many biggest attacks as such as DDoS attack, Identity theft, steal credit card numbers for financial gain etc. Botnet has some wide features as existence of Command and Control server makes it different from other malicious attacks. Other feature is its flexible nature, as Botmaster change the location of Command and Control server after each attack. A reason behind choosing botnet as a famous weapon for cybercrimes is it is easy to hiding attacker identity, difficult to find command and control server encryption of malicious traffic hide itself with normal traffic. Complexity of Internet and its

encrypted Command and Control server makes botnet very difficult to trace. Command and Control server can work properly until it gets detected.

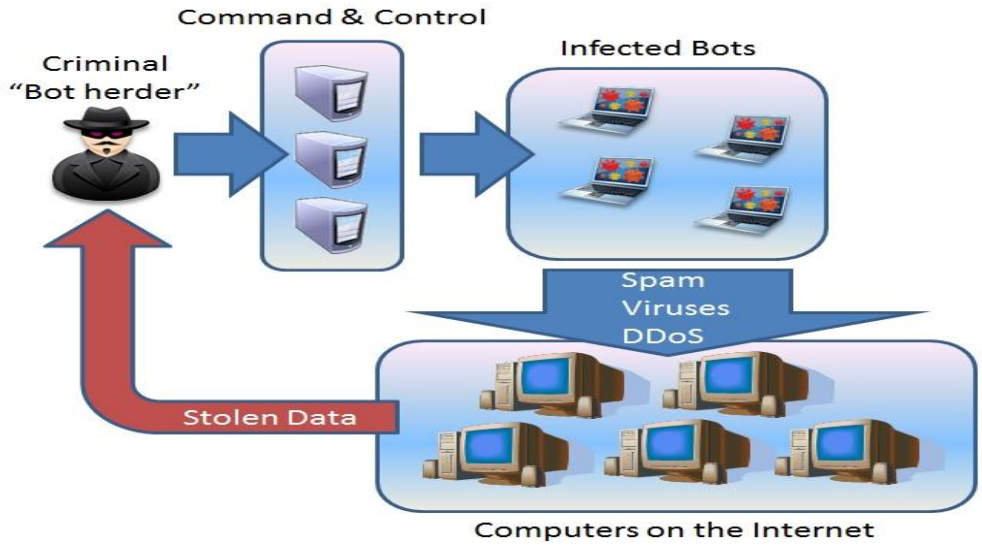



Figure 1.1 Botnet

Expert believes that approximately 16-25% of computers connected to the internet are members of botnets. One of the internet security threat reports indicates that US has 80% of infected traffic being part of Botnet network.

### 1.1.1 Botnet Components

Botnet is a collection of bots which are controlled by Botmaster under a Command and Control server. It is a network of compromised machines which are remotely controlled by botmaster to do various malicious activities with the help of Command and Control server and n-number of slave machines called bots. The main motive behind botnet is Identity theft, Denial of Service attack, Click fraud, Phishing and many other malware activities. Botnets rely on different protocols such as IRC, HTTP and P2P for transmission.

- **Bot**

The term Bot comes from a word Robot that automatically works according to a computer program or scripts written by the botmaster. Bot is a new type of malware which can be installed on victim machine without its owner's knowledge and remotely controlled by botmaster. When the malicious code written by botmaster is installed on victim machines then these machines becomes the bot or Zombie.

The type of bot, depends on the botnet structure and communication protocols used for them. As IRC based botnet generate IRC bot which is created with Ping-Pong named mechanism to get alive. Ping-Pong is a small size file which also act as a C&C sever but it cannot handle large number of data. HTTP bot created with HTTP based botnet is different from IRC bot as it does not need any TCP connection to stay alive.

- **Command and Control Server (C&C)**

Command and Control server is a center from where botmaster send commands to the entire Bots attacker controls the zombie army or bots from common C&C server. Location of C&C server and time when it will be placed depends on the model or structure used for creation of botnet. All infected machines need to know the address of a C&C server while downloading the script, so that they can easily communicate with the server. C&C server can be created with different topologies as: Centralized, Hierarchical, and Hybrid which is a combination utilizing HTTP and IRC protocols. In centralized model C&C server is designed in center host machine while in P2P model any bot can be selected as C&C server.

- **Botmaster**

Owner of Botnet is known as Botmaster or Bot Herder which infects and control the remote bots. Botmaster is an important entity of botnet structure that controls the all operations of botnet. It can be a single person or group of persons who can infect a number of computers without owner's knowledge. Botmaster design the botnet for own use or may rent botnet to others. Botmaster gives the command to all bots with the command and control server and decides the activities done by bots. Botmaster are also responsible to perform all malicious attacks done with their botnet.

- **Victim**

Victim is the target machine or host machine which is vulnerable and botmaster try to infect the victim machine with malicious traffic. Victim could be a single machine, network or person whose machine is to be targeted. It depends on the motive of attack and type of botnet

### 1.2.1 Role of Botnet

Botnet become the one of most dangerous attack to internet Security and favorite weapon for cyber-criminal to attack the internet. A term Bot is short form of Robot which acts according to the written Computer program or script. Bot can be written in various Programming Languages as many bots are written in C++. Botnet is collection of Bots also called Zombie machines which are infected by Botmaster with the help of Command and control Server. Owner of Botnet is known as Botherder or Botmaster who design and control the botnet to do various malicious activities. Botmaster can be a single person and group of persons who infect the victim machines which its owner knowledge. Botmaster find vulnerable Hosts connected in Internet and attack them with different techniques as Social Engineering, Spam etc. Like many other malware Botnet is also very dangerous attack to cyber security. But it become more harmful with its autonomous behavior and encrypts itself to hide with normal traffic. The common Command and Control server is center from where bot master send command to all bots. They infect victim machine much as possible to create large number of Zombie army .The Command and Control Server is the common server which is used the send and receive commands to all bot under a Botnet.one of the main reason for difficulty in tracking botnet is Existence of Common Command and Control Server. With this Command and Control server botmaster makes the botnet more complicated and very hard to Detect There are some new kind of Botnet which change the location of Command and control server after each Command.

Botnet can be categorized according to the architecture build over existing communication channels. At the starting traditional botnet were developed on internet relay chat (IRC based). Many Botnet were designed with IRC Protocols. Centralized architecture of IRC based botnet makes it vulnerable and can be trace by single IRC.

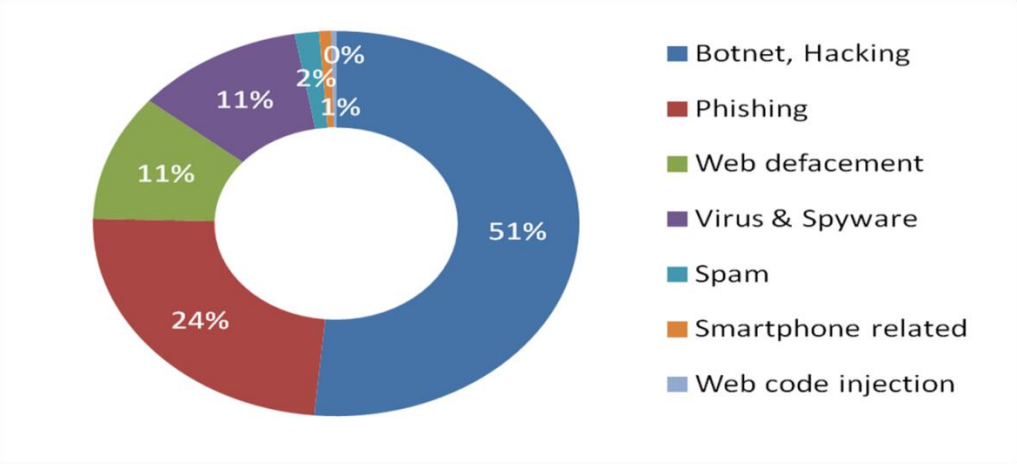



Figure 1.2 Botnet Attacks

### 1.2.3 Background of Botnet

Botnet become one of most dangerous attack to Cyber Security. Botnet was started in 1990 and in initial phase, botnet doesn't act as a malicious network. At starting, Botnet created as chat rooms for communication with IRC protocols. Earlier botnet was used to do legal activities such as controlling all organizations with one server, checking the activities of employees by controlling all the systems in a single network because of its cheap and many useful applications. Hackers use botnet to do malicious activities. One report discovered 35% infection on internet among the Zero Access Botnet infected countries, India ranks at third position.

In 2004 eBay was also infected with DDoS attack. Zotob named another P2P based Botnet launch the DDoS attack on many famous companies website located in U.S. CBI and Microsoft report states that they found around 57,783 hosts under botnet. The world largest botnet was introduced in 2008 named as Kraken, which has infected more than 500 companies. A new version of Zeus botnet is also one of the dangerous attack infected European banking customers and stolen around $47 million. One another IRC based attack was Darkbot worm which receive automated messages appeared as automated bot.

Ghostnet named botnet was one the biggest botnet attack in earlier year which infected the thousands of computes included government organizations located in different countries. It used the Remote Access Tool (RAT) which automatically downloaded with e-mail attachments. These botnet were worked with social

engineering tricks to made these malicious files resembles as original attachments. In 2010, Stuxnet named botnet was coming that controlled industrial PLCs. It has advanced structural design to communicate with Command and Control server to send messages. Microsoft also indicated in 2013 that they take down the eight botnet yet and also tracing many other botnet.

From previous year's botnet is used as a more powerful tool to do cyber-attacks as launch DDoS attack, send spam, and click fraud, theft credit card numbers and confidential data for financial gain. At earlier years, Botmaster use IRC based botnet but because of its many drawbacks as IRC protocols are rarely used for communication thus it catch easily. So new botnet were designed using HTTP and P2P protocols. There are many dangerous botnets that were established using HTTP and P2P protocol to overcome the IRC based detection.

Now a day, Botnet is coming with more difficult attack as Mobile botnet which is SMS and Bluetooth based. Botmaster exploit the features of latest smart phones which are using mostly web based applications. One other new kind of botnet is Botcloud which is design with using freely available cloud services. Cloud based botnet is very hard to detect because of its dynamic environment and less security provides on cloud services. So it can easily find vulnerabilities.

Table 1: Different types of bots, protocols used

| Bot Name | Protocol Used | Year |
|---|---|---|
| EggDrop | IRC | 1993 |
| Gt Bot | IRC | 1998 |
| SD Bot | HTTP | 2001 |
| Ago Bot | IRC | 2002 |
| Spy Bot | P2P, IRC | 2003 |
| RBot | IRC | 2003 |
| Sinit | P2P | 2003 |
| Bobax | HTTP | 2004 |
| Phatbox | P2P | 2005 |

| | | |
|---|---|---|
| Rustock | IRC | 2006 |
| Zeus | HTTP | 2007 |
| Torig | HTTP | 2008 |
| Storm | HTTP+P2P | 2008 |
| Stuxnet | HTTP+P2P | 2009 |
| Spyeye Bot | HTTP | 2009 |
| BingBot | HTTP | 2010 |
| Zeus P2P | HTTP+P2P | 2011 |
| Flashback | P2P | 2011 |
| Chancleon | HTTP | 2012 |
| Yandex Bot | HTTP | 2012 |
| Boatnet | - | 2013 |
| clickBot | HTTP | 2013 |
| RSS Bot | - | 2013 |
| Chat Bot | - | 2014 |
| Nero Bot | - | 2015 |
| Web Bot | - | 2015 |
| Smart Bot | - | 2016 |

## 1.3 Objectives of Botnet

Botnet is a term refers to network of interconnected computer known as Bots which are remotely controlled by Botmaster with the Command and Control Server. Botnet Become the most dangerous malicious activity done by hackers. Existence of Command and control server makes it as a hardest attack to find and control. These Command and Control server change their location frequently and making the detection a more challenging part. Bot which is a short form of robot also called as Zombie Computer. Botmaster infect the victim machine with the help of malicious code or script and made them a part of Botnet. Botmaster also known as a Botherder

is a person or group of people who make the Botnet for some malicious purposes. Command and control server is used to create and communicate with the Bots.

There are many reasons behind creating botnet and the main objective of creating Botnet is financial gain as Credit Card numbers, Banking etc. there are some following botnet attacks.

- **Identity Theft**

Botnet could be design to identity theft generally botmaster hide their identity with using infected host machines to spread the malicious traffic. It increasingly becomes a common problem as fraudsters find out more and more ways to take hold the information which is needed to steal anyone's identity.

- **Phishing**

It is a chance to take sensitive information like usernames, passwords, and debit card details (and sometimes money, indirectly), sometimes for malicious reason, by masquerading as a trusty entity in an electronic communication.

- **Information Gathering**

One Reason behind creating Botnet is information gathering is steal confidential information by infect the victim machine without its owner knowledge as Bot hide itself with normal traffic and never do any activity which can detect by antivirus. Motive behind information gathering could be financial gain by stealing confidential data or reconnaissance. As bots are also collect other party (from Competitor Company or nation) for reconnaissance. Botnet is also used for various search engines as Google also used Bot to steal the latest data from new website.

- **Click fraud**

It is also done by botmaster where some advertisements are as pay for clicking. Bots do this attack by using identity of any legal user. It is a type of fraud that happens on the internet in pay-per-click (PPC) online advertising when a person, or programming computer imitates a legitimate user of an internet browser by clicking on an ad, for a sake of generating a charge per click not even having any interest in the target of ad's link.

- **DDoS Attack**

One of dangerous attack done by botnet is Distributed Denial of Service attacks (DDoS attacks) which are very harder to detect and shut down those botnet. It is a type of DOS (Denial of Service) attack, where a number of compromised systems, which are sometimes infected by Trojan, applying to target a particular system causing a DDoS (Denial of Service) attack.

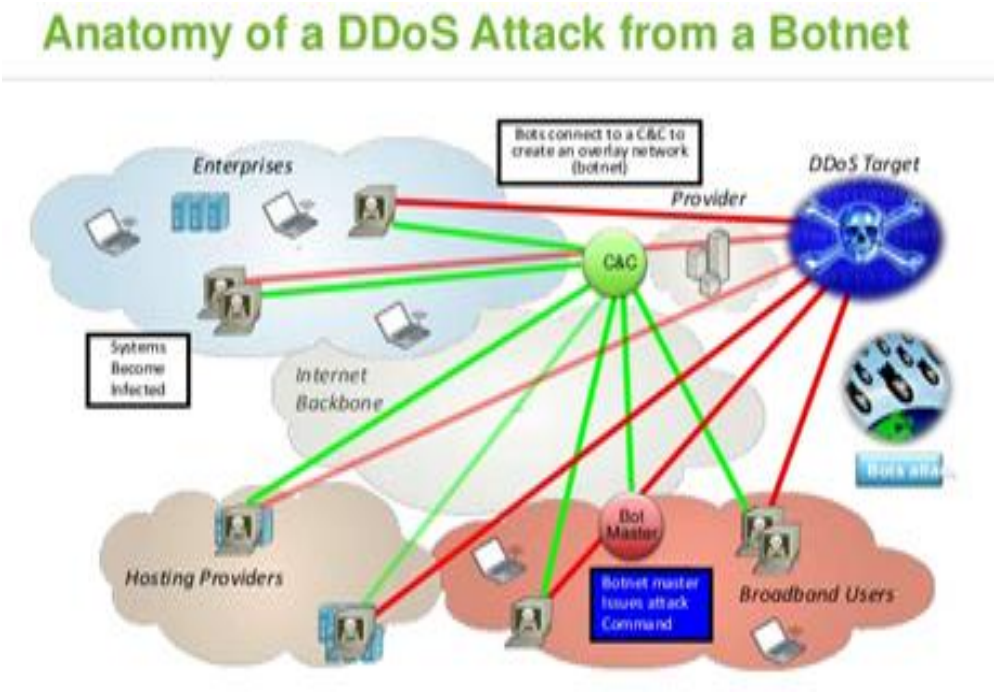



Figure 1.3 DDoS Attack

- **Key logging**

It is the action of logging (recording) the keys that struck on a keyboard, typically overtly, so that the user is unaware that their actions are being tracked or monitored by using it. It can also be used for studying human-machine interaction.

## 1.4 Life Cycle of Botnet

Botnet can create with a various components. Firstly, it needs to set up Command and Control server from where botmaster infect other vulnerable hosts. Second thing is writing a malicious script for making a bot this malicious program can be written in various programming languages like old botnet as Agobots and many other botnets were written in C++. Botnet send this script with using Social Engineering, e-mail attachments etc. One report indicates that 80 % of email are spam and generally sent

for malicious purposes. For design and maintain the strong botnet and make the infected bot active, Botmaster needs to go through various stages in order to combine all these components. Traditional Botnet can be created with using five steps initial injection, Secondary Injection, Connection, Command and Control Server and Upgrade and Maintenance

- Botnet creation is started from Initial Injection. At the starting phase, Botmaster try to find the vulnerable host and find the way how to infect them. Botmaster send a malicious script to the vulnerable host which is automatically installed itself in victim machine and wait for instruction come from Command and Control server. Botmaster choose the most reliable way as attach with infected files, malicious websites, spam etc. to send the script and hide this from the owner of Victim Machine. In this phase, botmaster spread the script to all vulnerable hosts. All victim machines where these scripts have been downloads become the part of botnet.
- Second phase is Secondary Infection which is requiring to completing the working of first initial injection. This phase is completed when user runs the downloaded scripts and after run the script successfully then victim machine become the real bot and a part of botnet. Botmaster needs to make the script similar with real software or by legal download link. After activation of bots these all become active and wait botmaster command.
- Connection is one of most important part of botnet life cycle. These previous phases are used to implement the structure of botnet. After create the bots, it needs to connect with Command and Control server that maintain a good communication between them to send and receive messages from server. Third phase is mostly known as Connection phase, which is very necessary to control the working of botnet. Here, botmaster create connection between every bot and Command and Control server. Connection phase needs to update after every attack to check the list of active bots and communication possible between them.
- The most important phase of Botnet life cycle is Command and Control server which is necessary for working of Botnet. It is also a most vulnerable part because like in centralized botnet, Command and Control server is also to catch all botnets it can be trace easily so creating and hiding the Command and

Control server is the big issue for botmaster at this phase after establish the Command and Control server and create connection between all bots. Thus message are communicate to all bots and get information back from all active bots. Command and Control server send command to all existing bots and also find the new vulnerable host to infect them .the number of bots in botnet called as bot army or Bot Zombie.

- After creating and working with botnet, Last phase of Botnet life cycle is upgrading and Maintenance it is necessary to update the botnet after each attack. Updated bots need to create connection with Command and Control server each time. One big issue is hiding the Command and Control server. Thus in this phase it change the location of C&C server constantly.

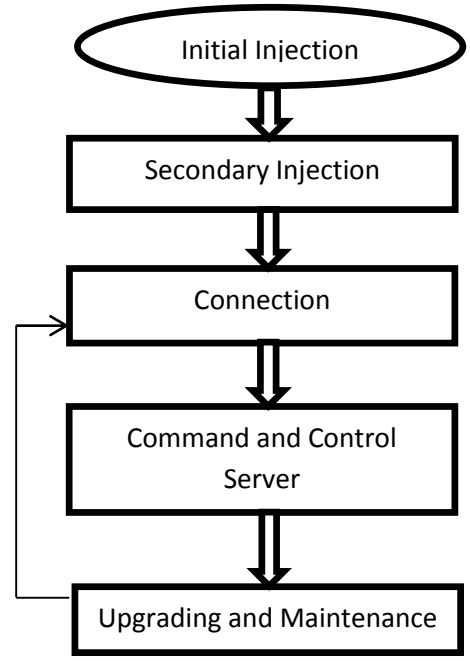



Figure 1.4 Life cycle of Botnet

# CHAPTER 2

# Literature Review

A bot is a malicious script or Computer program written by Botmaster to remotely infect the victim machine and to get control of that machine. A botnet is network of bots which are remotely controlled by Botmaster with the Command and Control Server. Botnet attack becomes very famous in previous years. Many researches have been done on the research work of knowing the botnet in brief and to find the detection techniques. There are many papers which get published on the topic of Botnet which are briefly defining the actual structure of botnet, its life cycle and botnet Detection Techniques. Most of Survey on Botnet has been done dated from 2009. Lots of work has been done in detection area to trace the botnet and defend against it. But still many work needs to done on Botnet and find the latest techniques to detect the Botnet and make the safe internet usage.

Zhu *et al*. [3] presented a survey on botnet that classifies different types of bots protocols used and also presents a metrics which are used for determining the size for botnet and identifies the new kind of botnet.

Bailey *et al*. [4] presented a short survey on Botnet and its Detection techniques in which they had defined the problem of botnet in three different sections as first is understanding the problem of botnets, second is understanding the network protocol used by the botnet and third one is botnet measurement studies as size estimation and behavior analysis.

Tyagi and Aghila [5] discussed about botnet problem in detail that defining the botnet, its life cycle, brief history and related work done on botnet. They also have proposed some mitigation techniques and prevention to botnet.

Silva *et al.* [6] presented a botnet survey that broadly defines the problem of botnet and also summarized the previous work done on botnet. In their paper they have classified the previous research result as comparison of existing detection techniques and had also indicated some challenges to for future research work.

Chang et al. [7] on botnet defines the Latest botnet trends and new botnet coming in the cyber world. Their survey also shows the different bot families and the launch of DDoS attacks. They have performed the analysis on different sixteen botnet families and reported new observation from the behavior of these Botnet. They purposed the new kind of botnet behavior to understand the working of botnet.

Mahummad *et al*. [8] also presented a survey which reviews the problem of botnet, its architecture and bot behavior. They have explained some botnet models that detect the botnet according to the botnet behavior and new emerging botnet as mobile botnet using SMS and Bluetooth services. In their survey they have used three methods for botnet detection

- Traffic Behavior
- Botmaster trace back Detection
- Using Virtual Machines to detect the botnet

## 2.1 Motive behind Botnet

Botnet is the famous tool used by attacker to perform various malicious activities. The main motive of the Botmaster for creating the Bot is the get the financial gain.

Chao *et al.* [9] had indicated in their survey that the motive behind botnet is spamming and they had discussed about the many European phishing attacks and spam that comes through network traffic. They have also proposed the concept of analyzing the information according to the network traffic and presented a framework, which identifies the botnet using three distinct levels. At the first level they have indicated the Single packet analysis, at second level packets are analyzed according to the network and at the third level tcp/ip traffic contents were analyzed.

These are some of the traced Botnet attacks that are done by various botmaster to achieve their motive of different types:

- DDoS Attacks
- Phishing
- Spamming
- Identity Theft
- Key Logging

- Click Fraud
- Traffic Sniffing
- Spreading New Malware
- Installing Adware and spyware
- Stealing Confidential information

## 2.2 Classification of Botnet

Botnet can be classified according to different methods, topologies and protocols that are used by the botmaster to create a strong Botnet. It can be classified in three ways based on topologies used for creating its architecture or it can be classified according to different communications and network protocols used by botmaster.

### 2.2.1 Based on Topologies

Botnet can be analyzed according to its architectural design created by Botmaster. To make the Botnet more complex and harder, Botmaster use different types of protocols and topologies to design a strong Botnet. According to these design botnet are generally divided into two parts. First is centralized that mainly use IRC and HTTP based protocols and decentralized that is created with peer to peer and hybrid architecture.

- **Centralized Model**

The simplest model for creating botnet is Centralized Model. This structure is having a single central Command and Control server for communication and creating all other Bot. All Bots are directly connected with a single C&C server. This central point needs a very high bandwidth. From one C&C server, Botmaster sends and receives messages to all other bots in network. Many previous Bots like AgoBot, SDBot and RBot were created with centralized model. The Biggest weakness of this architecture is single Command and Control Server which makes it more vulnerable. If single command and control server could get detected, then all other network can also be easily detected. Centralized model can be created using IRC and HTTP based protocols.

According to Zeidanloo *et al*. [10] the main advantage of using centralized model is botnet can easily design and launch all attacks with this model, because it has very small message latency. Other advantage of this model is central C&C server makes the communication easy between all bot network as all bots are directly connected to one C&C server.

Hossien *et al.* [11] explained the centralized model as one central point is responsible for all working of botnet. This C&C server is called as vulnerable point or weak point of a centralized model as all bots can easily be trace by using their addresses stored in the C&C server.

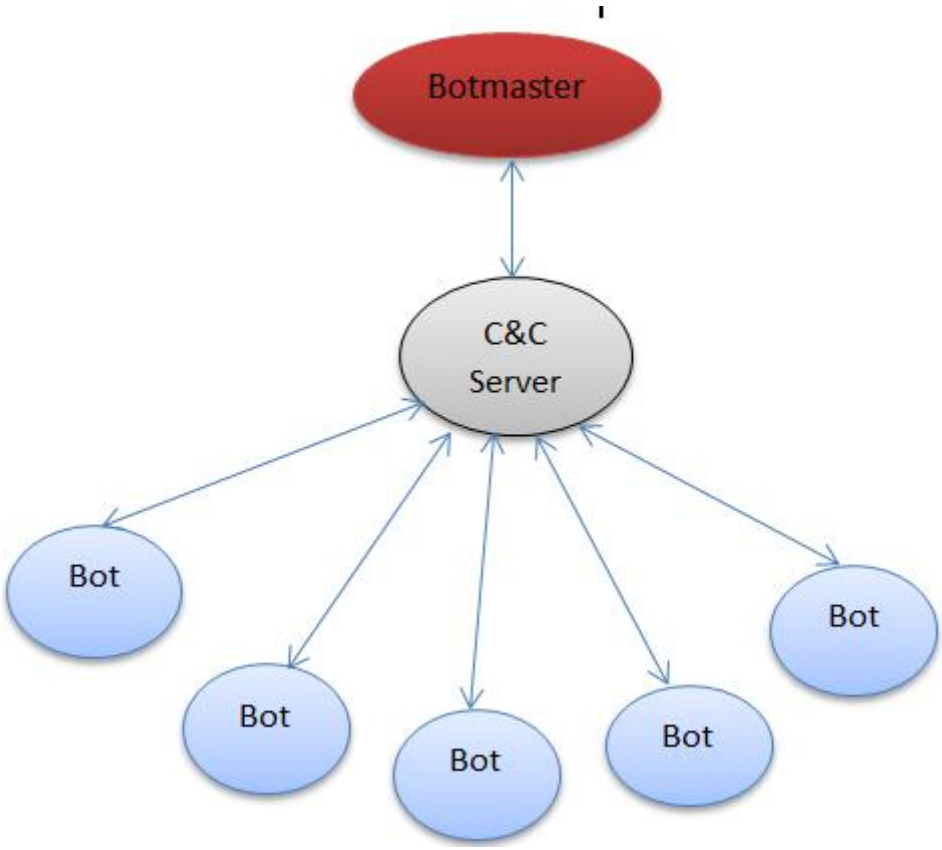



Figure 2.1 Centralized Model

- **Decentralized Model**

The biggest weakness of a centralized model is single command and control server which makes the botnet very easy to detect. To overcome this vulnerability bot owner developed decentralized botnets. Decentralized model can create large number of bots

in a single botnet and it is very difficult to trace. Decentralized Model depends on P2P protocols [11].

