Proceedings of the Second International Conference on Research in Intelligent and Computing in Engineering pp. 93–101
DOI: 10.15439/2017R28
ACSIS, Vol. 10 ISSN 2300-5963

A Framework on botnet detection and forensics

Harvinder Singh
Dept of Computer Science and Engineering,
Uttaranchal University,
Dehradun, Uttarakhand, India
sachin_ats@rediffmail.com

Anchit Bijalwan
Dept of Computer Science and Engineering,
Uttaranchal University
Dehradun, Uttarakhand, India
anchit.bijalwan@gmail.com

***Abstract*—The utilization of Internet on domestic and corporate front has been increasing at drastic rate. Each organization and enterprise exploits the internet to its fullest extent based on its requirements. In almost all areas, internet is proved to be a boon. But sometimes it lands the users into trouble because of unwanted and uninvited harmful software applications. There are so many types of threats and challenges that are faced by the internet users. Out of all the threats faced by internet users, botnets are at the top most position. Because of these prodigious threats botnets are the rising area of research. Botnet works as a coordinated or synchronized activity where different bots collectively participate to perform a malicious task. The botnet is different from other form of malware in its capability to compromise the computer systems or smartphones to set up a link with command and control(C&C) server controlled by bot controller. Because of the massive participation of compromised machines the losses caused by botnet attack are immeasurable. As a result, different researchers are showing keen interest in the field of botnets. The trend reflects that the number of researches in this field have gone up at tremendous rate in past 5 to 10 years. The present paper proposes a framework to systematically identify the presence of malicious bot, prevent it from spreading further and performing its forensic investigation.**

***Index Terms*—Bots, Botnet, Botnet detection, Forensics, Malware**

I. Introduction

Now a days , Botnets are becoming the first choice of hackers and crackers to take them to their very goal. These people perform their wicked activities through a Botnet. A Botnet is defined as a collection of interconnected clients that may be the Computer systems or mobile devices where each device is infected with malevolent piece of software called bot. The machine or host that is infected with bot is also sometimes referred to as a bot. A Botnet is created and controlled by humanware commonly known as botherder or botmaster.

A botmaster controls all the bots in his botnet by issuing them commands and instructions and instructions through a common meeting point on the internet and that is referred to as C & C (Command and Control) server. All bots directly or indirectly report to this C&C server and are controlled and coordinated by it.

Bots are used to perform an ample number of tasks that are marked by deep ill will. Bots are used to carry out the activities against hardware as well as software and such activities are deliberately harmful. Some examples of such vindictive tasks are DDOS(Distributed Denial of Service) attack. The impact of such attack is quite harmful. According of FBI, USA alone has faced the loss of around $20 million because of the bot attacks.

The main purpose of botherders behind the development and operation of botnets is the monetary benefit. The botherders reportedly earn huge profits by extending and rendering their services to different people and organizations. As per the available facts and figures many botnets have badly hampered the working of Internet and have definitely caused losses to world economy. These days, along with the botnets of computers, the botnets of mobile phones are extending their arms and are posing a big threat to safety and security of Internet. Because of the speedy expansion of botnets and their harmful impacts , many researchers and organizations are taking keen interest in studying botnets and developing solutions to find its existence, to reduce its impact, to make it stay apart and to eradicate it. So many security solution developers companies such as MCAfee, Symantec, TrendMicro have given some tools to fight against botnets and are still striving hard in direction of finding the whereabouts of botnets and also to freeze them. Botnets have major impact on the all categories of people who come under its influence. It is observed that a good number of researchers have shown their concern for the current problem of botnets , as there is a sharp increase in number of research articles on botnets from year 2005 to 2015.

The remaining part of the paper is organized as follows: Section 2 gives introduction of the botnet life cycle and architecture, Section 3 throws light upon research related studies, Section 4 defines architecture of botnet forensics, botnet defense mechanism which is required for investigation and reduction of botnet activity is detailed in Section 5, and some research challenges are presented in Section 6, and at the end we discuss conclusion and future prospects in Section 7.