Cooke *et al.* [12] explained the decentralized model as strength of this model is not a single C&C sever which controls the whole botnet. Decentralized model is very difficult to be detected because detection of some bots does not mean all entire botnet will trace using these bots. As decentralized model do not depend on one single point which have control of all botnet and if C&C sever will detect all botnet will trace easily with this server.

Nagaraja *et al*. [13] defined the decentralized model with peer to peer protocol model and benefit the efficient communication model. Less centralization give the ability to join and control the entire botnet from any bot to any place. Decentralized model also gives the benefits of low time delay, any to any communication from bots and less dependency.

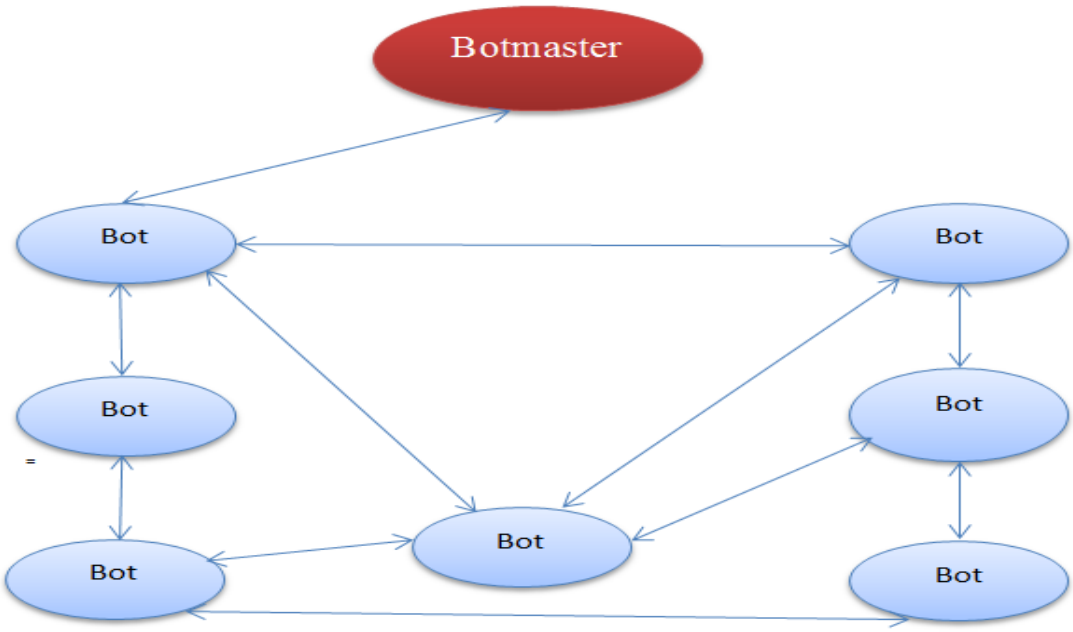



Figure 2.2 Decentralized Model

- **Hybrid**

Hybrid Model is a combination of both centralized and decentralized model. As each design of botnet have some benefits and drawbacks. For creating strong botnet architecture, Botmaster take advantages of hybrid model. In hybrid model, encryption

key is used to hide botnet traffic within normal traffic. This model use random vulnerable port and sends encrypted messages from any bot in the network.

Wang *et al.* [14] purposed the hybrid model which is categorized as servant bot and client bot. These servant bots can work as both server and client. Servant bots can configure with static and routable IP addresses. These are working with using self-generated encryption key which makes the detection of botnet very challenging task. Client bots are configures with dynamic and non-routable IP addresses. They do not need a global internet connection and can also bypass the firewall very easily.

Holz *et al*. indicated that the recent most wide spread botnet was peer hybrid model which are using peer to peer to protocols. They examined the working and communication of one of most famous storm botnet using case study of peer to peer botnet.

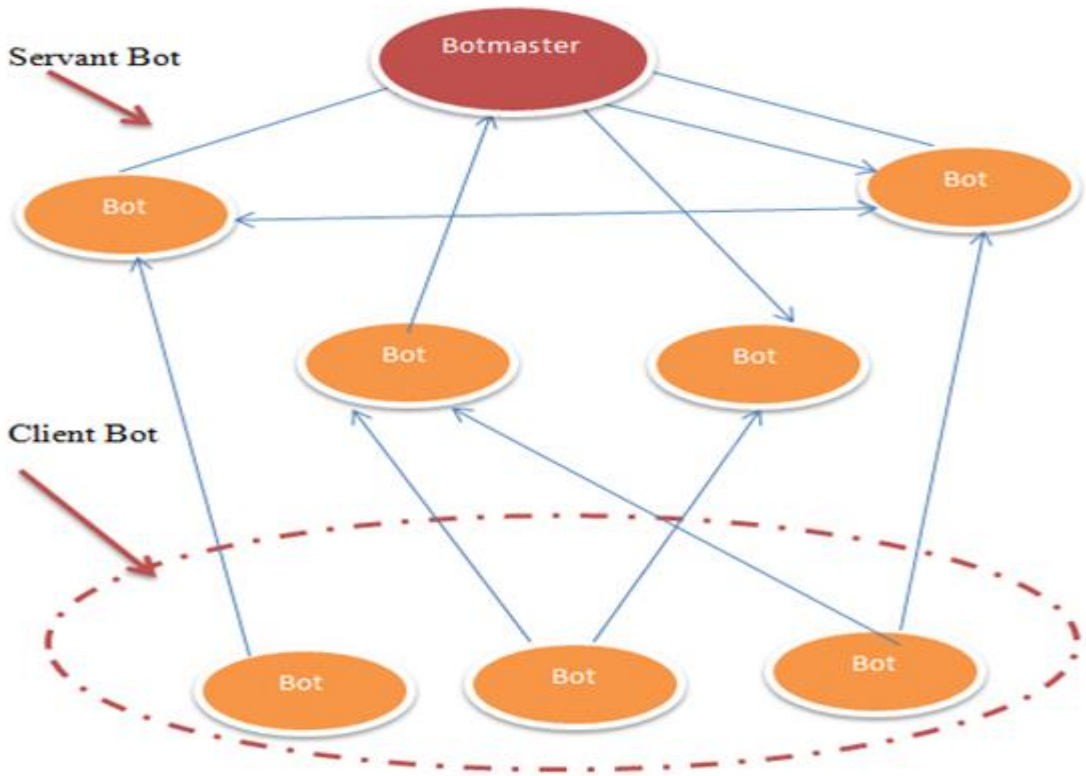



Figure 2.3

### 2.2.2 Based on Network Protocol

Botmaster can establish the connection between C&C server and bots using different network protocols. Each protocol has different communication rules for working

through network. Botnet can be designed using different network protocols follows as.

- **IRC Based**

First type of network protocol used for botnet was IRC protocol. IRC term stand for Internet Relay Chat works with real time internet text messages. Botmaster use IRC channels to create and communicate with all botnets. Due to its simple architecture and high flexibility, IRC botnet is mostly used by many botnet owners. This botnet is very effective in creating and reusing the bots. One limitation with IRC based network is its common usage of IRC protocol for communication which gets easily traced simply by seeing IRC traffic as part of normal traffic**.**

- **IM Based**

IM stand for instant Messaging. This type of network communication does not become very popular. Difference between IRC based and this protocol is only that it use instant message services. It needs to create individual instant messaging account every time for all bots so it is very less in use and bots also needs to remain online all the time in this network.

- **Web Based**

New type of botnet is mostly created with using web based network protocols. It controls the bot network over World Wide Web. One of the famous examples of it is Http based botnet where Botmaster create one web server. All bots send command to that server and wait for reply from server as, communication between all bots is done by using that web server.

### 2.2.3 Based on Communication Protocol

Botmaster need to establish an effective communication between all bots and control server for properly utilizing all zombie machines or bots connected in the botnet. Network communication between all bots is done with using different protocols follows as.

- **IRC Protocol**

IRC term stand for Internet Relay Chat works with real time internet text messages. Botmaster use IRC channels to create and communicate with all botnet. Due to its simple architecture and high flexibility, IRC botnet is mostly used by many botnet owners. This type of botnet is very effective in creating and reusing the bots. One limitation with IRC based network is its common usage of IRC protocol for communication which gets easily traced simply by seeing IRC traffic as part of normal traffic.

Zhuge *et al*. [16] analyzed the botnet behavior with tracking the unique 3,290 IRC based botnets in china and result shows that the IRC based botnet infected the most of computer over world. They found the large number of botnet which get automatically installed and spread bots. They mainly focused on autonomous bots.

Wang *et al.* [17] purposed an algorithm to detect IRC based Botnet which does not need any information about the previous botnet. As earlier IRC based botnet can easily detect with its similar behavior or signature. But this algorithm can detect the new IRC botnet without analyzing previous bots.

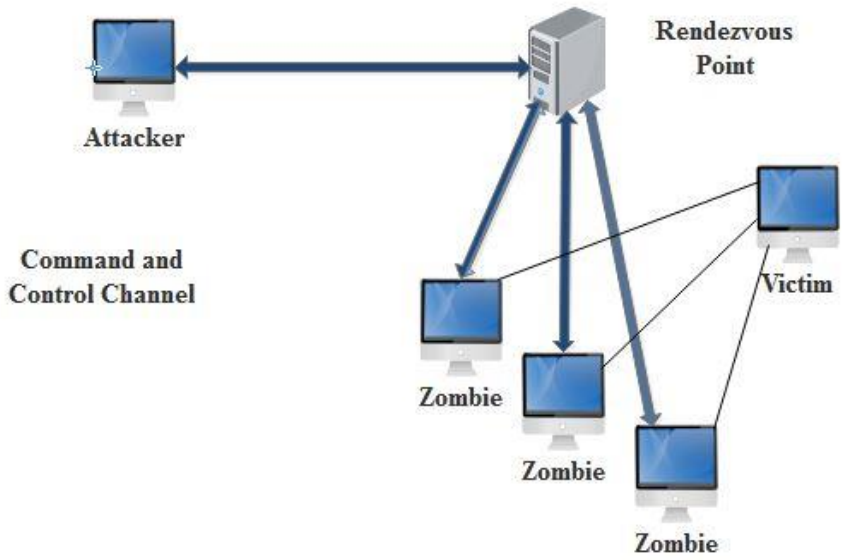



Figure 2.4 IRC Based Botnet

- **HTTP Protocol**

Hyper Text Transfer Protocols are also very popular for creating Botnet. It can easily hide botnet traffic with normal traffic. With the HTTP protocol Botmaster can easily bypass the firewall and hide malicious traffic with normal HTTP traffic. HTTP based

bots often download the instruction from web based Command and Control Server, which is more accurate then IRC based botnet [13]. Http based model is used by many famous botnet such as Bobox, Click Bot, Rustock. [10]. Many Researchers has purposed some web based models to Detect HTTP Based Bot from network traffic.

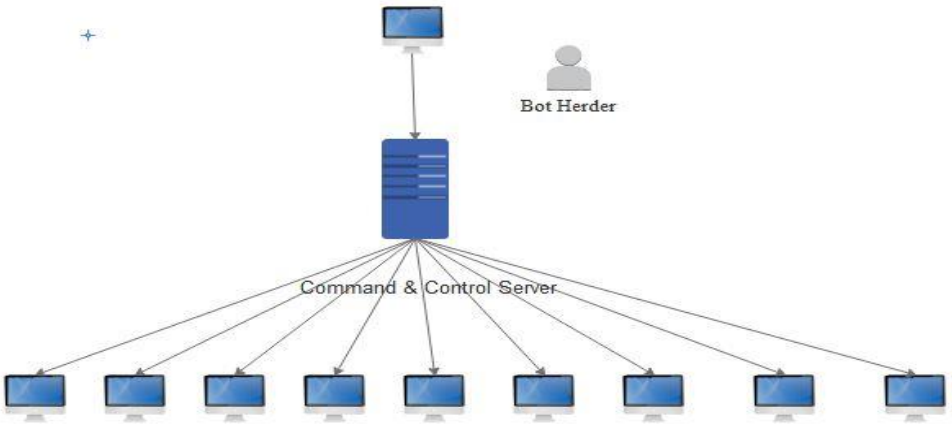



Figure 2.5 HTTP based Botnet

Lee *et al.* [18] indicated that now a days most of botnet are created using HTTP protocols. One report indicated that 75 percent botnet are HTTP based botnet. One of the most famous HTTP based botnet is black energy which is primarily used for launching DDoS attack. Black energy botnet is easy to use on web based server but it also needs to connect bots again and again to the server which makes the botnet easy to detect.

Eslahi *et al.* [19] described the HTTP based botnet which is created by HTTP protocol and publish commands to bots, through web server. As HTTP is commonly used for network traffic it is not easy to block all HTTP based traffic or to differentiate the malicious traffic from normal traffic. HTTP based botnet can easily hide itself with normal web traffic and by pass the security systems.

Perdisci *et al.* [20] explained the HTTP botnet as most famous and reusable malware which creates itself again and again and also available for sale on internet. As Zeus botnet toolkit is freely available on internet. They also purposed the system to detect network level botnet using network signature and performed experiment over large number of botnet.

- **P2P Protocol**

Peer to peer model provide decentralized model where all bots are connected with each other. The main aim of peer to peer protocol is to hide the command and control server. Botmaster uses different bots to issue commands every time. Bots are dependent on previous or other connected bots without having Single C&C server. Nearly 70% botnets are created using P2Pprotocols. Some advanced botnets like Phatbot, Nugache used P2P based bots for creating a botnet. P2P based model creates a very complex architecture which is very hard to trace. Botmaster can use any peer to communicate with other bots. It act as client server model where each node can work as client or server. For creating a new bot it just need an address of any bot connected in botnet for communication. Major benefit is detection of single bot doesn't mean detection of whole botnet.

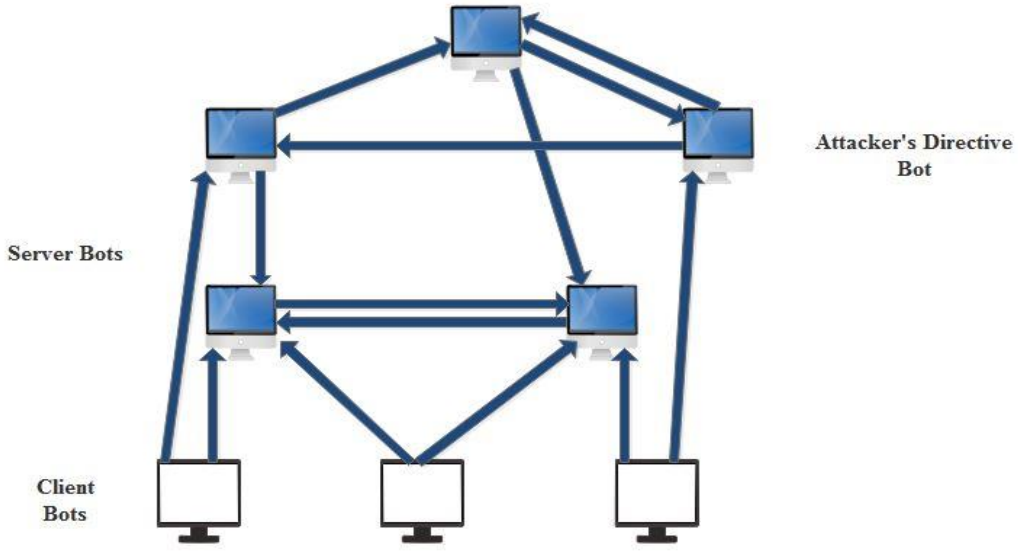



Figure 2.6 P2P protocol based botnet

Wang *et al.* [21] presented an advanced hybrid peer to peer botnet design. Recent botnet like Phatbot, Sinit and Nugache etc. have also designed by using different peer to peer protocols. Old P2P designs of botnets have many weaknesses.

A Sinit bot uses random probing to find other Sinit bots to communicate with. This results in poor connectivity for the constructed botnet and easy detection due to the extensive probing traffic. Phatbot utilizes Gnutella cache servers for its bootstrap process. This also makes the botnet easy to shut down.

## 2.3 New trends in Botnet

Mobile botnet attacks are Botnet attacks which can work with SMS or Bluetooth services. Another newly emerged Botnet by bot master is Bot cloud using cloud services. Cloud based botnet is very easy to build because of availability of its online services and they are very difficult to detect. One report claims that 35% of infection on Internet is generated by European Countries. Among the Zero Access Botnet infected Countries, India ranks at third position.

### 2.3.1 Mobile botnet

It is a type of botnet that points mobile devices like smartphones, trying to get complete access to the device and its contents. It is also providing control to the creator of botnet. Mobile Botnets take benefit of unpatched exploits to give root permissions over the compromised mobile devices to hackers, enabling to send text messages or e-mail, access photos and contacts, make phone calls, and more.

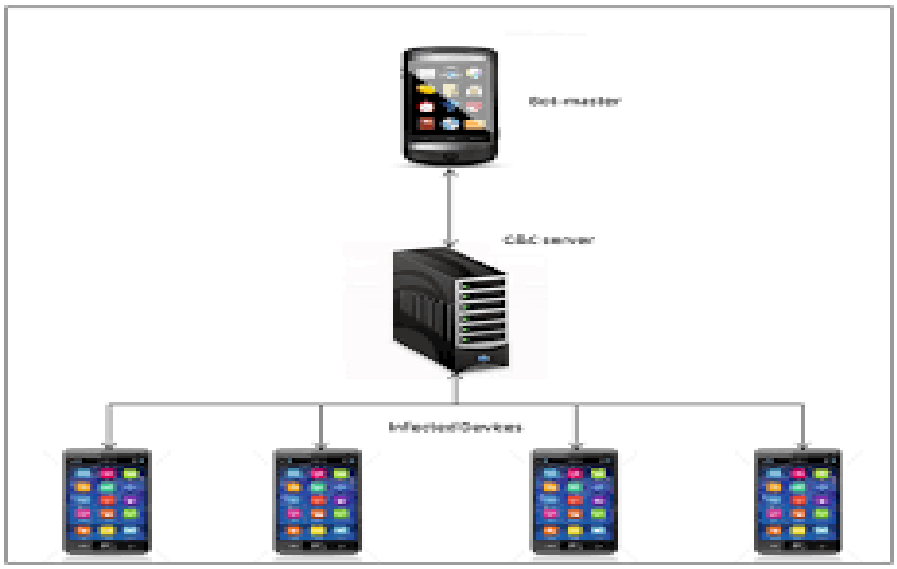


Figure 2.7 Mobile Botnet

Y Xiang *et.al* [22] introduced the new design of mobile botnet named as Andbot which is exploited with a novel command and control (C&C) technique named as URL flux. Andbot have many features such as low cost, low battery power consumption etc. The prototype of Andbot is implemented in the open source smart-

phone platform. Result of this experiment shows that this Andbot is suitable for smart phones and like all other botnet it is also very difficult to detect.

Chai *et.al* [23] proposed a mobile botnet detection using VPN. As they proposed a scheme that detects the botnet by finding the abnormal behavior of C&C traffic through VPN provided the shared path for ¾ G and Wi-Fi.

Karim *et. al* [24] investigated attacks of mobile botnet by exploring attack vectors and a well-defined presentation of thematic taxonomy. By identified remarkable parameters of taxonomy they conducted comparisons to look into effects of exited mobile botnets in related to their findings. They have presented the open research challenges in domain.

- **SMS Based**

Jingua Hua and Kouichi Sakurai [25] presented a design of a botnet for command and control medium using SMS (Short Message Service). They had covered almost all the aspects of the botnet design having stealthiest protection, botnet maintenance and selection of topologies. They also demonstrated that the mobile botnet is a serious threat on the computing environment security. So they further explored several defense strategies against botnets.

Zang *et al*. [26] proposed a mobile botnet design that makes many mobile services to disruption. The mobile botnet use SMS services for creating C&C server and P2P as its topology. A simulation resulted that a modified Kademlia structures architecture is better for mobile botnet topology

Alzahrani et al. [27] proposed a framework for SMS botnet detection that uses multiple agent technology on observation based of android smartphone features. Their system had detected the SMS based botnets and identifies different ways to block the attacks to prevent damage by different attacks. The model was designed to find out malicious messages by applying behavioral analysis to find a relation among suspicious SMS and reported profiling.

- **Bluetooth Based**

Singh *et al.* [28] investigated the challenges for constructing and managing botnets which were mobile phone based and communicated via Bluetooth services. From a

large scale simulation based on freely available Bluetooth tracer, they demonstrated that a malicious infrastructure was happened in many areas due to day-to-day routine of human nature. In general, they demonstrated that C&C manages can distributed to approximately 2/3 of nodes which were infected within 24 hours after issued by botmaster. Then they explored how defense mechanism can be taken into as advantage for the same information to be more effective.

### 2.3.2 Bot Clouds

Now a days, Cloud computing and big data is getting very popular for hosting Network services. Botmaster are also getting attracted towards the advantages of cloud computing for creating a Botnet. With the help of Cloud Services Botmaster can easily design botnet and go online for long time period with ease. Another reason for creating Bot cloud is that detection chances are very less because of less security and prevention. These Bot Clouds are also known as Dark clouds which borrow the network to infect other networks.

Bot Clouds become very challenging to trace because of volume and huge bandwidth availability. Traditional methods are not effective to detect Bot cloud. As very less work has been done to detect bot cloud. Bot masters are using cloud infrastructure to make new Botnet.

Jaideep Chandrashekar *et al*. [30] presented an overall state of the art of botnets with stealthy malware. They also presented and developed some trustworthy anti-botnet defense strategies that mainly target latest and emerging trends in development of botnets.

Jerome Francois *et al.* [31] proposed a distributed computing framework that powers a host dependency model and a page rank algorithm. They also reported experimental results from a Hadoop cluster which is an open source and pointed the performance benefits using real network from an internet operator.

Victor R. Kebande *et al*. [32] had face a problem that there were no techniques that existed for gather information in the cloud for readiness purposes of digital forensics as explained in ISO/IEC 27043 i.e. international standard for digital forensic investigations. They proposed a model that permits digital forensic readiness to be attained by executing a Botnet as a service (BaaS) in a cloud environment

### 2.3.3 Social Bot

Growing of Internet usage also increased the trend of social media applications while giving us benefits of many applications such as online communication, Banking Transaction, Messages and Gaming etc. Social media also attracted the botmaster towards its free services. Botmaster now try to infect the large number of people with the help of Social media. They generally attack social website like Facebook Twitter etc. to infect large number of people within very short time period. These kinds of attacks are known as Social Botnet.

Botmaster uses social media as people easily believe on link provided on social media because of unawareness or lack of knowledge. It becomes very easy to infect victim with the help of making malicious website. Botmaster generally hide themselves by using other person's identity, making website names very much similar with legitimate website as users cannot catch the little difference or making webpages as normal websites many security provider organizations such as FBI are also trying to design effective techniques which can quickly detect the social media attack.

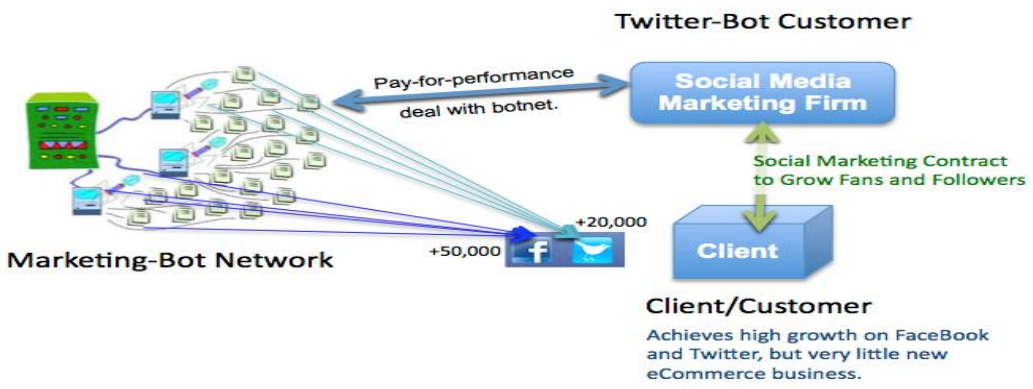



Figure 2.8 twitters Bot Network

Claudia Wagner *et al.* [33] studied data using Social Botnet Challenge 2011 which is an experiment conducted by the Web Ecology Project. In that project, three teams executed a number of social bots that expected to affect user behavior on Twitter. Using that data, they aimed to develop models in two parts: i) identified vulnerable users between a set of targets and ii) calculate user's level of vulnerability. They explored the predictive level of three different featured groups (behavioral, network and linguistic features) for these jobs. Their result suggested that vulnerable users

incline to use Twitter for a chatty purpose and incline to be more social since they connect with many users, shows more love then non-vulnerable users and use more social words.

Stefanie Haustein *et al.* [35] presented initial findings that automated Twitter accounts create a substantial amount of tweets to scientific papers and that behaved inversely than common social bots, had serious inferences for the use of raw tweet counts in research assessment and evaluation. They discussed some definitions of Twitter engagement from only bibliographic information to share or commenting on the paper content.

## 2.4 Botnet Detection Techniques

Botnet has become the most serious threat to cyber security. Its detection becomes the most popular research topic due to its large network, changing behavior and robustness. Botmaster develop new kind of encrypted botnets which can hide their presence and become harder to trace. Every individual user, businesses, organizations, needs to detect botnet. According to previous work done, botnet detection techniques are divided into two categories: Honeynet and Intrusion detection systems, which is further divided into four parts as signature based, anomaly based, DNS based and data mining based.

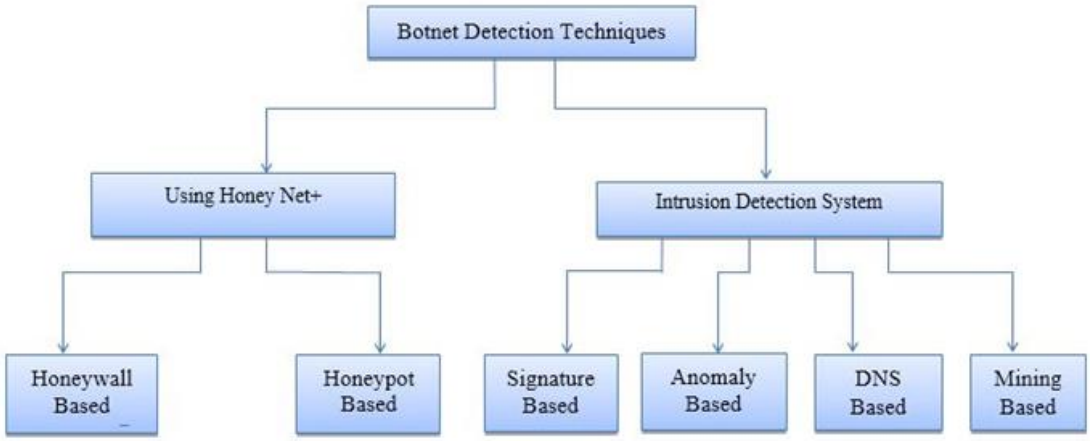



Figure 2.9 botnet detection techniques

### 2.4.1 Honeynet Based Detection

Honeynet based detection works with honeypot and honeywall. This technique is used to detect and monitor the behavior of botnet. Many researchers discussed about

detecting the existing botnet using Honeynet. It creates an environment which is best suited for understanding the Bot behavior and its characteristics. Honeypot term refers to a vulnerable pot which can be easily compromised. It also vulnerable with an intention of become a part of botnet and attracts botmaster to infect it [12]. Honeypot are always setup with unique idea.. Honeywall is a term used for software which is used to collect and control information from honeypot. Snort is one of the famous IDS used to track the botnets by analyzing the behavior of infected machine, botnet related information as location of bot, botnet type, and behavior can be collected.

Zhichun Li *et al.* [36] developed a common technique which had a minimum monitoring overhead for perceiving botnet behavior, and difficult to avoid by botnets. Therefore, people from all around the corners can easily accept it to calculate the characteristics of the behavior of botnets. If the measurements could be aggregated by them, possibly they can get a more precise picture of the botnets. After analyzing the behavioral list carefully, they found that the scanning behavior of botnet is rooted to the botnet because this is the actual way for them to adopt new bots. So, they believe in coming future, the botmaster will not giving up on scanning. Moreover, scanning monitoring is quite easy. People can get the botnet scanning traffic easily by installing a honeynet.

Anup Goyal *et al.* [37] proposed a framework that helps to extract global scanning events of botnets. From a large research institute based on one year Honeynet traffic, they studied six different characteristics of botnet scanning. They found botnets mainly from a small scale of ASes but certainly spread out all around the world from 2860 ASes totally. Two different botnet patterns arrival/departure: all collectively and gradually. They conjectured it to relate to different scan strategies. They also found the scan arrivals are running in time and inter-arrival time travels a exponential distribution, that might involve the scans are arbitrary scanning and its range is much larger than the detection sensor.

### 2.4.2 Intrusion Detection System Based Detection

- **Signature Based**

Signature based techniques works with the help of using the signature of existing Botnet it creates a database with existing botnets. Then by using pattern matching

method it compare the signature of network traffic with the existing Bots [18]. Due to existence of Signatures in a Database this techniques can immediately find the existing Botnet. Limitation of signature Based technique is that it can only find the Botnets which are known and already traced. But new Botnet are Difficult to trace using signature based technique. This technique cannot handle Zero Day Botnets.

Yinglian Xie *et al.* [38] focused on describing spamming botnets by providing both spam server traffic and spam payload properties. Near this goal, they developed a spam signature generation framework named AutoRE which detect spam emails of botnet-based and its membership. AutoRE does not need training data or white lists which are pre-defined. Moreover, it gets high quality regular expression signatures that can sense spammed botnets having low positive rate. In their depth analysis of the known botnets exposed few interesting findings concerning the mark of email obfuscation, botnet IP address properties, sending and correlation of patterns with network scanning traffic. They believed those observations are crucial information in botnet detection design schemes.

- **Anomaly Based**

Anomaly based techniques work with monitoring the network traffic. By differentiating the malicious traffic from normal traffic botnet can be detected. Brodsky et al surveyed that Botmaster send high traffic in short time period. Thus this technique captures the behavior of network.

George Nychis *et al*. [40] described that the previous work has confirmed the benefits of entropy-based anomaly detection, to understand the detection power there has been a little effort to understand comprehensively using entropy-based analysis of multiple traffic in combining with each other. They considered two classes of distributions: behavioral feature and flow-header feature. They observed that the port distributions and time series of entropy values are toughly correlated with each other and gives very similar anomaly detection. Further analysis using synthetically created anomalies also proposes that the address and port distributions have restricted utility in sensing scan and bandwidth flood anomalies.

Sajjad Arshad *et al.* [41] proposed a complete anomaly-based approach that needs knowledge of bot signature, C&C server addresses and botnet C&C protocols. They started from essential botnet characteristics. Bots connect to the C&C channel and

accomplish the received commands. Bots receive the same commands belonging to the same botnet that affects them having same netflows characteristics and delivering same attacks. Their method bot clusters with same netflows and assaults in unlike time windows and execute correlation to recognize bot infected hosts. They developed a system and estimated it with existing world traces comprising normal traffic with existing world's botnet traces.

- **DNS based**

DNS based technique is one of the most popular technique to detect botnet. It is a combination of both anomaly based and signature based techniques. It is also based on an abnormal traffic, generated by botnet. DNS based techniques works with information collected from DNS queries. Botnet needs every bot to connect and communicate with command and control server, thus it must use DNS queries that are typically hosts by dynamic DNS (DDNS) providers. By monitoring DNS traffic existence of Botnet can easily get detected. It can also trace the location of C&C server and Botmaster behind Botnet. Other Benefit of using this technique is as all Bots Use some domain to perform queries thus with detection of one Bot. whole botnet can get trace with this DNS tracing. With the help of DNS based techniques DNS based Black hole list is created which publish the location of networks or computers from where malicious activities are performed. DNS based technique is also useful to detect encrypted C&C Server as it utilizes IP Header.

Sebastián García *et al.* [43] surveyed by analyze and relates the most crucial efforts taken place in network based detection area. It achieves four tasks: i) a comparison of previous surveys and the bid of four new dimensions to evaluate their schemes classification; ii) a new comparison and classification of botnet detection proposal which is network based, includes the description of 20 favorite properties of every botnet detection paper; iii) a general comparison among the most representative detection proposals; and iv) the description of the most crucial problems and highlights those area. They concluded that the area has attained great improvement so far, but still many open problems are there.

- **Data Mining Based**

Data mining technique capture the high volume of network traffic and find the malicious traffic from it. With the help of existing techniques abnormal traffic can be

differentiated. But to detect C&C server and recognize its pattern used for Botnet is very difficult. As encrypted C&C Server hide itself with normal traffic so to detect this kind of Botnet attacks Data mining techniques are used with data Classification and Clustering.

Bhavani Thuraisingham *et al*. [44] discussed various data mining techniques that they had successfully applied for cyber security. Those applications comprise but are not restricted to malicious code detection by mining binary executable, intrusion detection network by mining network traffic, data stream mining and anomaly detection. They summarized their achievements and ongoing work at the University of Texas at Dallas on cyber-security research and intrusion detection.

- **Detection Techniques using Machine Learning**

Different Machine Learning techniques such as Classifiers, Decision Trees etc. are also used to detect the Botnet as they are more effective to detect chat Bots but cannot work well to Detects the Command and Control Server. Many researchers have use machine learning classifiers to work with IRC Log to detect IRC based and P2P Botnet. With the classification techniques large number of traffic can be analyzed and it becomes easy to find bot binaries.

# Chapter 3

# Problem Statement

## 3.1 Problem Statement

Internet makes our life simple and easy. With this positive impact of internet usage, it also increases many cyber threats on Internet Security. Among the various malware Botnet is one of most dangerous attack on Cyber world. The reason behind choosing botnet as a famous weapon for cybercrimes is that, it easily hides attacker's identity, difficult to find command and control server, encryption of malicious traffic and hide itself with normal traffic. Complexity of Internet and its encrypted command and control server makes the Botnet very difficult to trace.

Huge spread of internet usage with E-commerce processes makes the attacker goals move from fun to financial gain. One of the most famous financial malware is Zeus Botnet whose main motive to steal banking accounts. Zeus is also called as king of botnet. Zeus code is freely available online and allowing access to its complicated design. One of the main reasons behind Zeus botnet becomes very popular is that design of Zeus botnet can easily avoid detection by security software.

As previous surveys carried out many researches has been done on botnet and its detection technique but no technique is complete accurate to detect botnet. As Zeus botnet is responsible for biggest attack on Internet security. One of the Internet security threat report indicates that US has 80% of infected traffic being part of their network and is mostly generated with Zeus botnet. In this thesis, Zeus botnet infection process is implemented on windows machines in virtual environment.

## Objectives

- To explore and analyze Network based detection techniques.
- To set up a bot on host machine in virtual Environment.
- Check the working of Zeus botnet and find a way how to detect this kind of malware.
- To analyze created Bot and highlighted its behavioral aspect.

# Chapter 4

# Design and Implementation

## 4.1 Experimental Environment

Any research experiment on malware must ensure that the malware or any malicious script as bot doesn't infect the real machine unintentionally. In case of failure, a huge implications on security and privacy of concerned people in real world. Virtual machines would be preferred because of its control and secure environment manner. So, VMware machine is used in this experimental setup.

### 4.1.1 Virtual Environment

The techniques of hiding the physical characteristics of system resources in a way with other systems, end users and applications communicate with those resources comes under virtualization.

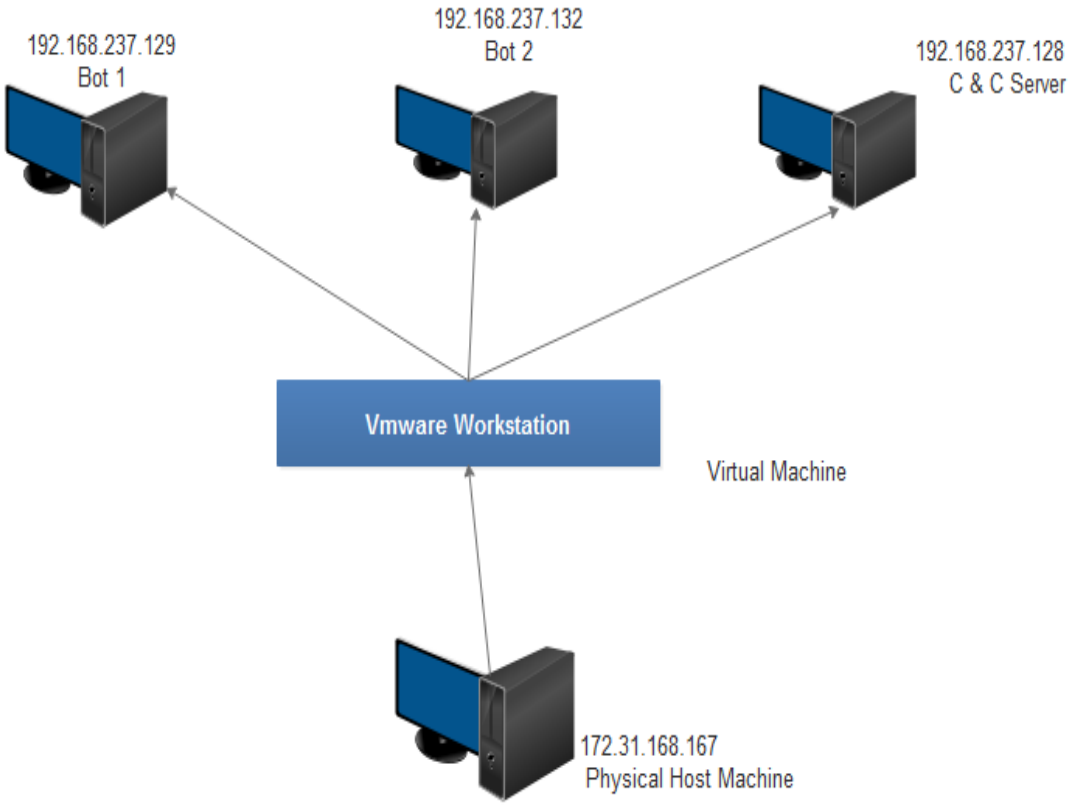



Figure 4.1 Virtual Environments in Host Machine

#### 4.1.1.1 VMware

VMware is a complete infrastructure virtualization suite that gives comprehensive virtualization, resource optimizations, application availability management and operational automation capabilities in an integrated offering. It gives the facility to create the multiple virtual machines in its infrastructure and also install their operation system from given .iso image or by using CD drive like other real machines.

For analyze the working of Zeus Botnet Toolkit and setup a complete Botnet architecture, VMware is used. It connects all windows machines in virtual environment so that all machines can easily communicate with each other and real host machine does not get infected with this malware. All virtual windows machine are isolated from the real host machine running VMware and internet.

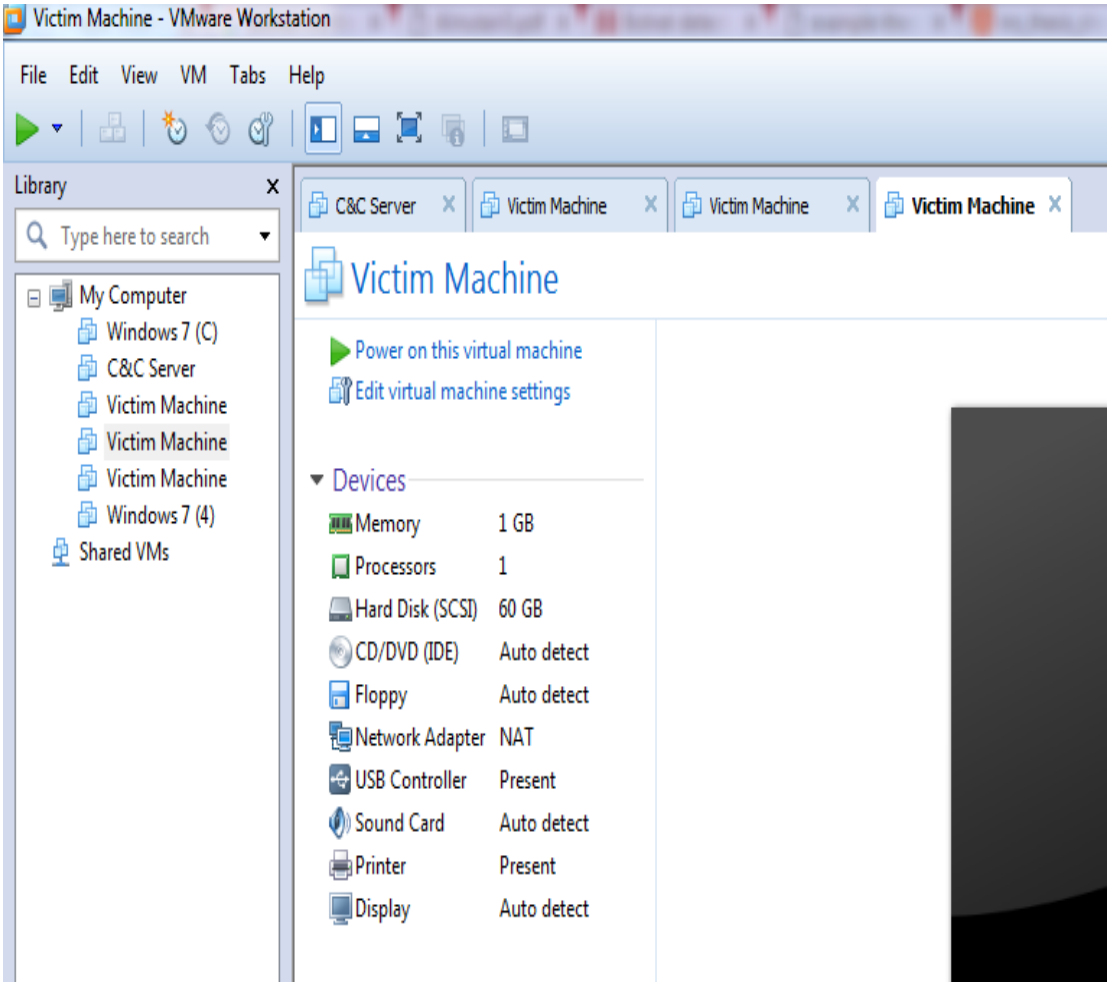



Figure 4.2VMware Workstation interface

### 4.1.1.2 Network Settings

In network adapter settings, there are options to choose the adapter setting as bridged where it acts as the real adapter of the physical host and another option is using NAT. This Zeus botnet analysis is done with using NAT settings on all virtual machines. NAT is a network address translation connection which is automatically done by follows the custom path in the new virtual machine wizard and select use network address translation.

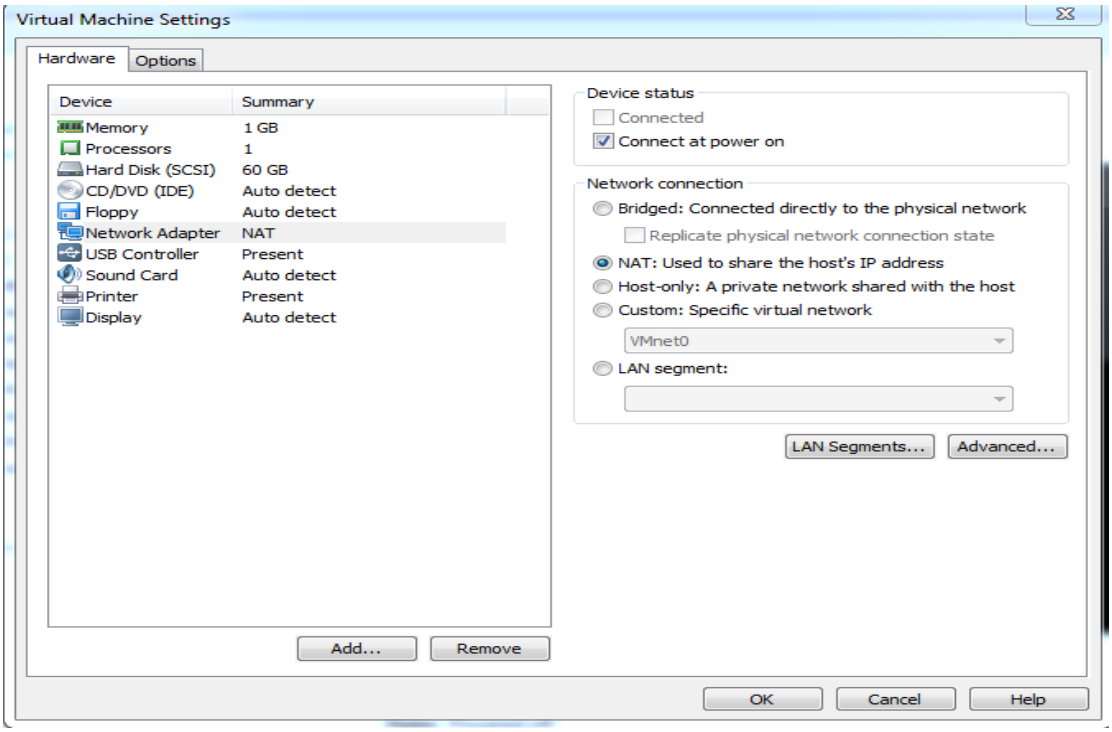



Figure 4.3 Network adapter setting

### 4.1.2 Wamp Server

Wamp server refers to a software stack for the MS windows operating system. It consists of the apache web browser, MySQL database, open SSL for SSL support and PHP Language. Wamp is a web server that also makes the windows machines to act as a web server and running the apache, PHP and MySQL.

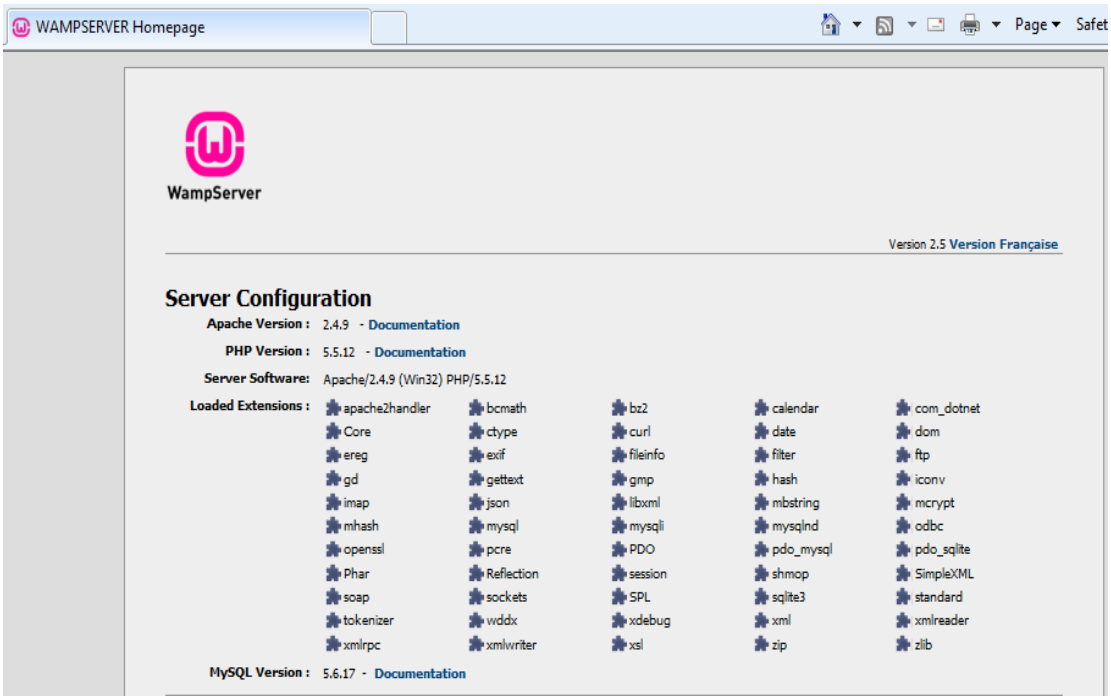



Figure 4.4 Server Configuration

Zeus Control Panel (CP) is developed in PHP and on backend it used MySQL. So here, Wamp server will be required to configure and host the Zeus control panel. Control Panel of Zeus toolkit is written in PHP with database "cpdb" using MySql on backend to perform its operations. Windows IIS (Internet Information Services) does not support PHP and MySql. Therefore, first step we need is to setup windows to act as a web server which is capable of hosting PHP and MySql. This could be done with the help of WAMP web server. It gives the facility of hosting PHP and MySql database in the windows environment. Before start installation of WAMP server in window machine, it is necessary to disable IIS. To check that, WAMP server is installed successfully in our machine, these addresses as "http://Localhost" and "http://Localhost/phpmyadmin" entered to check that local host and phpMyAdmin (main administration page for WAMP server) is accessible on our windows machine.

WAMP server menu option "www directory" displays the contents of directory in root directory of local host which contains index.php and testmysql.php. Index.php is the file which is used to display the home page of WAMP server and to test the connectivity with MySql, testmysql.php is used which is a small script file. To test the connectivity with MySql database, address "http://Localhost/testmysql"is used.

### 4.1.2.1 PHP Settings

PHP is a server site scripting designed for web development. It also used as a general-purpose programming Language. 'Personal Homepage' is originally stood for PHP. Wamp sever use phpMyAdmin as the main configuration page as shown in figure 4.2.1 and it also do configuration for apache and MySQL.