II. RELATED WORK

Many researchers have worked in this field and tried to find out some solution to the problem of botnets. Many of them have suggested some solutions and shared their experimental experiences to mitigate the problem of Botnets. In literature review it is highlighted that the past researchers have deployed various tools and developed the techniques such as Signature and Anomaly-based Intrusion Detection Systems (IDS) to tackle the problem of network security and detection of threat.

In [1] a generic framework is presented that is related to botnet detection and is based on the approach of passive monitoring or observation of the network traffic. The authors have also tried their level best to present the approach through the use of a flow chart. Authors also stress upon the statement that, to apply or test the mitigation efforts, detection must be performed in real time. There must be low false positives to notice botnet action as in intrusion detection system. Escaping the detection need to be considered as one of the most crucial features for bot attackers.

In [2] the authors have build up the framework on the advancement of tools belonging to open source category, such tools include Hadoop, Hive and Mahout to render a measurable effectuation of semi-real-time intrusion detection system. The effectuation is used to observe Peer-to-Peer botnet attacks using machine learning methodology. The fpcus points of their paper are as follows: (1) Creating a distributed framework using Hive for catching and handling network traces which enables the pull out of dynamic network characteristics. (2) Utilising the parallel processing ability of Mahout to construct Random Forest supported Decision Tree model which is employed in the job of Peer-to-Peer Botnet detection in semi-real-time. The effectuation setup and performance measures are presented as first observations and future elongations are also proposed.

[3] shows an open framework named *Dorothy* that allows to check the activity of a botnet. The authors propose to describe a botnet behavior through a collection of parameters and a graphical representation. In a case study, the authors penetrated and observed a botnet named *siwa* and collected details about its operational structure, geographical distribution, communication techniques, command language and processes. The framework of *Dorothy* is composed of various software modules applying all different steps of the mechanical joining to an IRC channel, tracking, study and graphical representation of botnet activity.

In [4] the authors presented a new detection framework which lays stress upon P2P based botnets. This proposed framework is related to their definition of botnets. The proposed framework is based on inactive monitoring of network traffics. Accordingly this model is not suitable for detecting botnet at that particular moment when hosts are contaminated with bots. The authors identify a botnet as a collection of bots that will perform similar interaction and malicious activity patterns within the same botnet. In this detection framework, authors observe the group of hosts that present similar interaction pattern in one stage and also performing malicious activities in another stage, and searching for the common hosts in them.

In [5] the researchers show the facts required to create a system capable of reducing the botnet problem in financial scenario. The projected arrangement stands on a new design that has been authenticated by one of the largest savings banks of Spain. The authors present that it is possible to *plot* financial botnet networks and to give a non-deterministic *grade* to its connected bots. The planned arrangement also encourages intelligence data sharing and distribution to concerned organizations such as law enforcement agencies, Internet Service Providers and financial establishments.

In [7] present an organized botnet framework to facilitate researchers to put together benevolent botnets with changing command and control (C&C) arrangements to allow researchers to produce imitated base for the intentions of illustrating existing and probable forthcoming botnet C&C structures in order to assist the practical expansion of efficient botnet security. This allows researchers to imitate recent and possible upcoming botnet traffic, illustrate it, and sketch valuable defense processes. In this paper, the authors portray the SLINGbot model and how it can be helpful for the positive improvement of botnet defense mechanisms.

In [8] the authors proposed the structure of IRC client nature in a route in order to differentiate between regular and botnet-linked action. The projected system for spotting botnet activity is based on a structure of IRC client performance. The suggested structure spots and interprets IRC movement within unprocessed network traffic and, by examining a group of expressive factors, enables an organizer to group and segregate regular activity occurrences from botnet-associated ones.