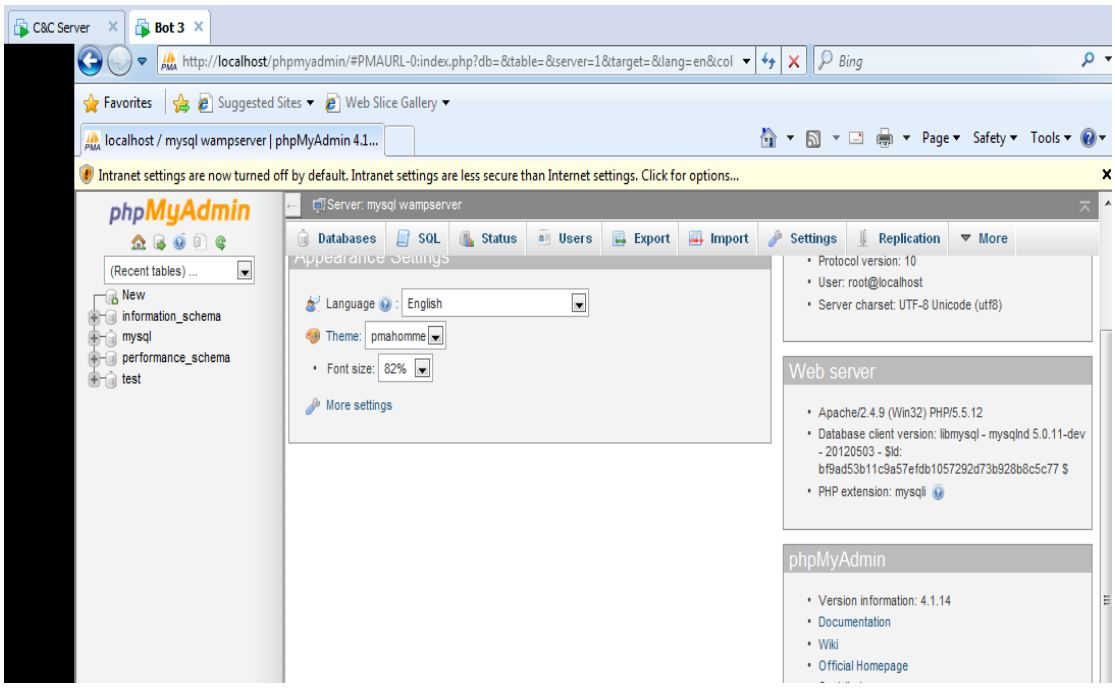



Figure 4.5 PHP settings

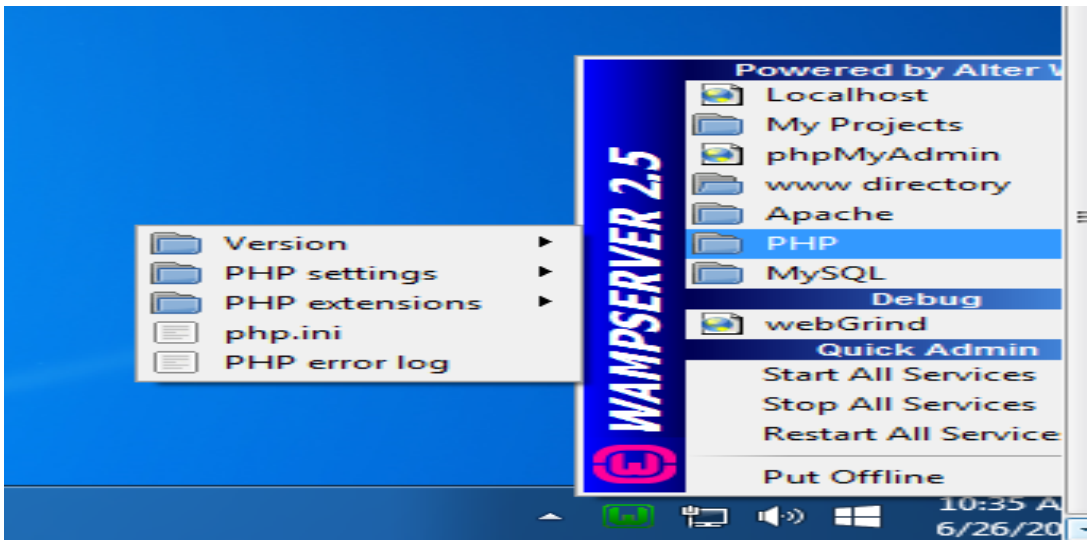



Figure 4.6 PHP Settings

### 4.1.2.2 MySQL

It is an open source relational database management system (RDBMS). It is a popular choice of database for web applications, and its main component of the widely used for open source web application software stack LAMP (and other "AMP" stacks)

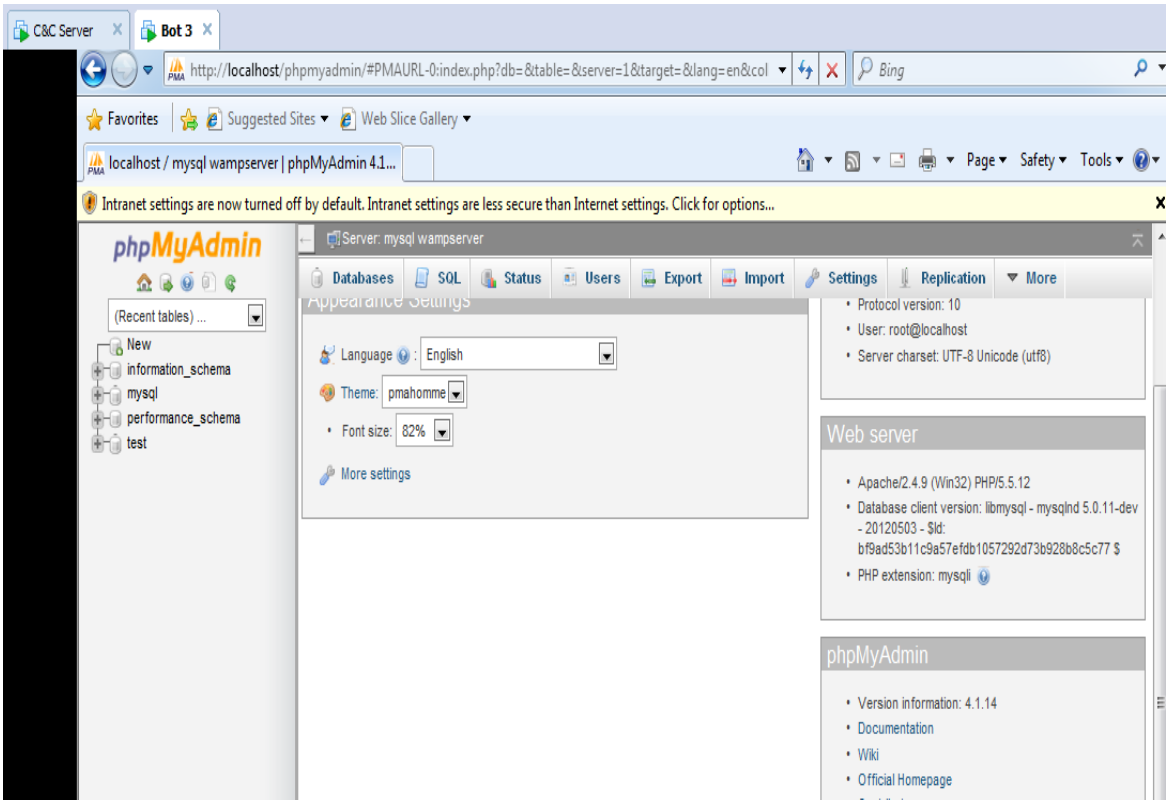



Figure 4.7 Database created in MySQL

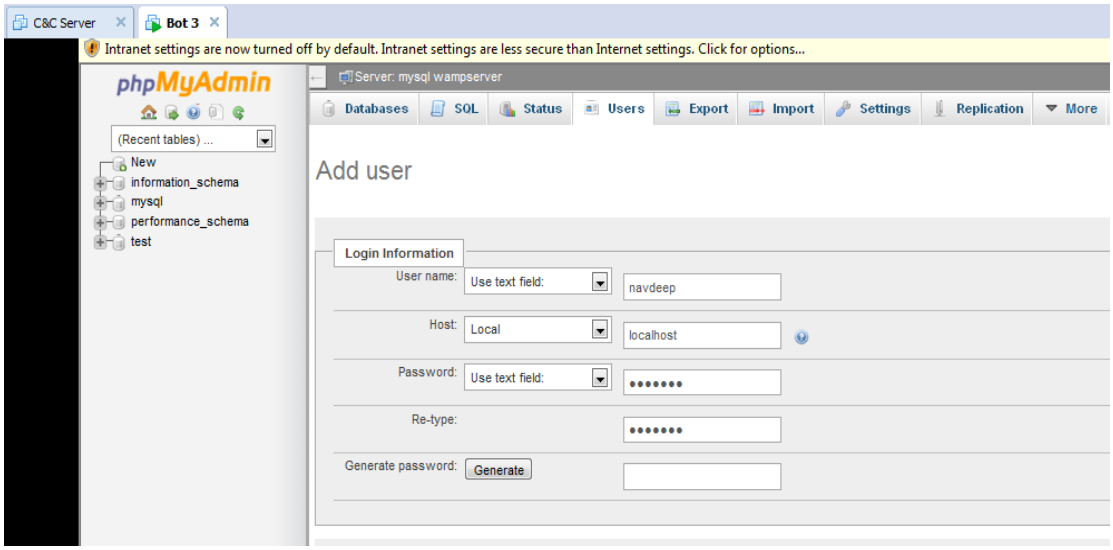



Figure 4.8 User created in database

#### 4.1.2.3 Apache Settings

Apache is HTTP based web server mostly used on Linux systems. Apache provides the multiple processing modules and also serves for many different websites with installation of single apache.

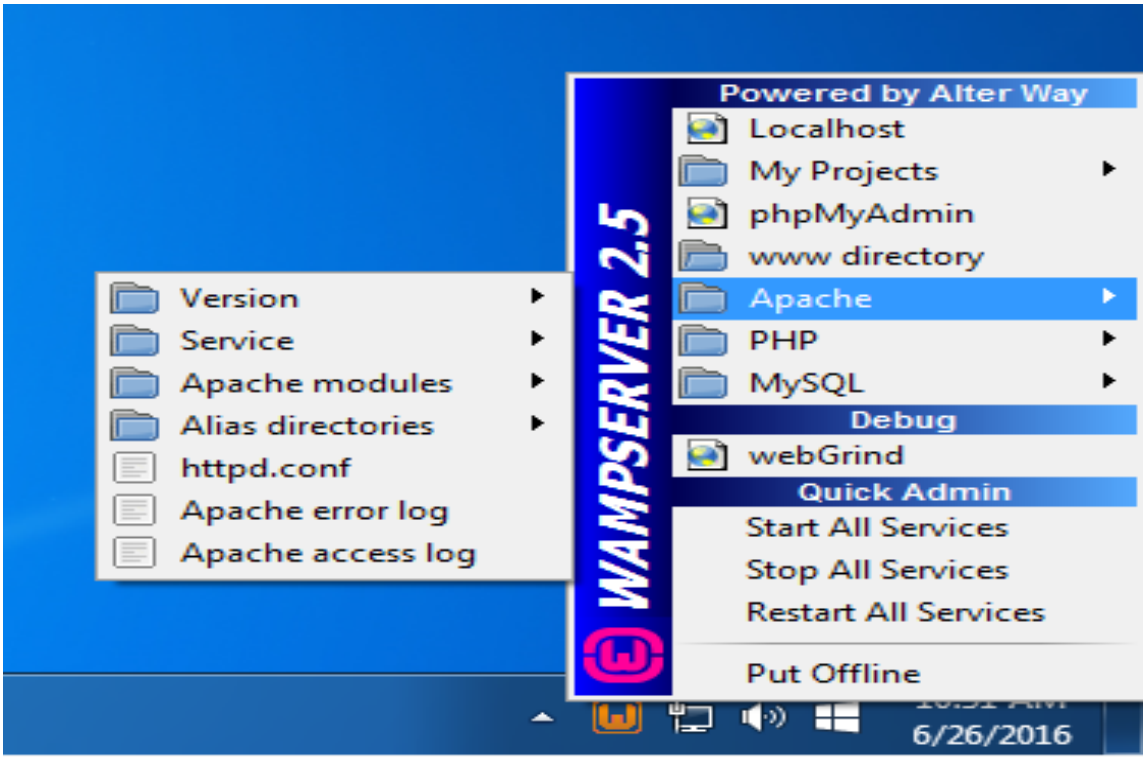



Figure 4.9 Apache Settings

## 4.2Zeus/Zbot Botnet

There are many types of botnets available on Internet. But from all these Zeus botnet has complete components required to analysis the botnet and its behavior. Zeus Botnet had leaked with its complete source code. So now Zeus toolkit is freely available on Internet. This toolkit has builder files to build bots and C&C server which is written PHP and MySQL on backend where all botnet activities and Login information of bots are stored.

### 4.2.1 Zeus Toolkit

ZeuS toolkit has two main Builder files. Configuration builder files have all files use for build a botnet and another is control panel (CP) files to create a command and control server.

#### 4.2.1.1 Configuration Builder tool

Zeus botnet is built with the configuration file as machine readable for .bin file generated by Zeus configuration builder. It involves the three files such as config.txt, .Zsb.exe and webinject.txt

- **Config.txt**

Config.txt is a text file fully named as configuration setting text file that contains the basic information and configuration setting. This file is used to generate the binary configuration file. It has basic setting such as name of botnet, List of bots and selects the time to send and receive commands.

```
;Build time:    15:06:54 14.04.2011 GMT
;Version:       2.0.8.9

entry "StaticConfig"
  ;botnet "btn1"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://localhost/config.bin"
  remove_certs 1
  disable_tcpserver 0
  encryption_key "secret key"
end

entry "DynamicConfig"
  url_loader "http://localhost/bot.exe"
  url_server "http://localhost/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"http://advdomain/cfg1.bin"
  end
  entry "WebFilters"
    "!*.microsoft.com/*"
    "!http://*myspace.com*"
    "https://www.gruposantander.es/*"
    "!http://*odnoklassniki.ru/*"
    "!http://vkontakte.ru/*"
    "@*/login.osmp.ru/*"
    "@*/atl.osmp.ru/*"
  end
  entry "WebDataFilters"
    ;"http://mail.rambler.ru/*" "passw;login"
  end
  entry "WebFakes"
    ;"http://www.google.com" "http://www.yahoo.com" "GP" "" ""
  end
end
```

Figure 4.10 configuration Builder Config.txt code

Config.txt has many sections started with “entry” and end with keyword “End”. This config.txt file has advanced and dynamic entry list of URL from where all configuration file can be downloaded such as bot.exe, gate.php and webiject.txt. Advanced settings have alternative URL for downloading the backup configuration files. Some main parameters in this configuration settings files are as

- **Staticconfig**

It is the basic static configuration setting file which is used to execute the bot at first time. In this section basic bot settings are involved as Botnet parameters, Time interval for working of botnet like Timer, config parameters, Timer_log parameters.

There are some other parameters as url_config parameters specifies the URL to download the dynamic configuration, encryption key parameters shows the key which is used to encrypt the information and blacklist_Language parameter which specifies the language code used by botmaster to communicate with all bots and C&C server.

- **Dynamic config**

Dynamic configuration is a second step done by bot. After complete the installation of bot, it automatically download the dynamic config settings in victim computer in specific time interval mention in static configuration entry parameter. It has the main information related to working of botnet as a method will be used by botnet to collect the data from victim computers and how it will be sent to C&C server.

Dynamic configuration files have various parameters in it as url_loader to load the files, url_server where bot can upload the files in it. File_webinjects have the list of websites addresses where additional data to be upload.

Config file also has entry web filters used to specify the URL masks to find the correct website and prevent logging at the given URL.

#### 4.2.1.2 Webinject.txt

Web inject text file is used to inject the webpages from official websites by adding some additional parameters in it which are not design in real web page. This file is used to collect more information from infected pages. This web inject file does not give any impact on that web link as URL will remain same. It only add some new parameters so it looks like a genuine web page and users can trust it and put information in all the parameters that is collected by botmaster when users entered. Botmaster can add any number of parameters to collect the information about infected pages. It is difficult to differentiate the real parameters from fake parameters added by botmaster.

Webinject.txt has some following parameters as

**Set_url parameter** which gives the information about the web address format or full address of victim machines that to be attacked.

**Data_before parameter** gives the information about entry point that is used to start the inject web page.

**Data_inject parameter:** This parameter has the actual data that is needed to inject the web page.

#### 4.2.1.3 Zsb.exe

Zeus configuration builder executable is actual software that has GUI interface with tab information, Builder and Zeus botnet settings and License. Where License files gives the information related to Zeus botnet license needed for the builder.

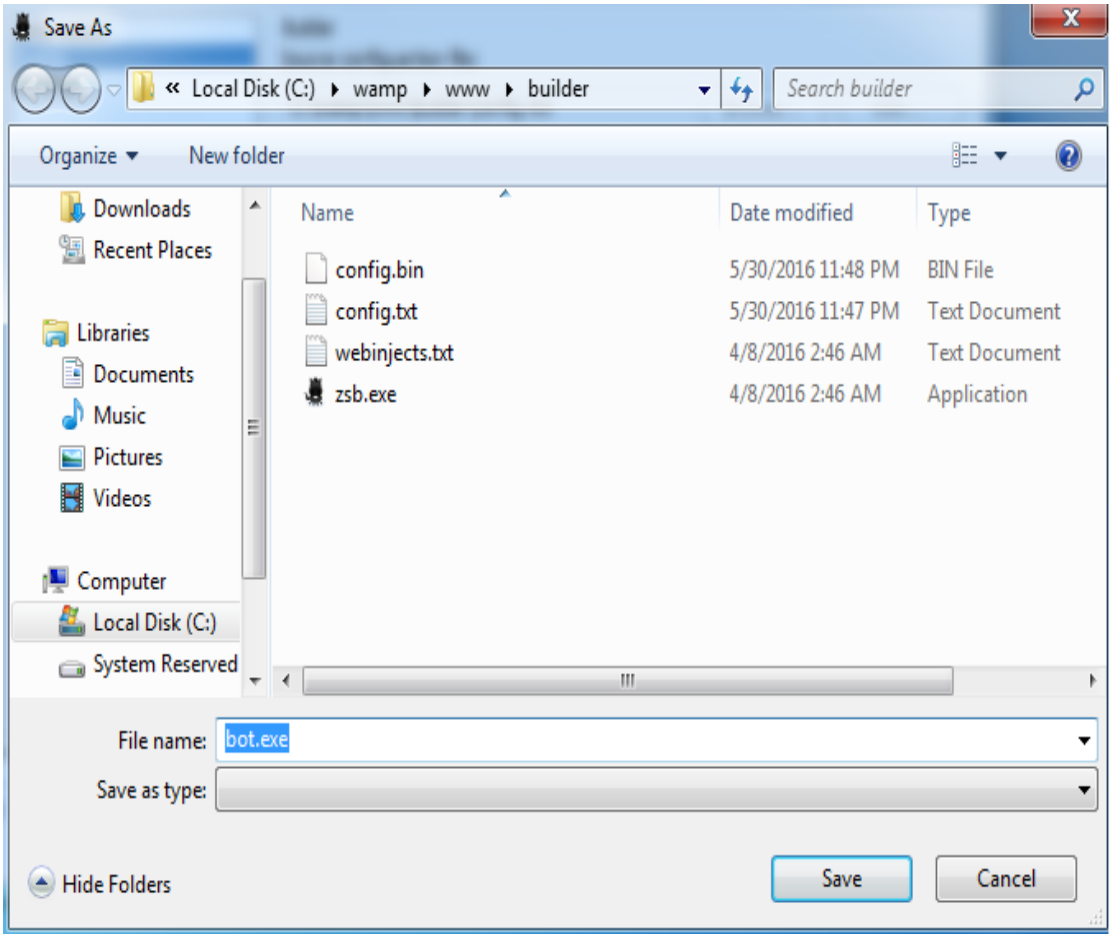



Figure 4.11 Bot.exe generated by zsb.exe

This folder also gives the option to choose the language in which botnet will communicate as English or other languages. This file also contains the bot removal utility where it has remove bot option to delete the bot from list.

Zeus builder needs to put encryption key to build a bot which is specified in config.bin. Command and control server sends same key to all bots to communicate with encrypted messages. This key is send in configuration setting file and also used for encrypt and decrypt the bot binary file generated the Zeus builder as binary (.bin).

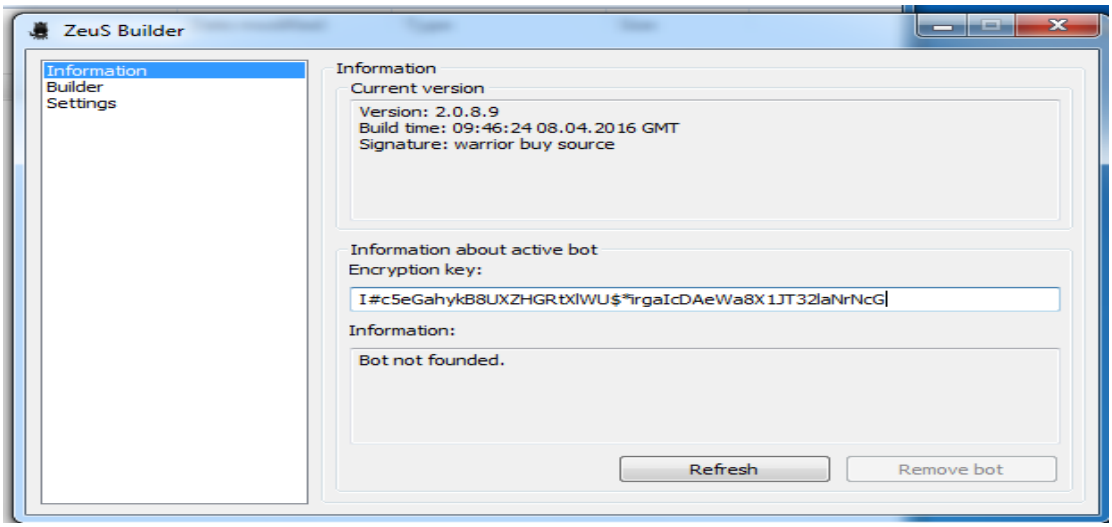
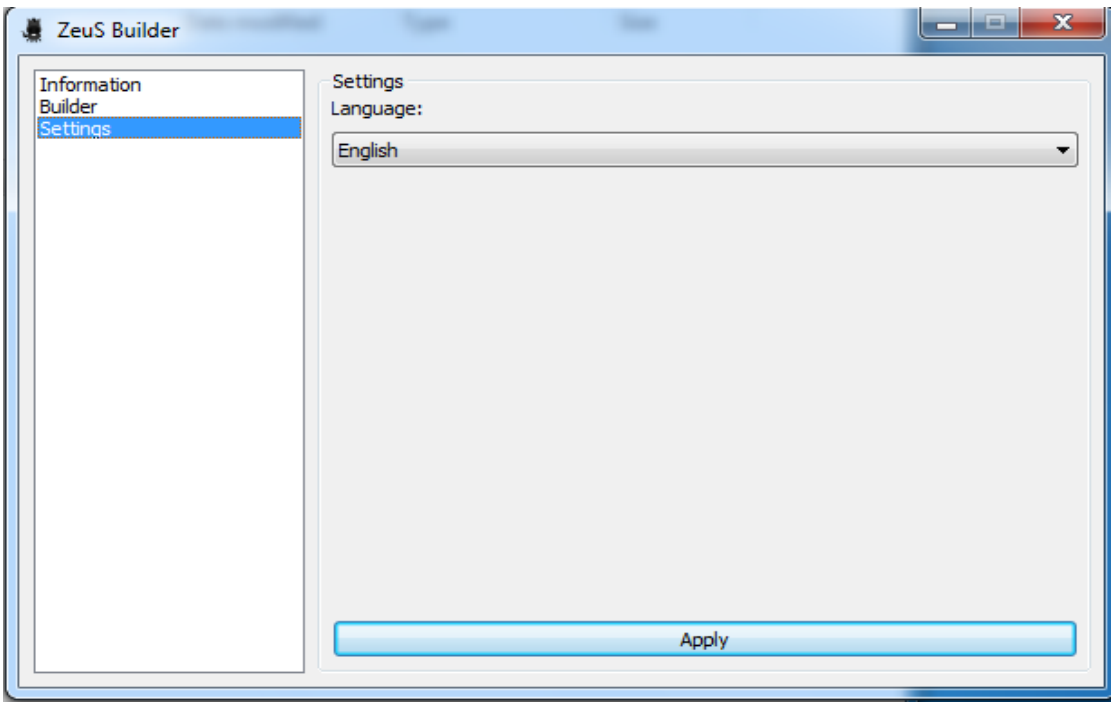



Figure 4.12 Zeus Builder information option




. Figure 4.13 Zeus Builder Settings

### 4.2.2 Zeus Builder

Zeus builder has information tab which gives the all information about botnet as current version of botnet and gives information about active bot. This tab determine that bot is successfully installed or not. Second tab is builder tab which is used to build a new bot with using configuration files as specified in config.txt which generate the binary interface as .bin file.

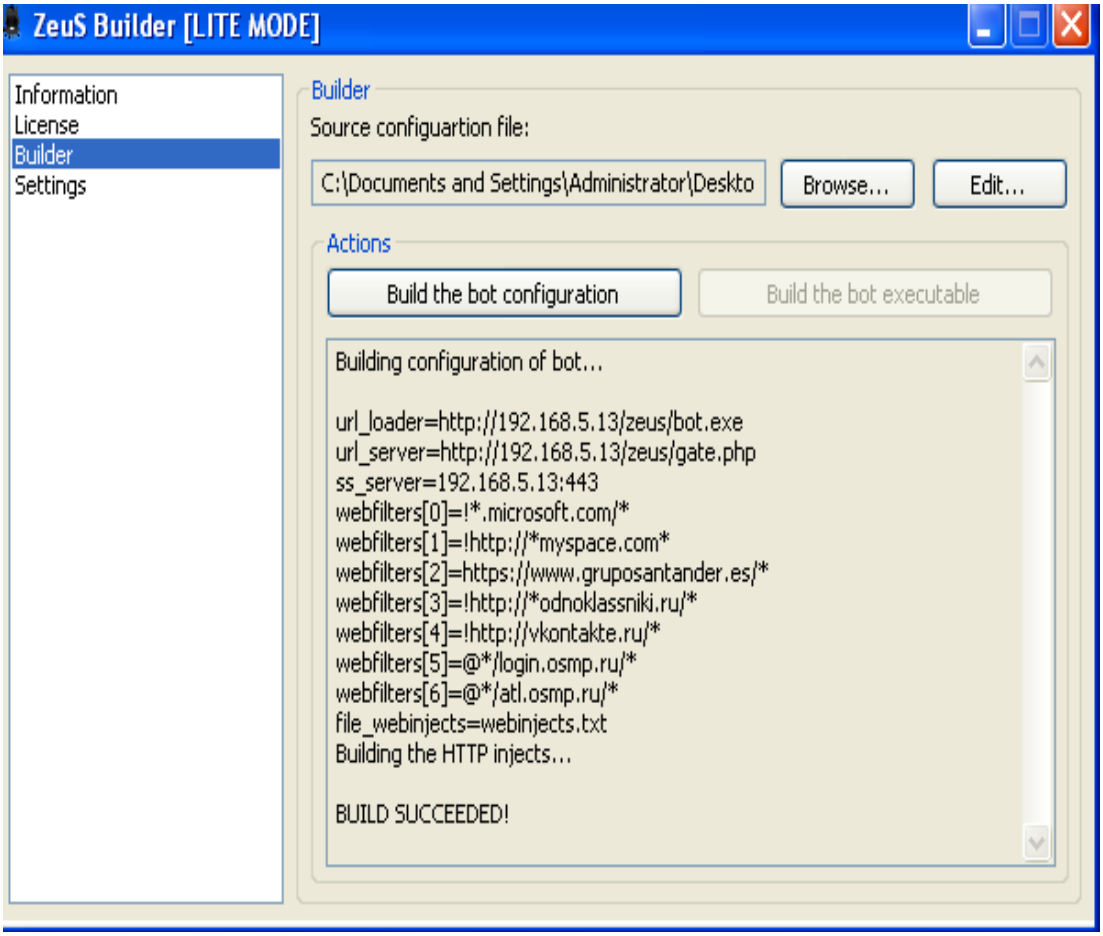



Figure 4.14 Zeus Configuration Builder

### 4.2.3 Control Panel (CP)

Zeus control panel is installed after complete installation of Wamp server. First step is to copy the control panel files in WWW directory as shown in figure 4.14

Cp.php is the main file that is created the main page of control panel that can be access by entering the URL address as “http://Localhost/cp.php”. Just by entering the address, it displays the message as “how are you?” means control panel files are copied successfully into wamp and ready for installation.

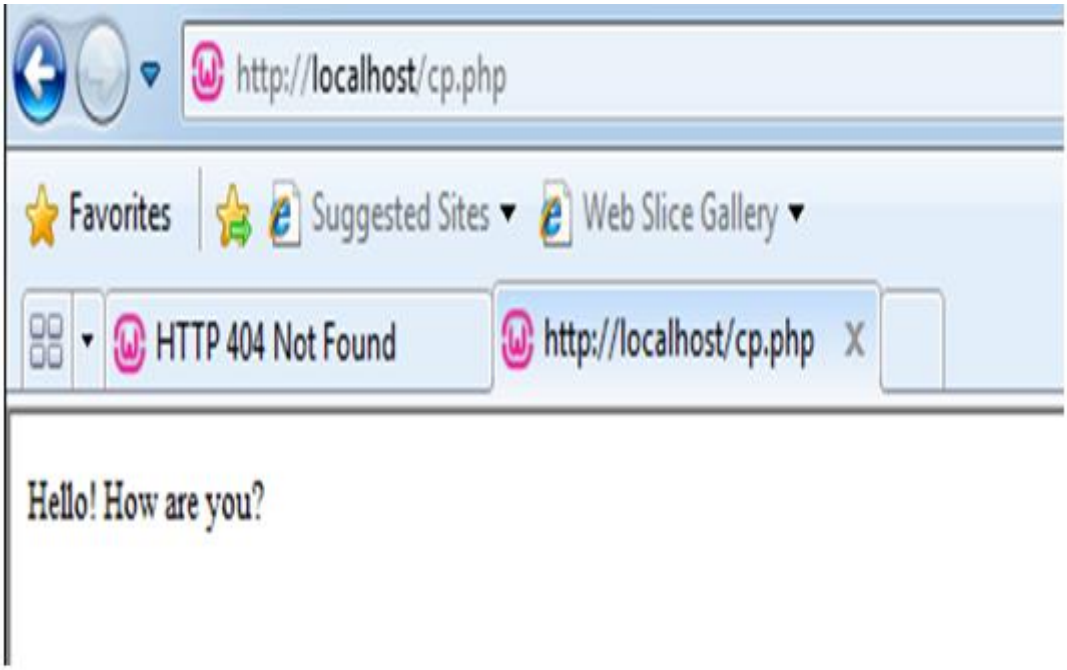



Figure 4.15 Wamp Server ready for installation

This indicates that control panel (CP) is successfully copied into the WWW directory. To start installation of Zeus botnet, it needs to access the "index.php" which is stored in "install" folder from local host. To access this file type the URL as "http://Localhost/www/install" in address bar as shown in figure 4.15 Index.php file shows the steps to start the installation.

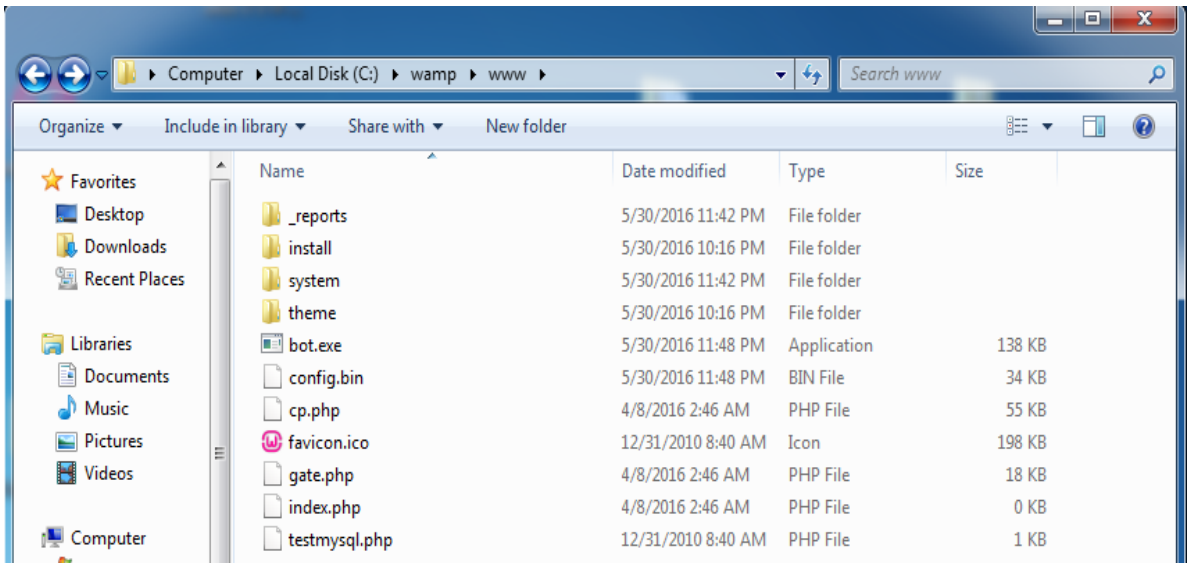



Figure 4.16 Zeus Control Panel Files

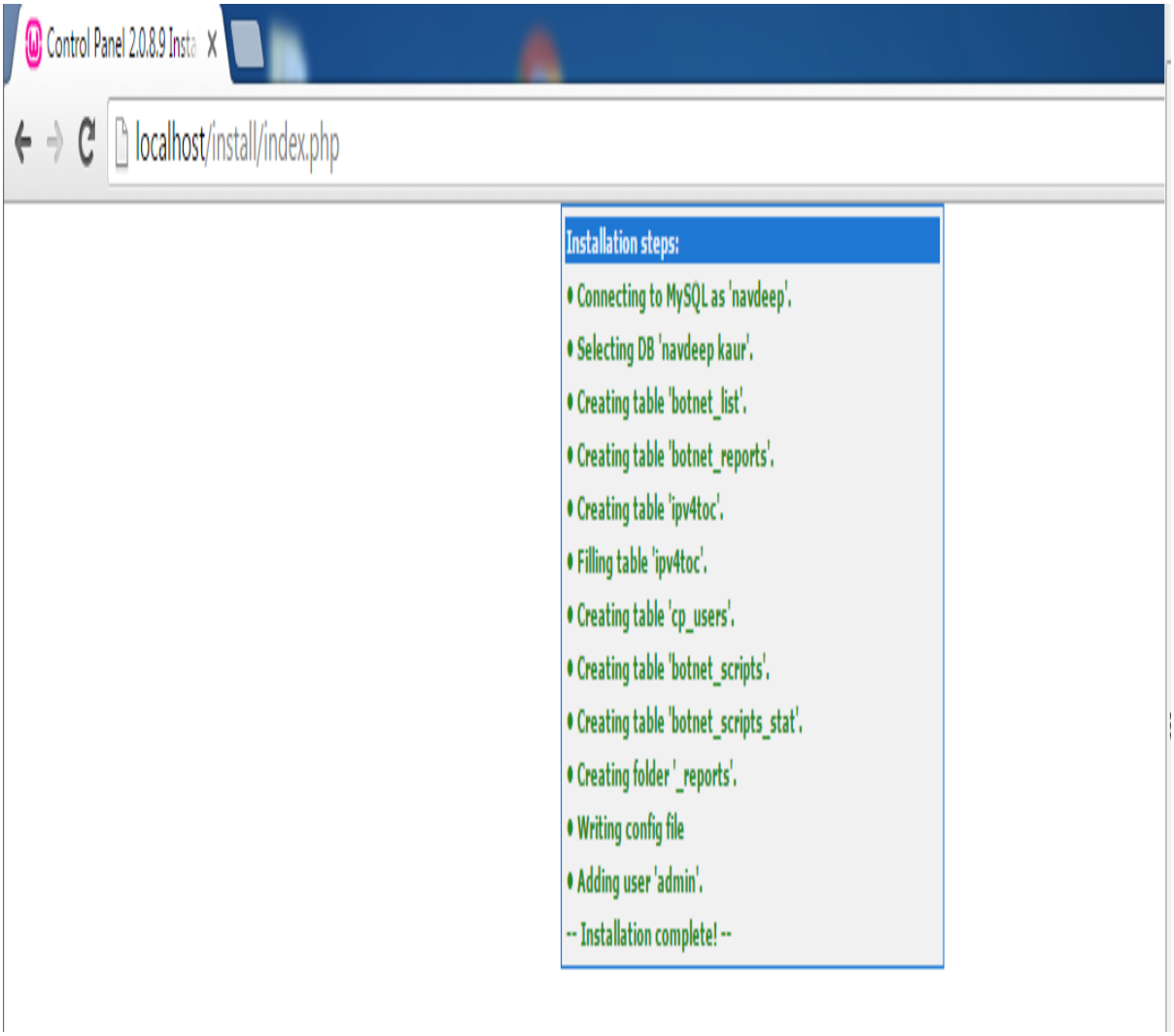



Figure 4.17 Steps for control panel installation

By aceesing the install folder with url "Localhost/install" it shows the main page for control panel installer as shown in figure 4.17. In this page, it require the information about username and password which is created in wamp server using phpmyadmin as username is "admin" and password. This username and password will be used to login into botnet as adminstrator. Username and Database created in MySql server is also required to fill in this page where information about all bots will be stored.

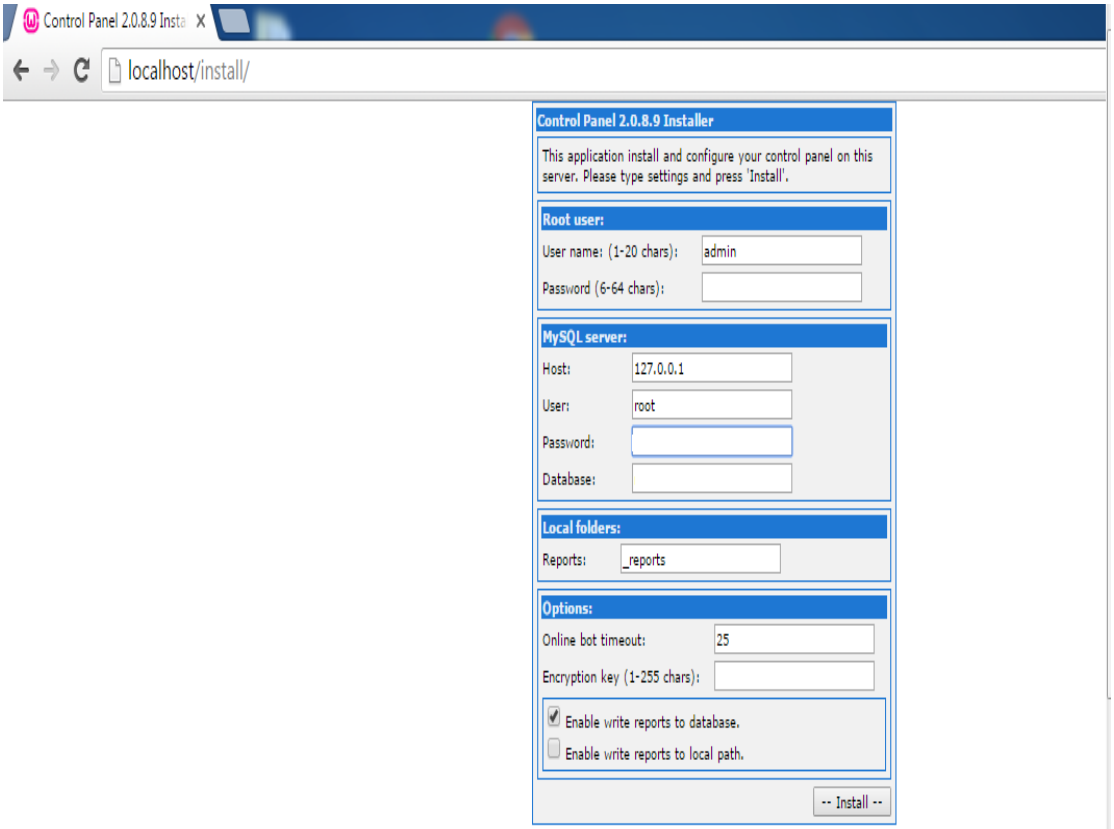



Figure 4.18 Control Panel installer

In Figure 4.18 shows the control panel installer. This page also require a encyption key that is specified in the config.txt file. This encryption key is used to encrypt the bot file as binary (.bin) using configuration settings. By pressing the install button after entering all details it intiate the installation of botnet.

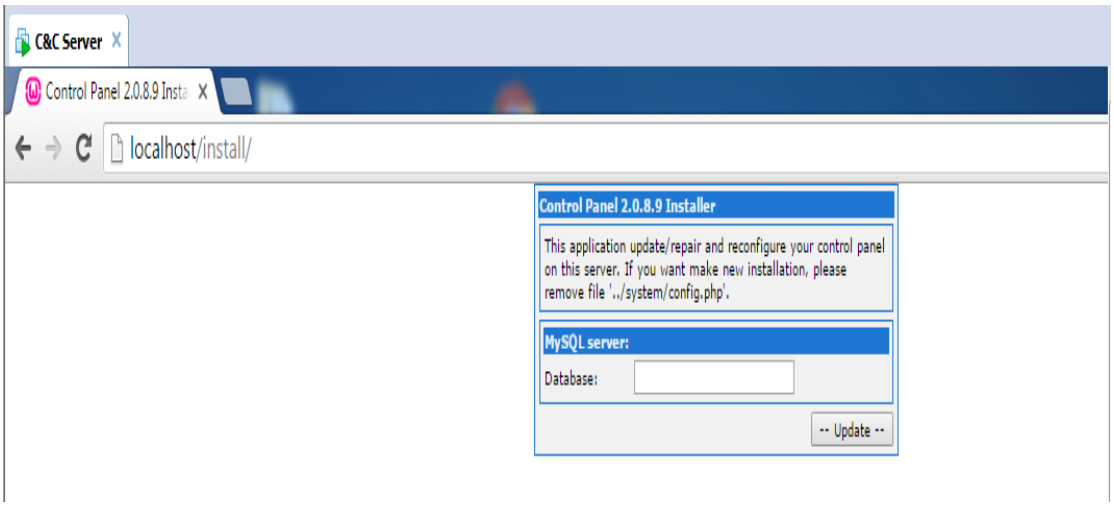



Figure 4.19 CP Installer Database

### 4.2.4 Bot/Infected Computer Set up

There are two another running window 7 machines in VMware which are used to infect and treat as a bot in botnet. Bots are to be generated by bot.exe and executed on these windows machines. Config.txt file settings are done to enable these bots machines to access command and control server on IP address 192.168.237.128. Bot.exe can send by using different social engineering methods as spam, email attachment, infect legitimate website etc.

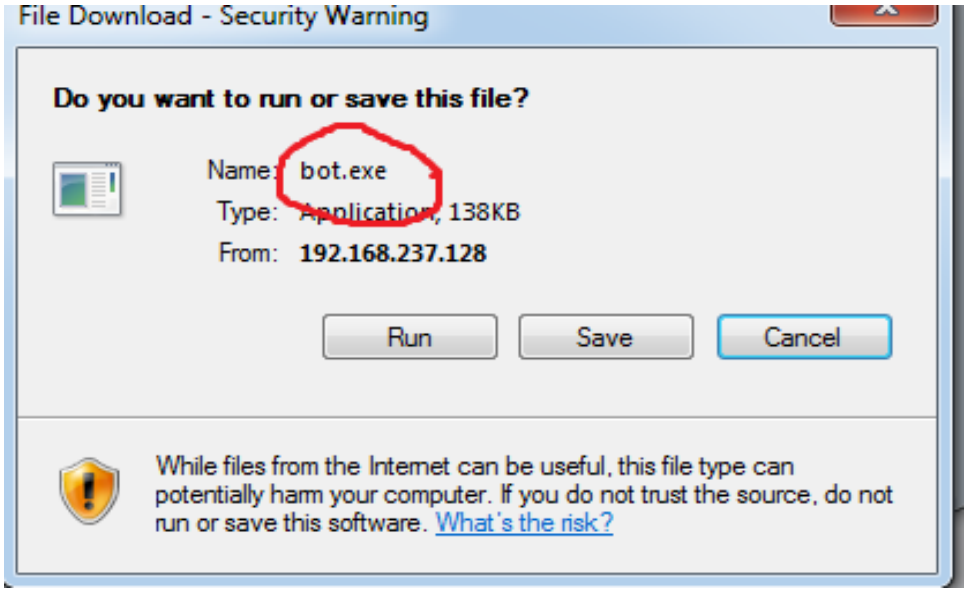



Fig.4.20 Downloaded bot.exe file

User can download this Bot.exe file from any infected website or software.Bot.exe file hide itself after run in victim machine.

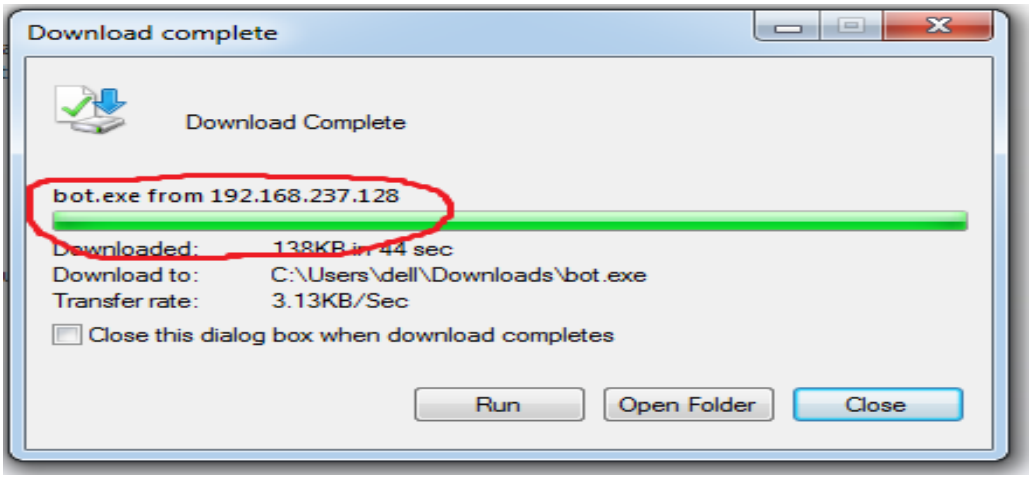



Fig. 4.21 downloads bot.exe from C&C server (192.168.237.128)

On victim machine which act as a bot/ infected machine following tools are installed for analysis the behavior of bot.

**Wireshark:** It is used to capture the traffic generated by bot machine to communicate with command and control server. It shows the communication between bots and C&C server also helps to find their location with the help of IP addresses of those infected machine.

**Process Monitor:** Procmon is an advanced monitoring tool for windows which is used to monitor the behavior of machine during bot building and execution. It is used to check the .dlls files form window32 which are also involved when bot configuration settings are installed in victim machine.

**Olly debugger:** It is used for binary code analysis to check the time stamp of bot activities and it is useful if source is not available.

### 4.3 Working of Zeus Botnet

When installation of Zeus botnet is completed it display the login screen in link localhost/cp.php. To test the working of botnet needs to enter the username and password given in installation time. By pressing the submit button it will show the main page of control panel. Which shows that botnet is successfully executed in local machine (192.168.237.128).

Control pannel of botnet have detail of all bots connected with command and control server such as unmber of bots, Time of fisst activity, Active bots, Versions of bots etc. The Main page of control pannel has summary statistics and following important options

**Information:** first option is information which display the basic information as name of owner of botnet, date and time of current botnet activition.

**Statistics:** This option has the summery option that displays the informations about total reports of bots stored in database, Bot activity time, Number of bots . Total active bot in 24 hours.

**Botnet:** Display the detail of all bots in botnet and having two options as bot and script. In bot page it has option to search the bots. By chosing the bot and pressing the

“Full information” it display the complete information about bot as bo id, botnet name,operting sytem on which that bot is installed, IP address, Bot activation time etc.

Another option is script which is used to create the script that is used to sent the commands to bots in botnet . This script could be used single or multiple commands that are stored in “context” field of botnet .

**Reports:** This options display the details of bot activites like by clicking on search in database it give option to chose the bot then it displty the all acticites done on that infected machine which is used to collect the information from owner’s activities , Search in files shows the iformation stored in files send by bots in botnet.

**System:** This option have basic information as users in botnet, Users of botnet as botmaster name etc.

**Logout:** this option is used for close the contol panel and exit from the botnet.

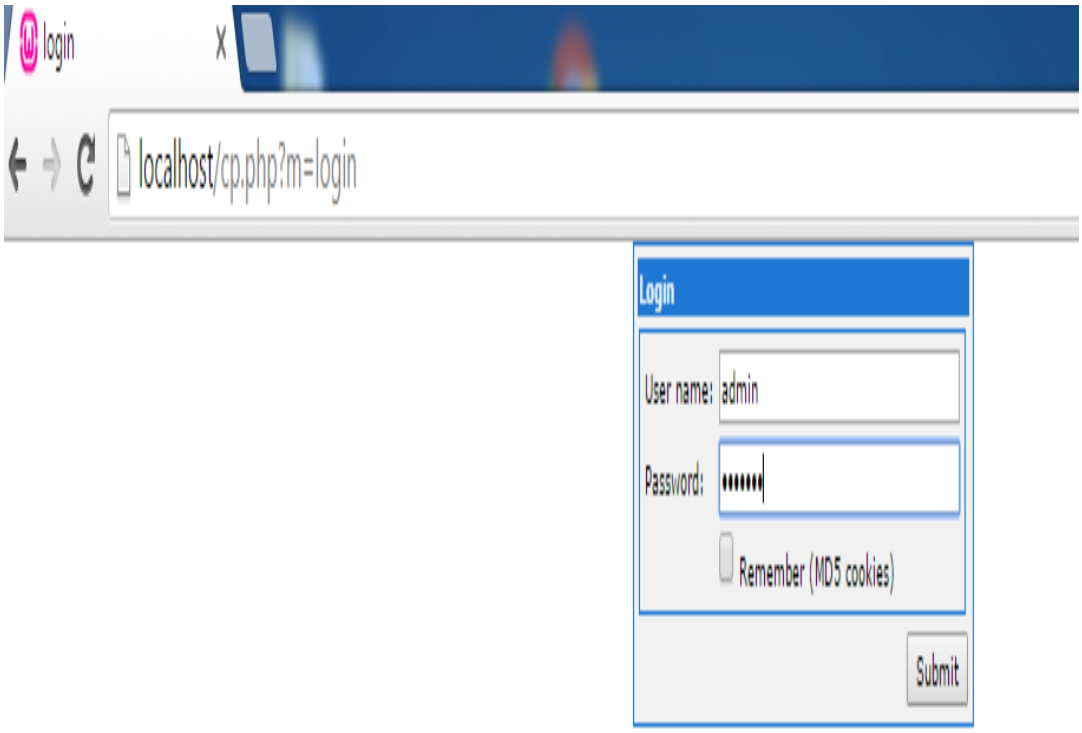



Figure 4.22 Zeus Botnet Login Page

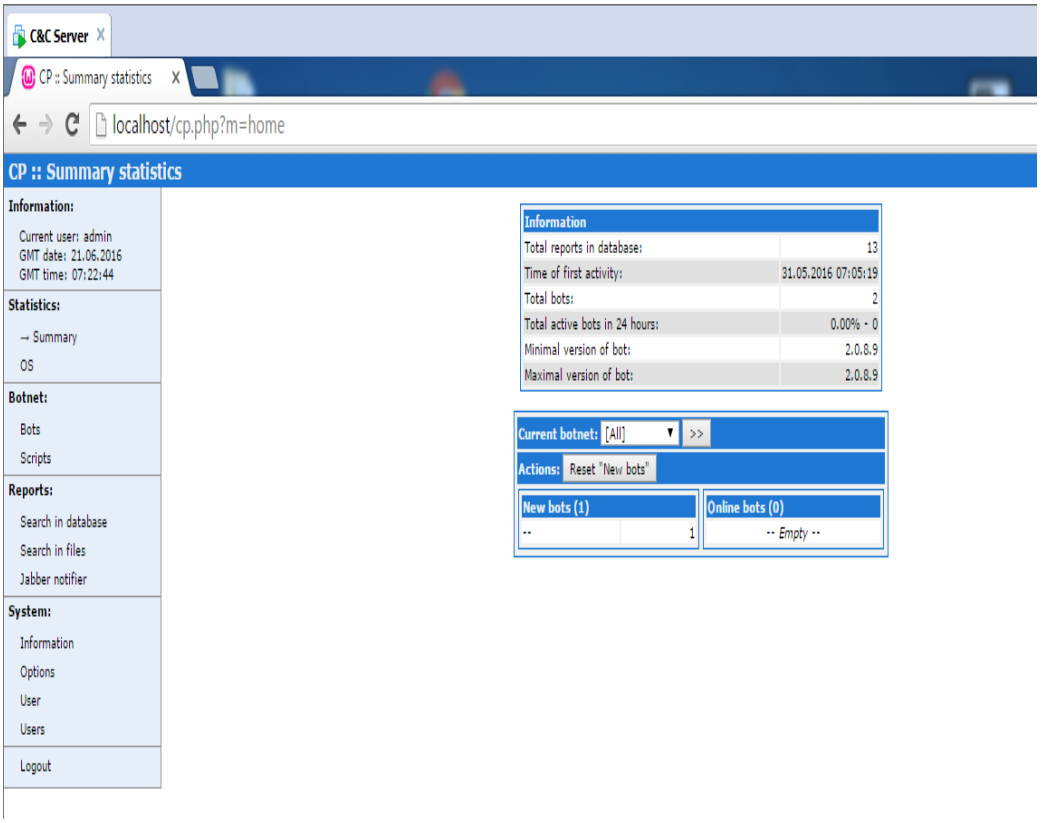



Figure 4.23 Botnet Summery

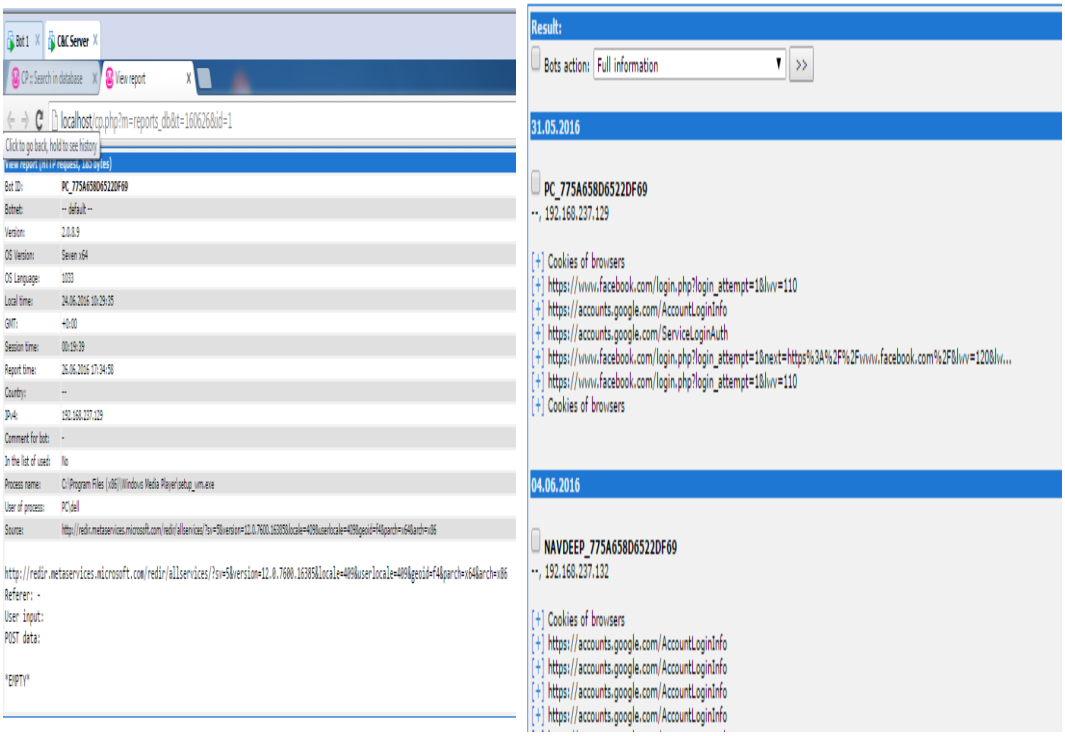



Figure 4.24 Information stored in Control panel

### 4.3.1 Social Web Sites Attacks

Bots send the information captured from victim machines to botnet which are stored in database as shown in figure 4.24. There are some examples of social websites attacks users Gmail, Facebook username and password is stored in this database send by bot in botnet. Banking information as user account number, pin code etc. and other confidential information is stored by bots and send reports to botmaster.