In [12] suggests a novel methodology to spot botnet movement relying on traffic performance investigation by grouping network traffic manners applying machine learning techniques. Traffic activities investigation techniques do not rely upon the packets consignment, which signifies that they can operate with encrypted network interaction protocols. Network traffic data can generally be conveniently extracted from multiple network

tools without influencing major network operation or service accessibility. The researchers learn the possibility of spotting botnet movement without having seen an entire network stream by grouping actions build on time gaps. Examining the available information, the authors demonstrate practically that it is feasible to spot the occurence of identified and strange botnets activity with maximum correctness even with quite little time gaps.

In [13] presented a distinctive, bottom-up concept. That is, to deprecate botnet techniques and tools by dejecting or putting on trial the customers of the embezzled records. To make the idea tangible, the researchers put forward a case study of relating the concept to a well known botnet toolkit, *Zeus*, along with two techniques, called, reverse engineering and behavioural analysis. The benefit of this concept is that it points at the fragile point of a botnet food chain (the customers). The pouring effect will ultimately influence the peak level of the chain (the toolkit creator) by reducing his/her earnings when trading latest data to existing customers and new customers. In accumulation, since the assault is on the business prototype, malware developers would require to modify how they do trading to avoid our attack, which is additionally tough than changing the application of their tools and techniques.

In [14] an arrangement located at the network border is set up with the ability to spot rapidly changing domains via DNS interrogation. Numerous domain characteristics were investigated to ascertain which of them would be highly successful in the grouping of domains. This is attained applying a C5.0 decision tree classifier along with Bayesian statistics, with affirmative illustrations being labeled as possibly malicious and pessimistic illustrations as genuine domains. The approach spots harmful domain names with a maximum probability of accuracy, mitigating the requirement of blacklists. Some of the statistical tools, such as Variation distance and Probability distribution, Naive Bayesian, Bayesian are employed to spot harmful domain names. The spotting methods are tried out against modeled traffic and it is highlighted that the harmful traffic can be spotted with low false positive rates.

In [15] Demonstrates the study and examination done to describe or identify an effective set of traffic factors capable of depecting both usual and unusual working of networks, throwing light upon botnet activity spotting through abnormal and supportive behavior. An identification framework model is also suggested and examined through real data traffic.

In [17] analyze the potential threat of botnets based on mobile networks. The author discusses about mobile botnets.
The term mobile botnet refers to a group of compromised smartphones that are remotely controlled by botmasters via C&C channels. The author also gives brief account of Waledac and challenges involved in the study of mobile botnets and tracing their activities. A light is also thrown upon the defence mechanisms for mobile botnets.

In [18] authors suggest methodologies to spot botnets by examining network data traffic movement or flood. The authors constructed patterns for catching traffic data movement with extra pertinent features for botnet spotting. The researchers or authors have made use of the IPFIX standard for the specification of the patterns. Hence their methods can be applied to find the presence of various bot families with minimum outlay and are dealer impartial.

III. BOTNET FRAMEWORK AND LIFE CYCLE

The actual strength of a botnet is present in its architecture. It it's the skeleton which provides a backbone to the entire botnet. The botnet architecture involves the formation of botnet and who and who involved in it.

A. BOTNET ARCHITECTURE

Under the given heading we are going to throw some light upon the key features of Botnets and rest of the paper will be based on such features. As already mentioned a botnet is a network of compromised machines under the direct control of an individual operator called botherder or botmaster. A botnet may be thought of as melding of many threats into one. A botnet usually consists of bot server, bot clients or bots and botmaster. There can be small as well as large botnets. It means the botnets formed with the network of several hundred or thousands of botnets are regarded as small botnets whereas the botnets with millions of botclients are called large botnets.
The term botnet is derived from Robot Network. It reflects the fact that the botclients will act as Robots and server the botmaster who quietly sits at one central location to send them the commands and fulfill his goal of launching the attacks such as DDOS, sending Spam mails, phishing attacks, identity thefts, stealing credit card credentials etc. In modern days one botmaster handles or tackles a collection of bot servers by creating several divisions. In this way if somehow any communication channel is hampered by security people then only one particular division is lost and rest of the divisions are still active, The other divisions are very well used for launching the illegal activities. A botmaster normally establishes communication with bots using IRC (Internet Relay Chat) on a remote Command and Control (C&C) Server. The five main

stages that are performed in this communication from joining of a new bot to launching an attack are as follows:-

(i) A new vulnerable machine is attacked and compromised by copying into it a malicious piece of code. On execution of the malicious code the machine searches out for the C&C server, attaches itself to the server and becomes part of botnet. Using the rallying mechanism it informs about its presence to the botmaster that it is now ready to receive the commands.