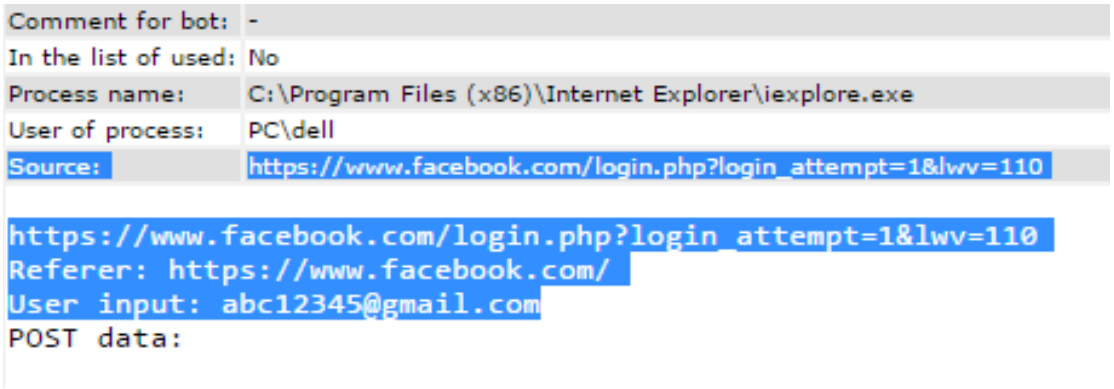



Figure 4.25 Facebook password stored in C&C server

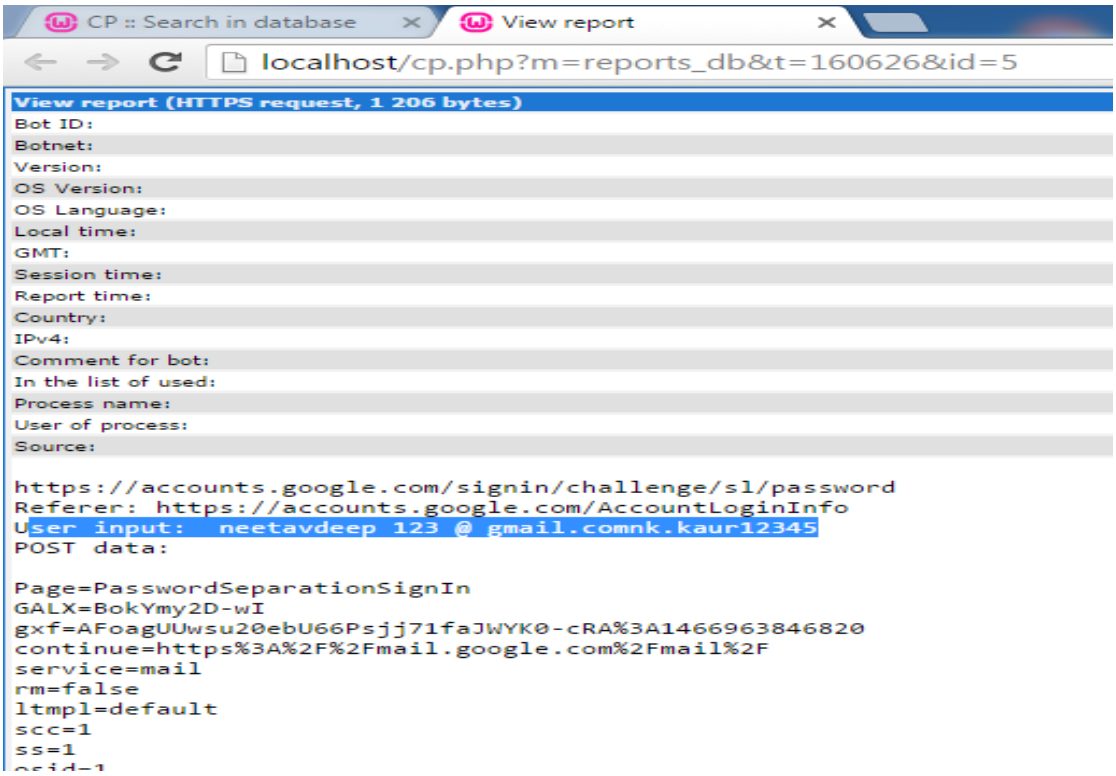



Figure 4.26 Gmail password saved in C&C server

### 4.3.2 Banking Information

Information about user account number, Email id are stored in files by bot and send to the command and control server as shown in figure 4.27.

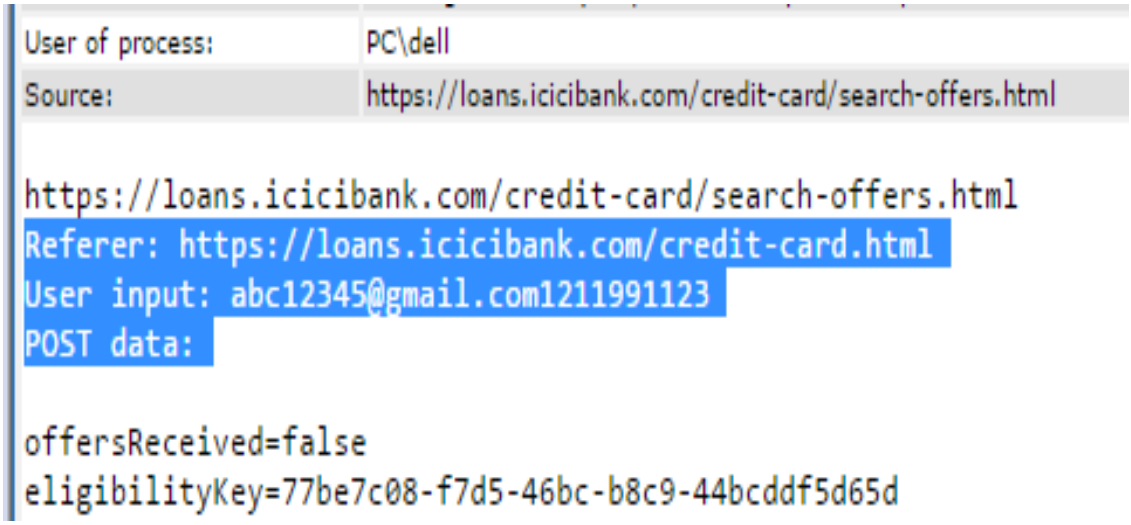



Figure 4.27 Credit Card information stored IN C&C server

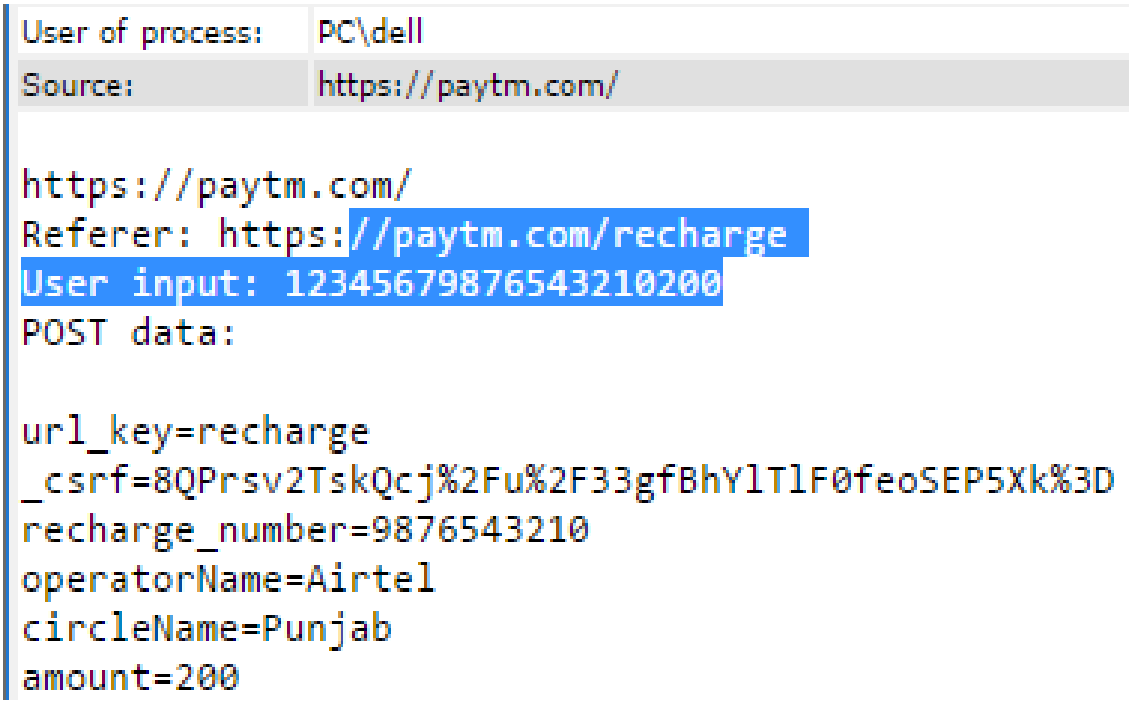



Figure 4.28 Information stored from Paytm.com

## 4.4 Network Analysis Tool

### 4.4.1 Wireshark

Wireshark is a free and open source packet sniffer. It captures the packets with pcap. Wireshark uses different colors such as red, green, blue and black to identify the specific types of traffic. It is divided into five different parts starting as capture menu which has pull down menus with different basic options as save and choose the capture interface etc. Second display filter specification bar is the main layer which defines the captured packets interface, protocols used by packets such as TCP, HTTP and UDP etc. Third layer is packet listing window which defines the information about packet such as packet numbers, source address, destination address time, protocol and flag used for communication. At fourth part, it defines the packet header details by selecting any packet from list of captured packet. It shows the information in details as source IP address, destination IP address destination MAC address etc. In last layer it defines the packet contents in ASCII and hexadecimal from.

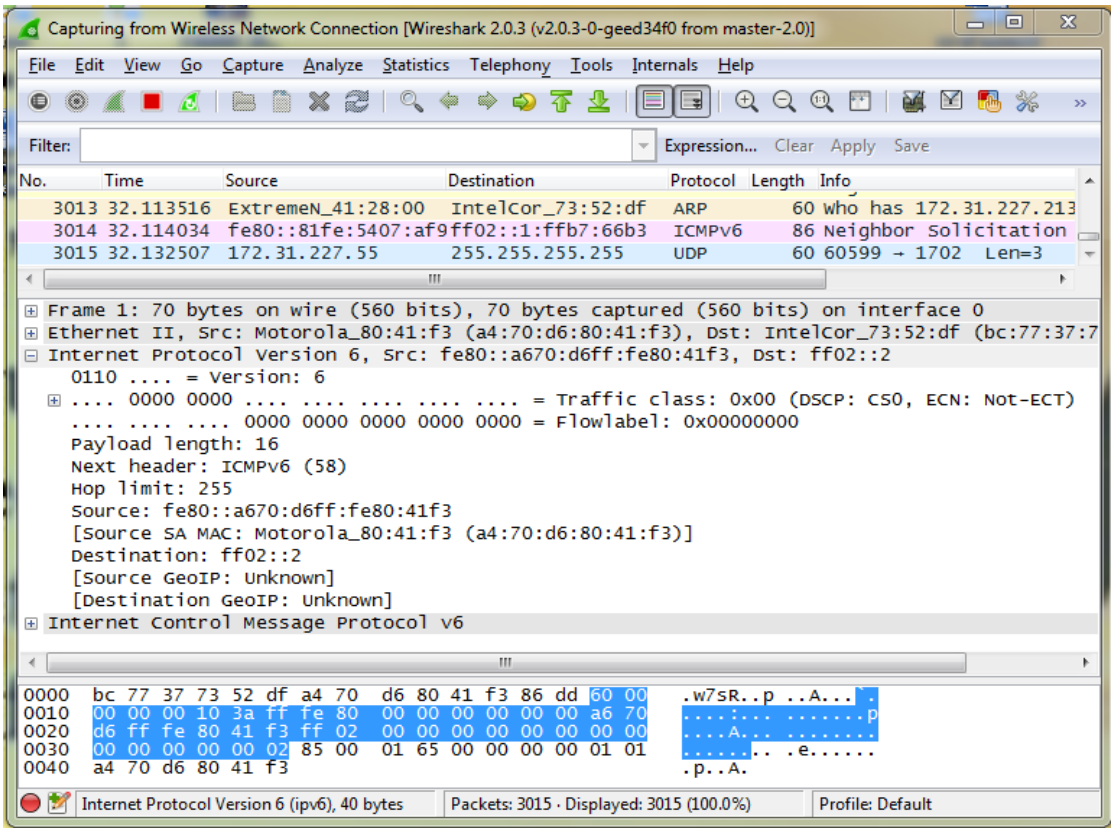



Figure 4.29 Wireshark Interface

In this Zeus Botnet analysis Wireshark is used to capture the network traffic between different bots and Command and control server.

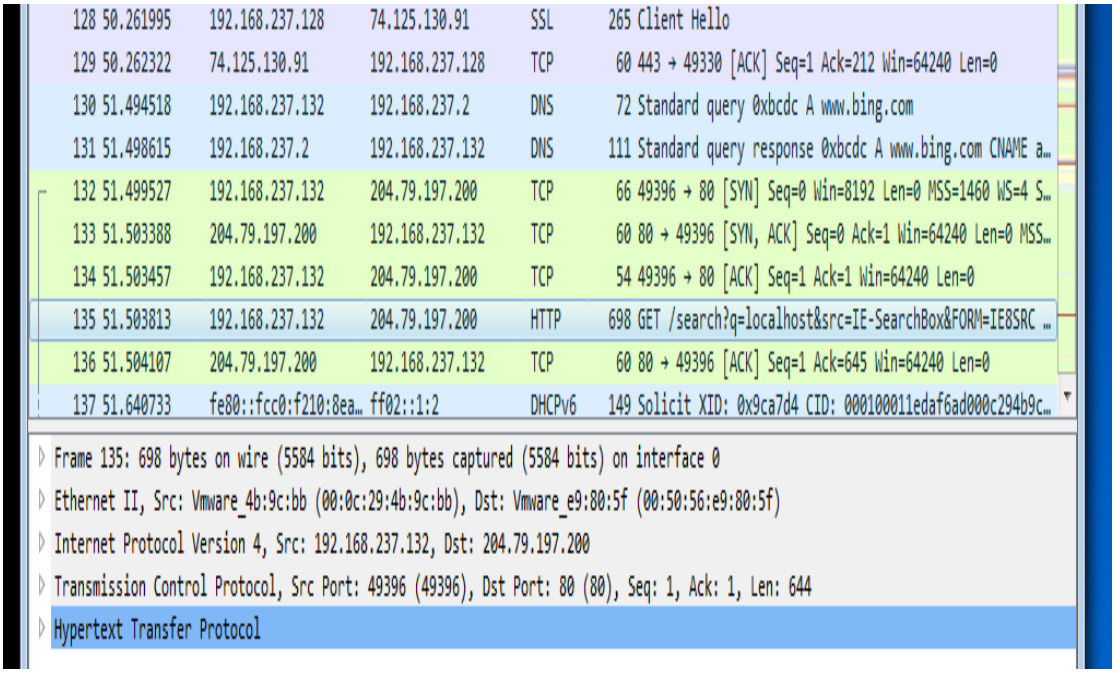



Figure 4.30 Connection with Local host

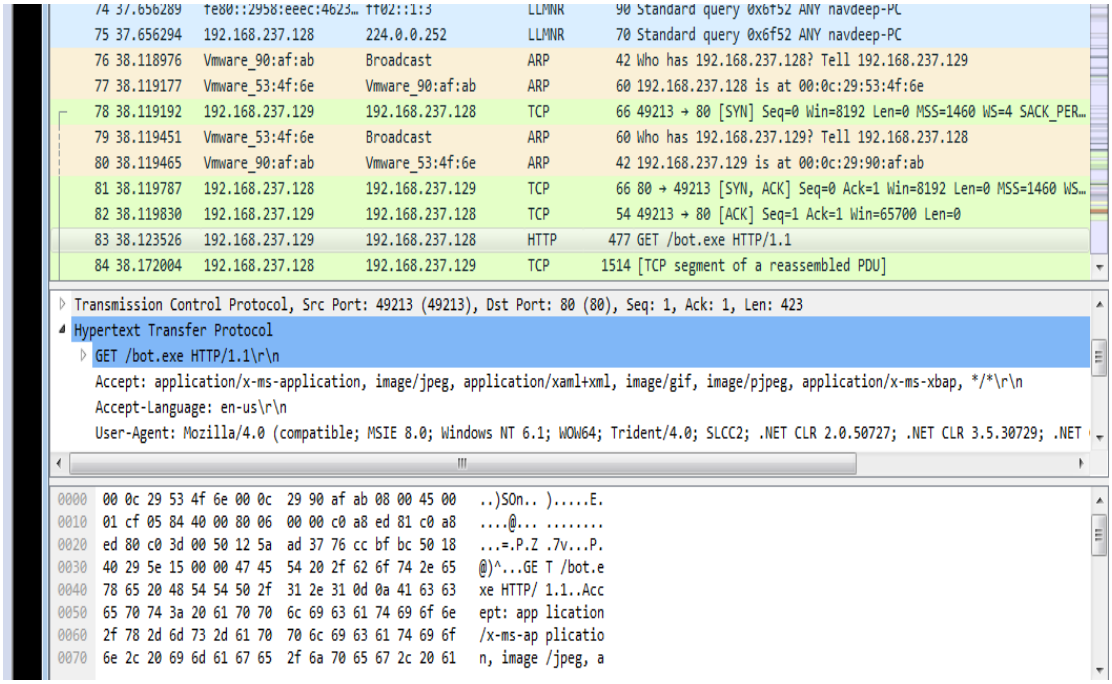



Figure 4.31 Installing Bot

Data captured during execution of bot.exe shows that bot following three way hand shake with command and server.

Configuration file as config.bin is sent by command and control server to bot machine after downloaded the bot.exe to install configuration of bot. Config.bin has also encryption key in it to encrypt/ decrypt the bot file.

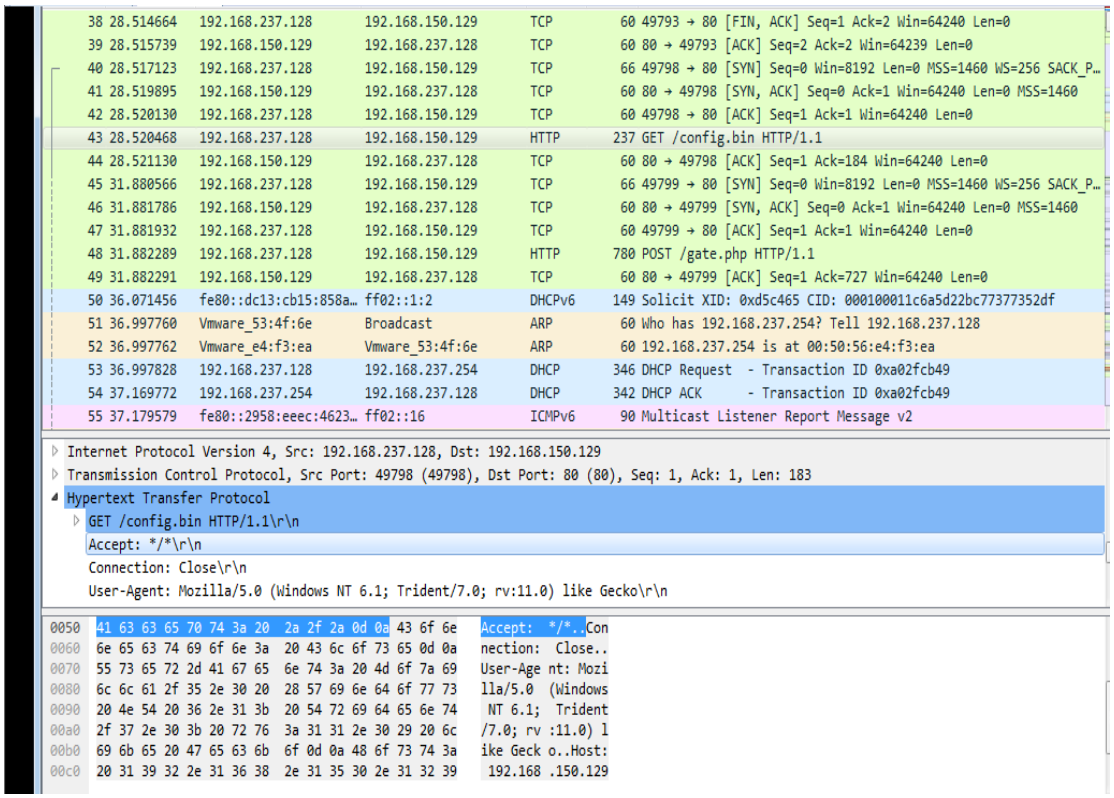



Figure 4.32 Bot GET / config.bin request packet sent to Control Panel

After using Get/Config.bin, configuration file has been downloaded and decrypted by the key which is written in bot itself. Downloaded bot.exe with any email attachment or from any website can installs and updates itself with any permission given by owner of machine. The main feature of this bot is hiding itself after downloaded and starts its operation without showing any activity to owner. Second step is send the collected information to command and control server. For this POST method is used to send the information as a parameter to gate.php.

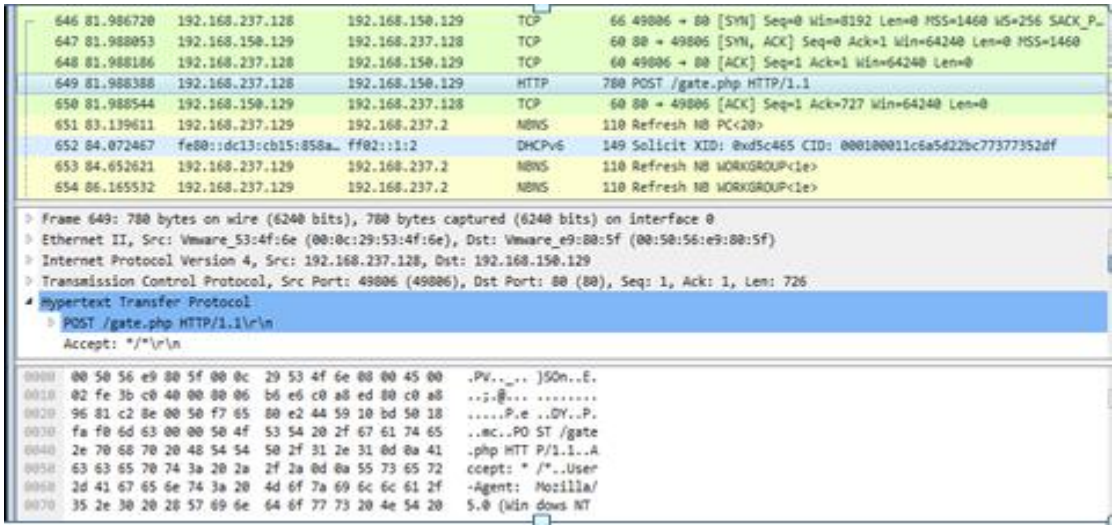



Figure 4.33 post/gate.php packet sent to control panel

Packet captured by Wireshark in fig 4.34 shows the POST/gate.php function is used to send the information by bot machine to command and control server controlled by botmaster.

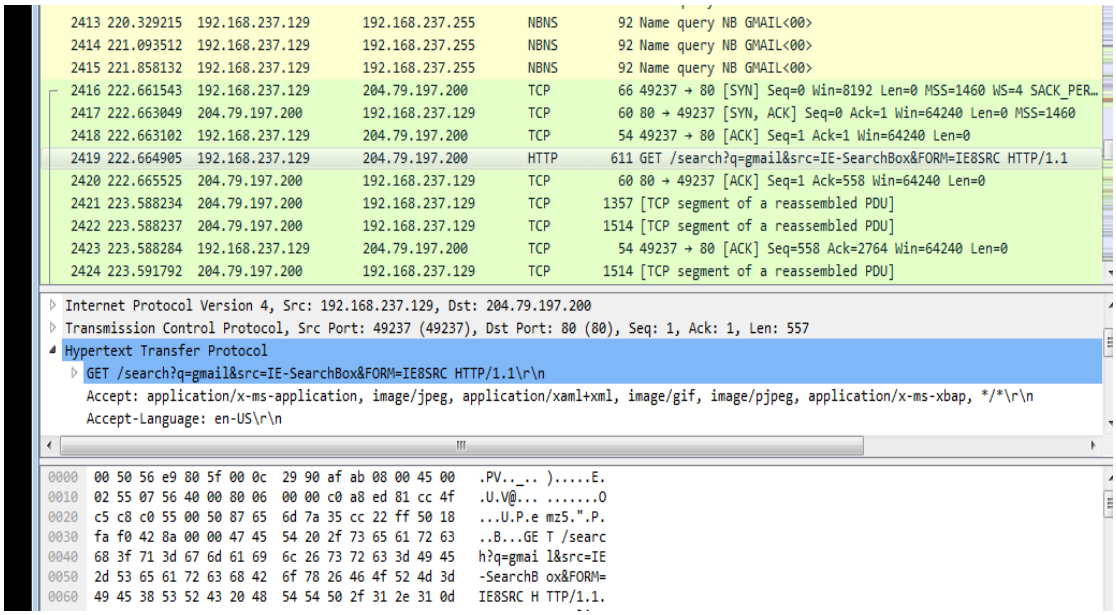



Figure 4.34 Bot/infected machine send data to C&C server

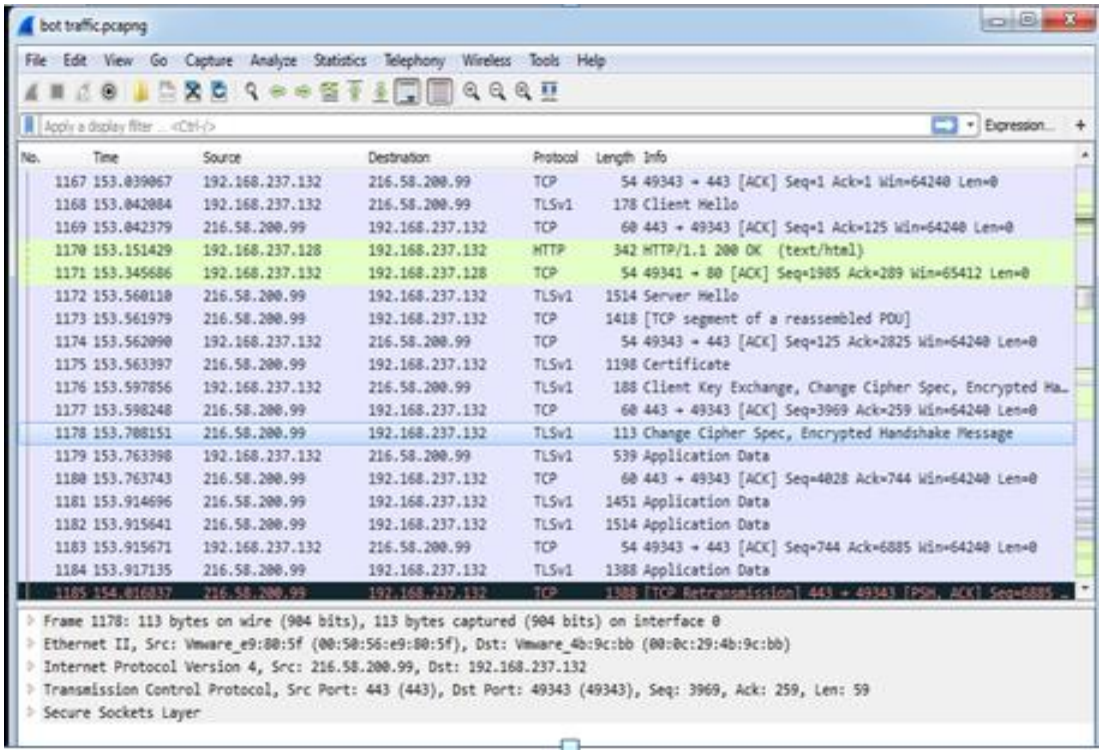



Figure 4.35 encrypted message send from C&C server to victim machine

### 4.4.2 Process Monitor

Process Monitor is a tool which is used to monitors the real-time window operating system as its file system activity. It is a combination of two another tools named as filemon and regmon also have some additional features as application debugging, computer forensics and system adminstration. Procomon records all actions done against window registry and shows the working of all files and dlls with applications. It has also fiter option to filter the required information such as specific process, key and process id etc.

Procomon should be executed as administrator privileges to fetch the all results. It shows the operations in details such as file system, process networking and registry. To anaysis the Zeus botnet behavior in detail, procomon is used to monitor the botnet activities during bot execution on victim machine. For this, it capture the bot configuration builder file, Bot executable file and bot execution process on victim machine.

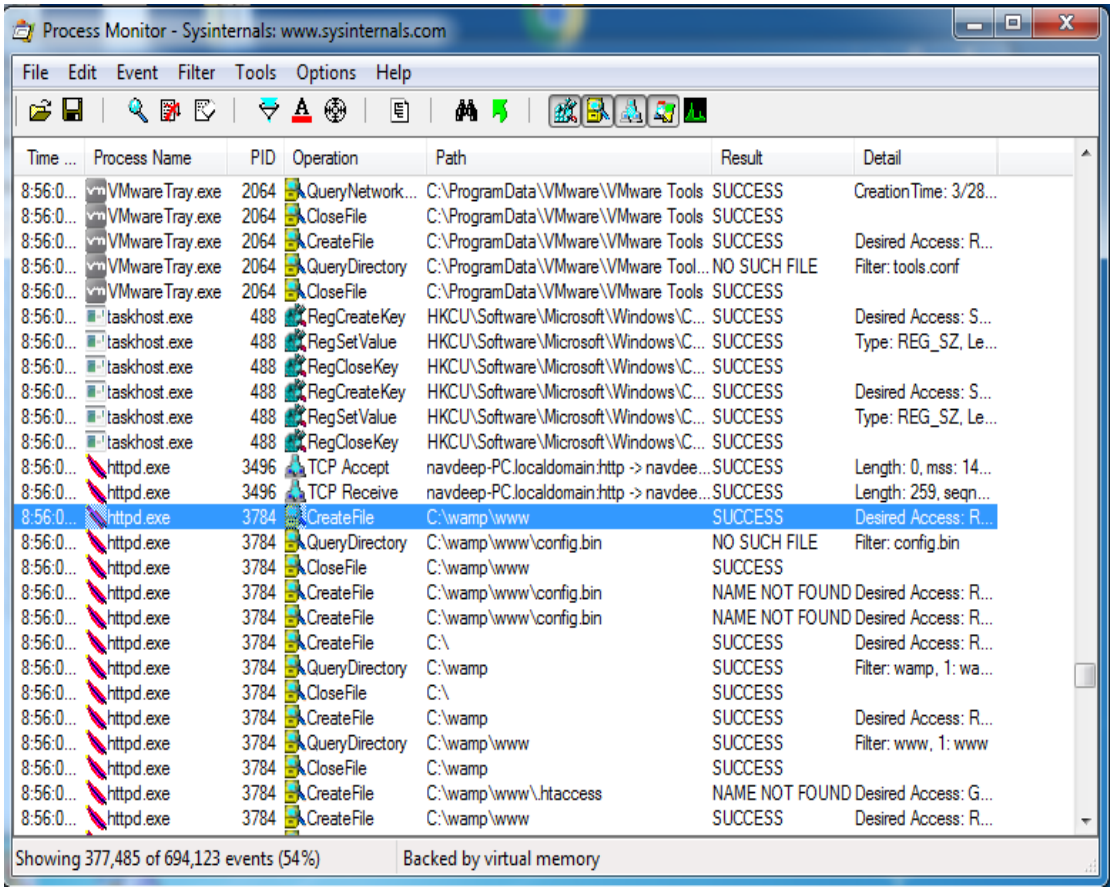



Figure 4.36 Process Monitor Interface

Procmon capture the process of download and install bot configuration builder file on victim machine as shown in figure 4.36.

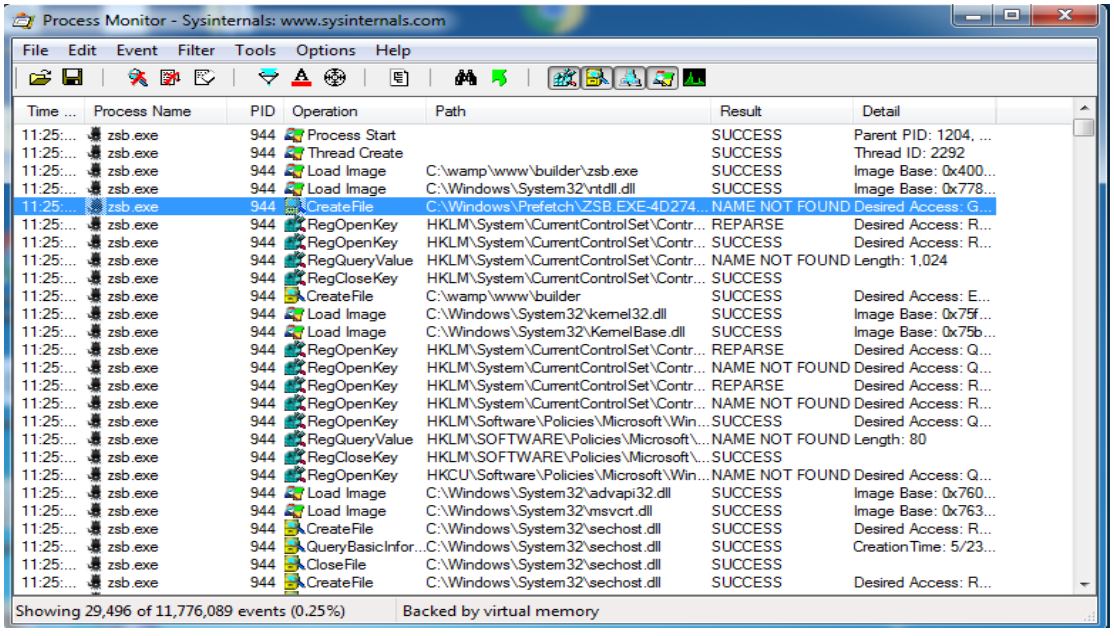



Figure 4.37 Process of the Zeus Configuration Builder

Zsb.exe configuration builder file build the bot binary which is encrypted using encryption key defined in config.exe in RC4 encryption. To find this encryption key it needs to disassemble the zsb.exe. Same encryption key used for build the binary file is required for establish the communication between bot and control panel. Zsb. Exe utilizes many .dlls files from system32 in windows. Some most important .dlls files like rsaenh.dll are also used by configuration builder.

**rsaenh.dll** is Microsoft enhances cryptographic service provide with 128 encryption. Procmon shows that Zeus configuration builder is using these .dlls files many times for encryption and decryption process during building the bot binary file.

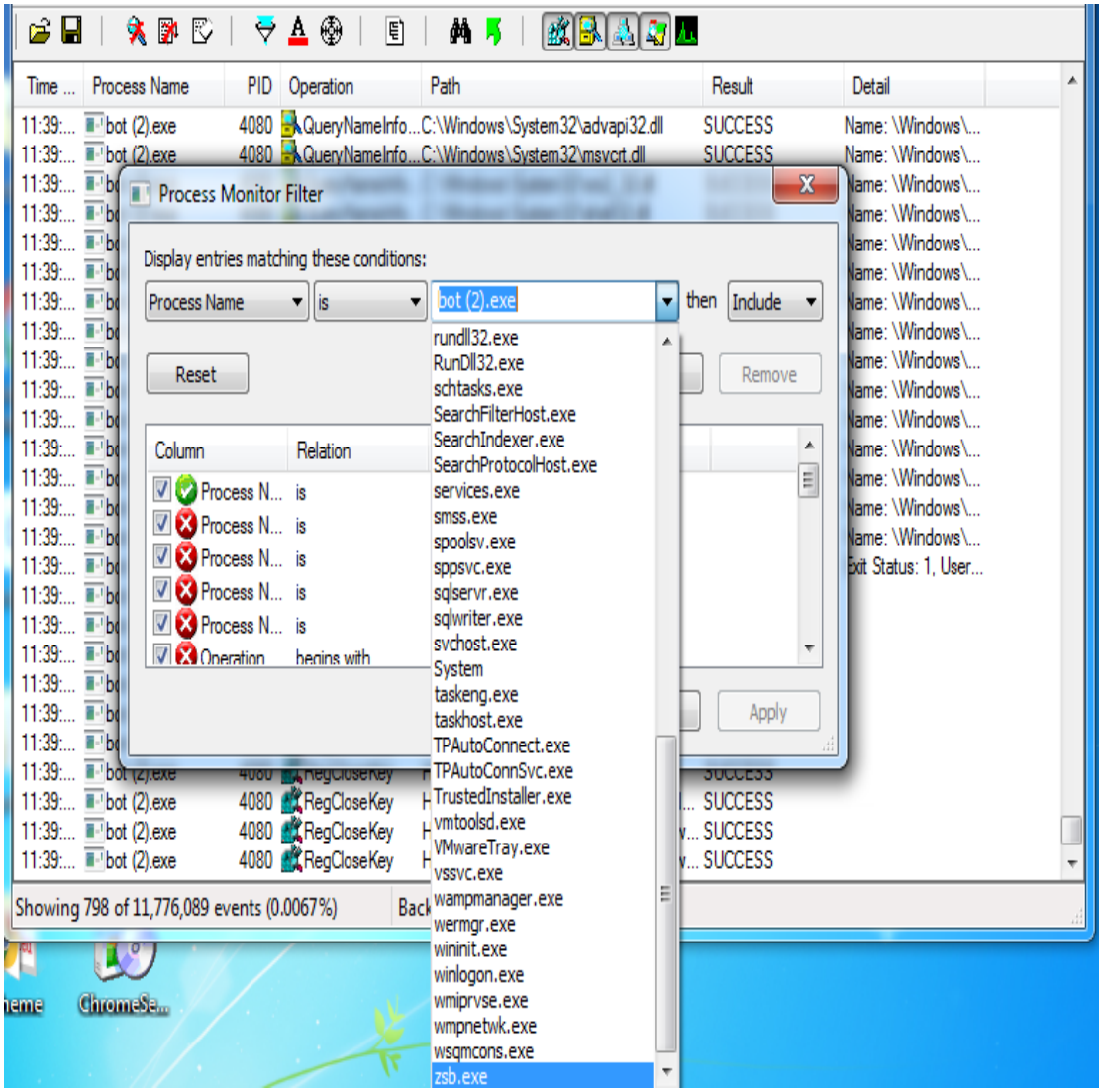



Figure 4.38 filter option apply on Process Monitor

Procmon has filter option to filter the specific data about any process by choosing from dropdown options available such as process, Process id, Authentication id, Time and Date and parent PID etc. So, it is easy to capture the details about bot process in process monitor by filter the bot.exe and zsb.exe to capture the process of Zeus configuration builder.

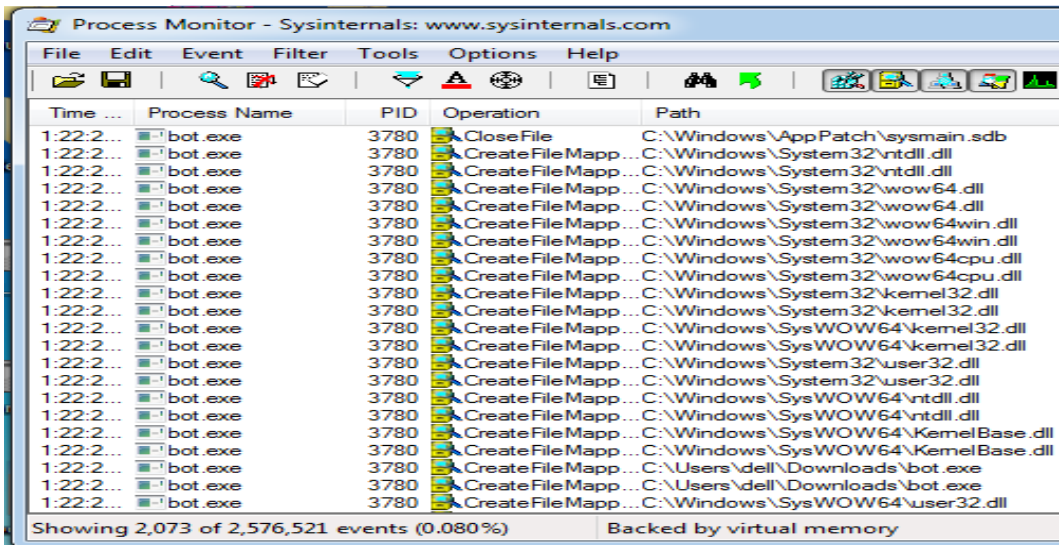



Figure 4.39 .dll files utilized by bot execution process

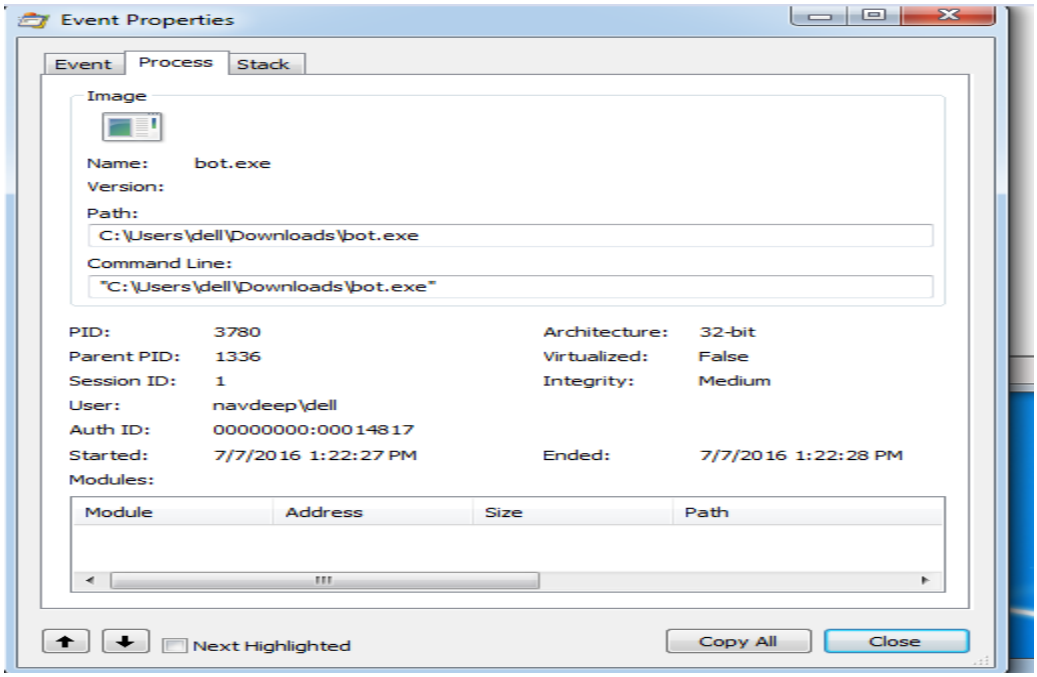



Figure 4.40 details of Bot.exe

### 4.4.3 OLLYdebugger

Ollydbg is a x86 debugger and reverse engineering tool used for binary code analysis. This tool is used to crack the software which is developed by other developer. Because of its user friendly interface and free of cost availability, Ollydbg has most famous tool for malware analysis.

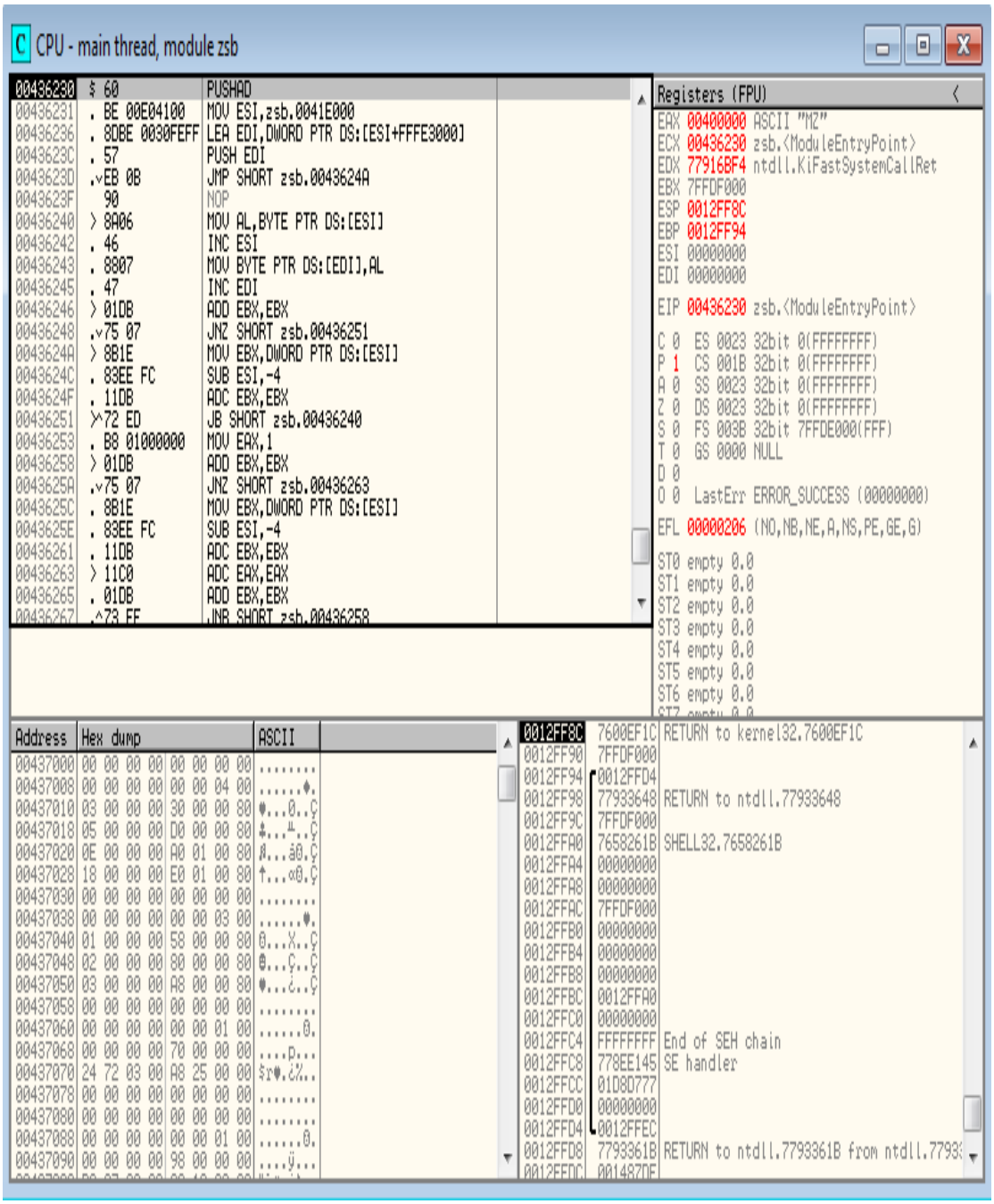



Figure 4.41 Olly Debugger Interface

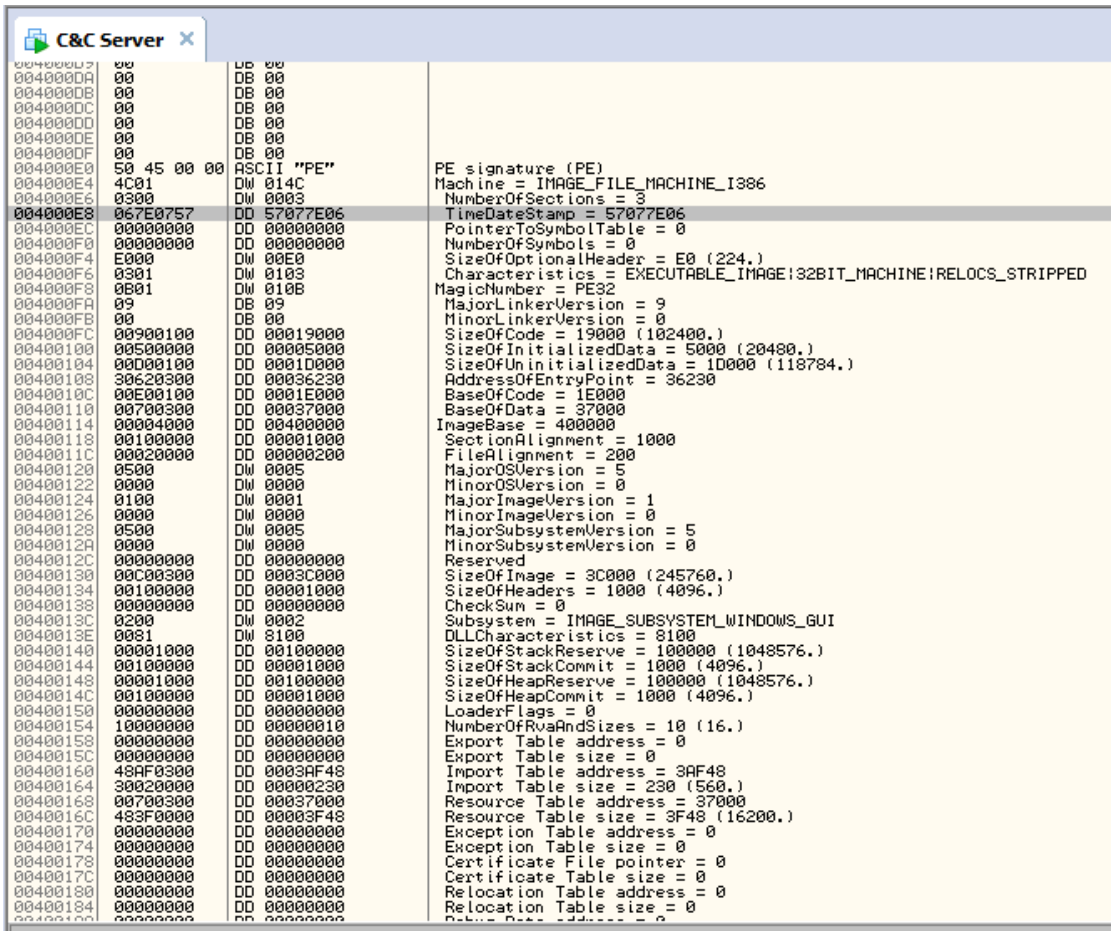



Figure 4.42 time stamp during bot execution

Olly debugger can be used to search and time stamp of bot execution as shown in figure 4.42

## 4.5 Signature Based botnet Detection

Signature based techniques works with the help of using the signature of existing Botnet. This technique is work with creating a database where signature of all existing malware is stored. Then by using pattern matching method it compare the signature of network traffic with the existing bot signatures stored in database. Due to existence of Signatures in a Database this techniques can immediately find the existing Botnet if signature match with database.