(ii) It then receives commands from the botmaster to perform some malicious activity or task.

(iii) The commands received by the machine from the botmaster are then executed by the bot client.

(iv) The attack is initiated as per the given commands.

(v) The bot client communicates back with the botmaster to inform him about the success of the attack.

There are some more people who are directly or indirectly related to the botnets and they are:-

(1) Bot Creator:- This person is responsible for the development, design and implementation of a botnet. A bot creator may be a botmaster or some other person or group of persons. These people develop special kits called botkit and sell it to those people who are of malicious intent and want to build up and maintain their own botnet.

(2) Bot Users:- These are those people who either avail the services of any botnet by paying some amount of money or they themselves become botmasters by purchasing the botkits or developing the code for bots and form botnets. In this entire process an illegal monetary transaction is also involved.

(3) Dupe:- A dupe is the one who is victimized by a bot. It is that machine which is compromised by exploiting its one or more vulnerabilities. Such machines or people associated with these systems may receive spam mails or be the part of various attacks constituted by bots.

(4) Inactive player:- He or she may be the possessor of a host machine which has been exploited or victimized and hence becomes a part of botnet without any acceptance. It starts doing illegal activities on behalf of the botmaster or as per his indications.

B. BOTNET LIFECYCLE

A life cycle may be thought of as a process starting from the formation of a bot to fulfilling its very purpose. Many papers presented by different authors throw light upon the life cycle of botnets. Most of the authors have presented the various process sequences but the detailed overview is not provided. we have tried our level best to analyse its stps and presentedit in detailed form, clearly stating the purpose of its each stage. The various steps in botnet life cycle are interrelated. In order to vindicate our statement, we are dividing the life cycle of a botnet into 5 steps or stages. A small overview of each stage is given in figure 1.

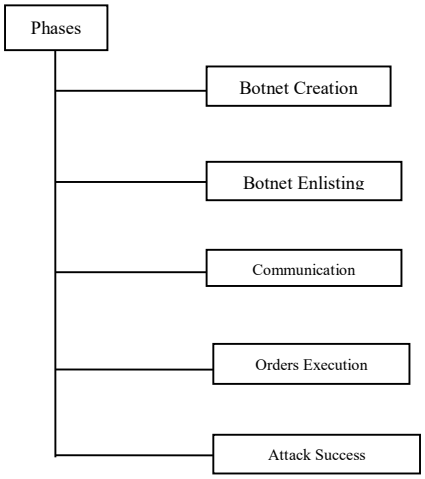

Figure 1: Phases of botnet lifecycle

(a) Botnet Creation:- It is the very first level in the life cycle of a botnet. In this phase the birth of a botnet takes place. The person behind the creation of botnet gives a physical shape to his intentions by framing the initial structure and framework.

(b) Botnet Enlisting:- It is also referred to as bonet recruitment. Once a botnet is created, then arises the need to find out other hosts and if the botmaster locates any vulnerable host through an existing client, then it is compromised and that particular host becomes a member of the botnet.

(c) Botnet communication:- In this stage a process called rallying is taken place. In this process the botnet client setup its first interaction with the botmaster through C&C channel or any other mechanism. At this point or stage a botclient informs the botmaster about its presence in the botnet and it also may request updates. The updates may include the names of various C&C servers, the list of IP addresses, channel names etc. The botclient also takes orders from the botmaster to

initiate an attack or gets information about the location of current antivirus and ensure its removal or making it passive.