We have applied signature based techniques to detect the Zeus botnet in this thesis. There are many antivirus scanners available that look for signature as typically a sequence of bytes with malware code that is scanned by program to involve in doing any malware activity. Antivirus listed as threat and detects this kind of malware file during scanning. Zeus signature is also available and can scan by some good antivirus with its signature.

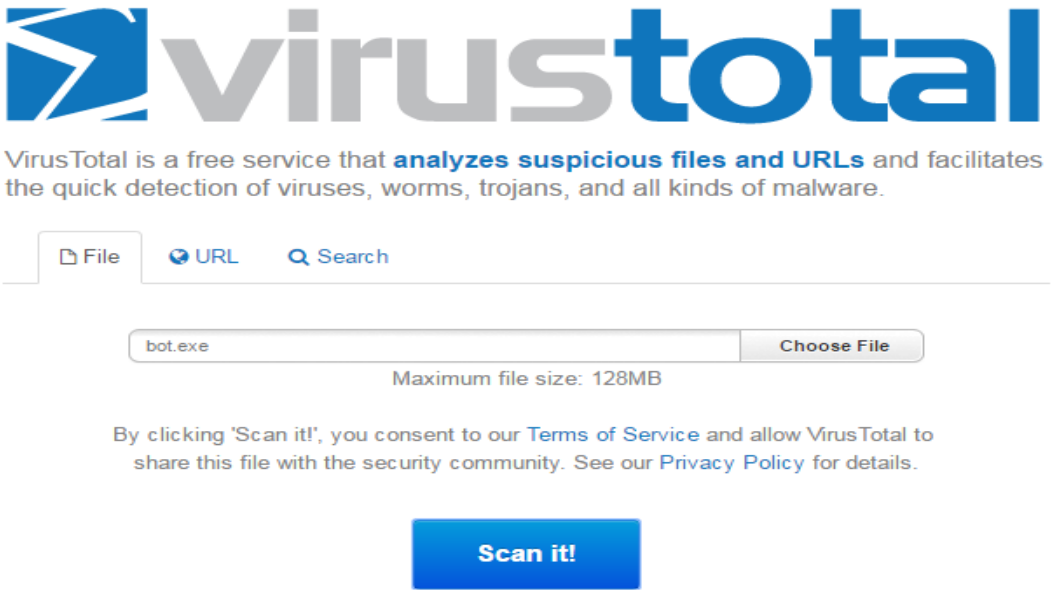



Figure 4.43 Scanning Bot.exe on Virus Total

Bot.exe which is generated using builder configuration setting and used by Zeus bot master to infect other computer is scanned to check its signature can detect by any antivirus or not as shown in Figure 4.43 As if the signature of bot.exe is not encrypted antivirus can easily detect it but there are also some new kinds of botnets designed by botmaster where signatures are encrypted. Botmaster send malware file with using new signature every time to avoid detection.

| | | |
|---|---|---|
| F-Secure | Trojan-Spy:W32/Zbot.AVTH | 20160708 |
| Fortinet | W32/Zbot.YW!tr | 20160708 |
| GData | Gen:Variant.Kazy.165 | 20160708 |
| Ikarus | Trojan-Spy.Banker.Citadel | 20160708 |
| K7AntiVirus | Spyware ( 002891031 ) | 20160708 |
| K7GW | Spyware ( 002891031 ) | 20160708 |
| Kaspersky | HEUR:Trojan.Win32.Generic | 20160708 |
| Malwarebytes | Trojan.Zbot | 20160708 |
| McAfee | PWS-Zbot.gen.ds | 20160708 |
| eScan | Gen:Variant.Kazy.165 | 20160708 |
| Microsoft | PWS:Win32/Zbot!ZA | 20160708 |
| Qihoo-360 | HEUR/QVM20.1.0000.Malware.Gen | 20160708 |
| Sophos | Troj/PWS-BSF | 20160708 |

Figure 4.44 Results shown by different Antivirus

Figure 4.44 shows the result of bot.exe scanning with different antiviruses. It shows that many antiviruses catch it as type of malware or Trojan. Thus it means that Zeus signature is available in many antiviruses database. If we scan the files download from internet it can catch the malware file send from any botnet. Signature based technique is easiest way of prevent our system from botnet infection.

| | | |
|---|---|---|
| ClamAV | Win.Spyware.Zbot-1275 | 20160708 |
| Comodo | TrojWare.Win32.Agent.~wkcf | 20160708 |
| Cyren | W32/Zbot.BR.gen!Eldorado | 20160708 |

Figure 4.45 bot.exe file name in different antivirus

Zeus botnet is also called as Zbot. Some antiviruses like ClamAV and McAfee indicated this file as Zbot spyware.

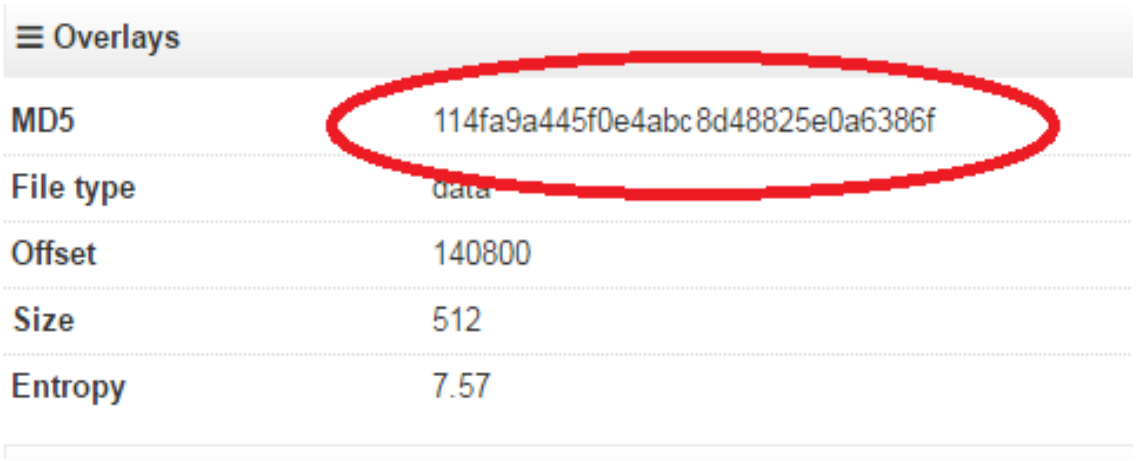



Figure 4.46 Hashes generated by MD5

MD5 generated hash for bot.exe antivirus match this hash with database where haaashes of existing botnet are avalible . As Zeus is most famous and 80% of infected traffic is generated with it.We find that Signature of Zeus botnet is available in data base of antivirus and detect it as malware.

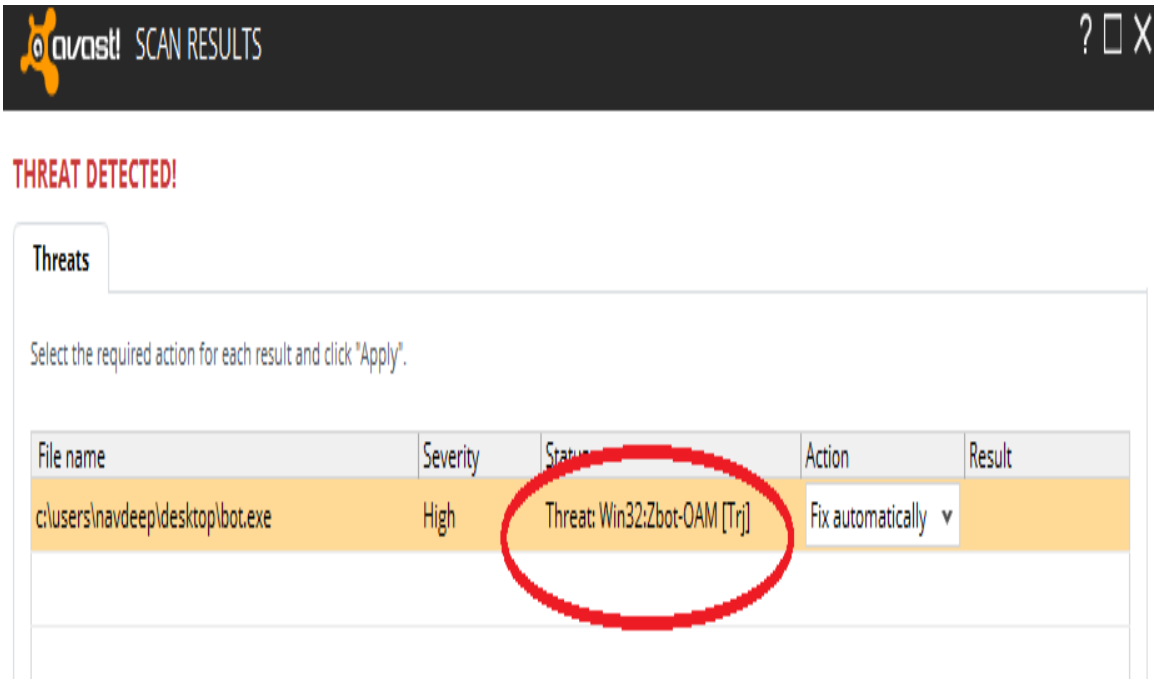



Figure 4.47 Avast Scan Report

Bot.exe scanned by avast anitvirus as shown in figure 4.47 found the bot.exe as threat and show its detail.

Signature based technique has limitation as it can only find the botnets which are known and already traced. But new Zeus botnets are coming with using different signatures which are difficult to trace using signature based technique.

# Chapter 5

# Conclusion and Future Scope

This chapter shows the final conclusions of botnet analysis and direction for future research on botnet. The analysis of botnet with malware and network sniffing tools proves the existence of botnet. With the sniffing tool like Wireshark communication between command and control server and different bots can be captured. Our analysis provides the details of botnet, infected machines behavior and how infected machines are controlled by botmaster.

So before starting the botnet analysis it is necessary to know the botnet in brief. Chapter 2 Literature review has covered the all parts of botnet in details such as botnet history, life cycle, botnet attacks and existing botnet detection techniques.

To analyze the Zeus botnet it is important to know the Zeus toolkit briefly. First section of chapter 4 named as design and implementation described the components of Zeus botnet toolkit. Zeus toolkit is free available on internet but code of zeus botnet is hardest to understand because of its length as there are around 1500 lines of code in zeus toolkit. An isolated virtual environment using VMware has created for analysis the Zeus bots. Section 4.1 described the setup of virtual environment created for Zeus toolkit installation in VMware. Zeus botnet is required the connectivity with PHP and MySql in backend. Thus wamp server has been installed on the window machine used for creating C&C server.

Zeus botnet toolkit has different components and complex installation process as described in Section 4.2. After the creation of command control server on one window machine there is need to infect other machines using it to check the working and complete installation of command and control server. Victim machines are infected with bot.exe generated by configuration files sent from command and control server. These machines are isolated from real host machines and internet. In Section 4.2, bot machines set up has been defined, in these bot/ infected machines sniffing tools like Wireshark, process monitor and Olly debugger are installed to capture the behavior of infected machines and communication between bots and C&C server.

Section 4.3 described the working of Zeus botnet and checks the synchronization between botnet. It shows how bots sent information collected from infected social and banking websites. Complete botnet analysis and evidence of existence of botnet can be done with checking its network based communication captured with using network sniffing tool. Wireshark captured the Get/config.bin and Post/gate.php packets during communication between C&C server and bots as describes in Section 4.4.

Procmon captured the process of download and installation of bot configuration file on victim machine sent from C&C server. It monitored the bots/infected machines and shows the Domain name, IP address and .dlls files used from infected machines. Existence of bot and timestamp when it is executed can also check with the help of Olly Debugger.

The analysis of botnet with reverse engineering and network sniffing tools proves the existence of botnet. As we can capture the communication between C&C server and various bots, it helps to trace the location of C&C server.

Botnet detection using signature based techniques shows that as Zeus Signature is available and can detect by using some good antivirus. There is a need to give more concern on web security while using Internet for financial purposes as internet banking. And also needs to keep virus software up-to-date so it can also detect latest virus signatures.

## Future work

Future work needs to focus into design an efficient system or technique to detect Zeus Botnet because many dangerous attacks on cyber security in previous years has been done using Zeus botnet and it is becoming the largest botnet attack over the days until now. Main difficulty with Zeus botnet detection is its encryption/decryption method use for communication. So there is a big need to find the method or technique to detect this encrypted traffic. There is also a big need to monitor the complete working of different botnets and build a complete list of all the bots with its signatures which will be helpful to develop new botnet detection models and techniques.

# Chapter 6

# References


[1] Jang-Jaccard, Julian, and Surya Nepal. "A survey of emerging threats in cybersecurity." *Journal of Computer and System Sciences* 80.5 (2014): 973-993.

[2] Rodríguez-Gómez, Rafael A., Gabriel Maciá-Fernández, and Pedro García-Teodoro. "Survey and taxonomy of botnet research through life-cycle." *ACM Computing Surveys (CSUR)* 45.4 (2013): 45.

[3] Zhu, Zhaosheng, et al. "Botnet research survey." *Computer Software and Applications, 2008. COMPSAC'08. 32nd Annual IEEE International*. IEEE, 2008.

[4] Bailey, Michael, et al. "A survey of botnet technology and defenses."*Conference for Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology*. IEEE, 2009

[5] Tyagi, Amit Kumar, and G. Aghila. "A wide scale survey on botnet."*International Journal of Computer Applications* 34.9 (2011): 10-23..

[6] Silva, Sérgio SC, et al. "Botnets: A survey." *Computer Networks* 57.2 (2013): 378-403.

[7] Chang, Wentao, et al. "Measuring botnets in the wild: Some new trends."*Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 2015.

[8] Mahmoud, Muhammad, Manjinder Nir, and Ashraf Matrawy. "A Survey on Botnet Architectures, Detection and Defences." *IJ Network Security* 17.3 (2015): 264-281.

[9] Li, Chao, Wei Jiang, and Xin Zou. "Botnet: Survey and case study."*Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on*. IEEE, 2009.

[10] Zeidanloo, Hossein Rouhani, and Asrulnizam Abd Manaf. "Botnet command and control mechanisms." *Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on*. Vol. 1. IEEE, 2009.

[11] Hossein Rouhani Zeidanloo, Farhoud Hosseinpour , Farhood Farid Etemad, ”New Approach for Detection of IRC and P2P Botnets” , International Journal of Computer and Electrical Engineering, Vol.2, No.6, December, 2010, 1793-8163.

[12] Cooke, Evan, Farnam Jahanian, and Danny McPherson. "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets." *SRUTI* 5 (2005): 6-6.

[13] Nagaraja, Shishir, et al. "BotGrep: Finding P2P Bots with Structured Graph Analysis." *USENIX Security Symposium*. 2010.

[14] Wang, Ping, Sherri Sparks, and Cliff C. Zou. "An Advanced Hybrid Peer-to-Peer Botnet." *IEEE Transactions on Dependable and Secure Computing* 7.2 (2010): 113.

[15] Holz, Thorsten, et al. "Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm." *LEET* 8.1 (2008): 1-9.

[16] Zhuge, Jianwei. *Characterizing the IRC-based botnet phenomenon*. Universität Mannheim/Institut für Informatik, 2007.

[17] Wang, Wei, et al. "A novel approach to detect IRC-based botnets." *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on*. Vol. 1. IEEE, 2009.

[18] Lee, Jae-Seo, et al. "The activity analysis of malicious http-based botnets using degree of periodic repeatability." *Security Technology, 2008. SECTECH'08. International Conference on*. IEEE, 2008.

[19] Eslahi, Meisam, Habibah Hashim, and Nooritawati Md Tahir. "An efficient false alarm reduction approach in HTTP-based botnet detection." *Computers & Informatics (ISCI), 2013 IEEE Symposium on*. IEEE, 2013.

[20] Perdisci, Roberto, Wenke Lee, and Nick Feamster. "Behavioral Clustering of HTTP-Based Malware and Signature Generation Using Malicious Network Traces." *NSDI*. 2010.

[21] Wang, Ping, Sherri Sparks, and Cliff C. Zou. "An Advanced Hybrid Peer-to-Peer Botnet." *IEEE Transactions on Dependable and Secure Computing* 7.2 (2010): 113.

[22] Xiang, Cui, et al. "Andbot: towards advanced mobile botnets." *Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats*. USENIX Association, 2011.

[23] Choi, Byungha, Sung-Kyo Choi, and Kyungsan Cho. "Detection of mobile botnet using VPN." *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on*. IEEE, 2013.

[24] Karim, Ahmad, Syed Adeel Ali Shah, and Rosli Salleh. "Mobile botnet attacks: a thematic taxonomy." *New Perspectives in Information Systems and Technologies, Volume 2*. Springer International Publishing, 2014. 153-164.

[25] Hua, Jingyu, and Kouichi Sakurai. "A sms-based mobile botnet using flooding algorithm." *IFIP International Workshop on Information Security Theory and Practices*. Springer Berlin Heidelberg, 2011.

[26] Zeng, Yuanyuan, Kang G. Shin, and Xin Hu. "Design of SMS commanded-and-controlled and P2P-structured mobile botnets." *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2012.

[27] Alzahrani, Abdullah J., and Ali A. Ghorbani. "SMS mobile botnet detection using a multi-agent system: research in progress." *Proceedings of the 1st International Workshop on Agents and CyberSecurity*. ACM, 2014.

[28] Singh, Kapil, et al. "Evaluating bluetooth as a medium for botnet command and control." *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer Berlin Heidelberg, 2010.

[29] Karim, Ahmad, et al. "Mobile Botnet Attacks-an Emerging Threat: Classification, Review and Open Issues." *TIIS* 9.4 (2015): 1471-1492.

[30] Chandrashekar, Jaideep. "The dark cloud: Understanding and defending against botnets and stealthy malware." *Managing Editor* 13.2 (2009): 130.

[31] Francois, Jerome, et al. "Botcloud: Detecting botnets using mapreduce."*2011 IEEE International Workshop on Information Forensics and Security*. IEEE, 2011.

[32] Kebande, Victor R., and Hein S. Venter. "A Cloud Forensic Readiness Model Using a Botnet as a Service." *The International Conference on Digital Security and Forensics (DigitalSec2014)*. The Society of Digital Information and Wireless Communication, 2014.

[33] Wagner, Claudia, et al. "When social bots attack: Modeling susceptibility of users in online social networks." *Making Sense of Microposts (# MSM2012)*2 (2012).

[34] Ferrara, Emilio, et al. "The rise of social bots." *arXiv preprint arXiv:1407.5225* (2014).

[35] Haustein, Stefanie, et al. "Tweets as impact indicators: Examining the implications of automated “bot” accounts on Twitter." *Journal of the Association for Information Science and Technology* 67.1 (2016): 232-238.

[36] Zhuge, Jian-wei, et al. "HoneyBow: An automated malware collection tool based on the high-interaction honeypot principle." *JOURNAL-CHINA INSTITUTE OF COMMUNICATIONS* 28.12 (2007): 8.

[37] Li, Zhichun, Anup Goyal, and Yan Chen. "Honeynet-based botnet scan traffic analysis." *Botnet Detection*. Springer US, 2008. 25-44.

[38] Xie, Yinglian, et al. "Spamming botnets: signatures and characteristics."*ACM SIGCOMM Computer Communication Review* 38.4 (2008): 171-182.

[39] Ranjan, Supranamaya, Joshua Robinson, and Feilong Chen. "Machine learning based botnet detection using real-time connectivity graph based traffic features." U.S. Patent No. 8,762,298. 24 Jun. 2014.

[40] Nychis, George, et al. "An empirical evaluation of entropy-based traffic anomaly detection." *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*. ACM, 2008.

[41] Arshad, Sajjad, et al. "An anomaly-based botnet detection approach for identifying stealthy botnets." *Computer Applications and Industrial Electronics (ICCAIE), 2011 IEEE International Conference on*. IEEE, 2011.

[42] Kang, Brent Byung Hoon. "DNS-based botnet detection." *Encyclopedia of Cryptography and Security*. Springer US, 2011. 362-363.

[43] García, Sebastián, Alejandro Zunino, and Marcelo Campo. "Survey on network-based botnet detection methods." *Security and Communication Networks* 7.5 (2014): 878-903.

[44] Masud, Mohammad M., et al. "Peer to peer botnet detection for cyber-security: a data mining approach." *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*. ACM, 2008.

[45] Thuraisingham, Bhavani. "Data mining for security applications: mining concept-drifting data streams to detect peer to peer botnet traffic."*Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on*. IEEE, 2008.

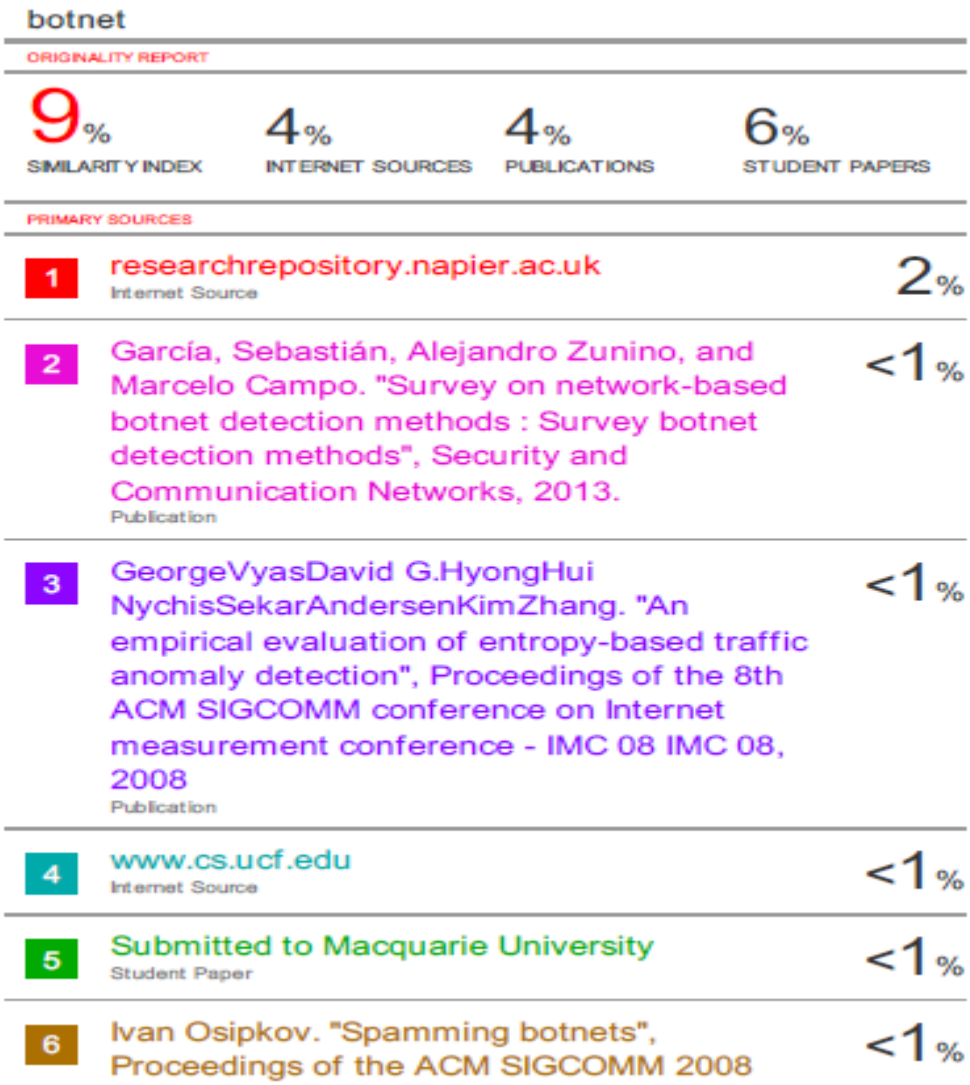
# List of Publications

Navdeep Kaur, Maninder Singh, “Botnet and Botnet Detection Techniques in Cyber Realm", *International Conference on Inventive Computation Technologies (ICICT 2016) to be held from August 26-27, 2016 Tamil Nadu, India* [Accepted].

# Video Link

Url: “https://www.youtube.com/channel/UCYOwaDiM6ydgpQnV_-9dvvg”

# Plagiarism Report



botnet

ORIGINALITY REPORT

| 9% | 4% | 4% | 6% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | researchrepository.napier.ac.uk<br>Internet Source | 2% |
| 2 | García, Sebastián, Alejandro Zunino, and Marcelo Campo. "Survey on network-based botnet detection methods : Survey botnet detection methods", Security and Communication Networks, 2013.<br>Publication | <1% |
| 3 | GeorgeVyasDavid G.HyongHui NychisSekarAndersenKimZhang. "An empirical evaluation of entropy-based traffic anomaly detection", Proceedings of the 8th ACM SIGCOMM conference on Internet measurement conference - IMC 08 IMC 08, 2008<br>Publication | <1% |
| 4 | www.cs.ucf.edu<br>Internet Source | <1% |
| 5 | Submitted to Macquarie University<br>Student Paper | <1% |
| 6 | Ivan Osipkov. "Spamming botnets", Proceedings of the ACM SIGCOMM 2008 | <1% |