(d) Orders Execution:-On getting the commands or Orders from the botherder to perform an attack, the bot client execute such commands. A bot client may perform various actions on the basis of instructions obtained from the botmaster. Such actions may be to launch Distributed Denial of Service attack, sending bulk amount of spam mails, doing click fraud, launching phishing attack, performing identity theft, compromising othet systems or recruit the systems to become part of the botnet, password guessing and installation of adaware etc to the other machines. In some cases the bot clients have special capability to sniff the running network traffic for passwords. According to C A Schiller, the botclients use little but able softwares to grab the usernames and passwords and also use other softwares to creck them. There are various tools available for password breaking or cracking.

(e) Attack Success:- The main goal of any botnet's conception is to successfully carry out the orders of the botmaster and earn desired amount of monetary profit. On successful execution of the attack the bot informs about the success to the bot master.

C. BOTNET TOPOLOGIES

The word topology means the configuration or design in which different bot clients are connected together and form a massive network called botnet. As per the Command and Control(C&C) Channel, the botnet topologies are divided into two categories or models, and that are:

(1) Centralized model
(2) Decentralized model

Both, centralized model and Decentralized model have their own pros and cons. The detailed discussion of both the models is provided here.

1) Centralized model

In centralized model there is one central server or central point that is responsible for setting up communication between the Botherder and Botclients. Using this channel the exchange of messages and commands is taken place. The central server is referred to as Command and Control (C& C) server. Many available Botnets such as SDBot , AgoBot, RBot etc use C&C for the purpose of communication. The central computer or server is usually a powerful computer system because it has to handle the entire Botnet whose size may vary from a few thousands to many millions. It must have a high bandwidth since at any single point it may require to serve many bots. Even though the central server is a powerful one but it is regarded as a weak point of this model. If someone is able to locate and launch an attack on C&C server then the entire Botnet will be deactivated and will no more be able to send to receive messages to the server. The figure 2 gives diagrammatic representation of command and control architecture of centralized model.

There are two protocols which are frequently used by C&C to perform communication and that are HTTP (Hyper Text Transfer protocol) and IRC(Internet Relay Chat).

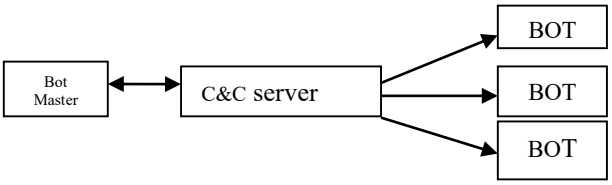

Figure 2: Centralized C&C botnet

1.1 IRC based Botnets

IRC is a protocol for real time Internet text messaging (chatting) or synchronous conferencing based on TCP that may also use secure socket layer. IRC offers various useful features. It helps in transferring files between users and the programs running on systems. IRC based botnets use centralized Command and Control structure in which infected machines try to establish connection to the IRC server and join the same channel.In these botnets the C&C server works on IRC service. The IRC protocol is based on client- server model. It Offers flexibility in communication and is quite simple to setup. It is regarded one of the most popular protocols to setting communication among Botnets.

1.2 HTTP based Botnets

IRC may be thought of as an originating protocol for botnets. IRC gained a lot of popularity and most of the botnets operated on IRC, so many researchers started focusing on IRC based communication. IRC also had some demerits. As IRC contains information about the port number before initiating an attack, the attack can be smoothly detected. So the hackers switched to HTTP protocol. This protocol is generally used in any category of network. It offers various advantages. It has the capability to hide malicious botnet traffic in normal web traffic which could not even be detected by firewall. The HTTP based botnets are easy to easy to form and implemented. There are some botnets

which use HTTP protocol and they are Rustock, Clickbot, Zeus, There are two types of HTTP based botnets:

1. Echo based HTTP botnets
2. Command based HTTP botnets

2) Decentralized model

A decentralized model is a model in which there is no central command and control. The protocols used by centralized botnets are IRC and HTTP but this type of botnet works with different types of protocols. Example of decentralized model is Peer to Peer (P2P). The P2P network of compromised machines is much harder to detect and destroy. P2P systems normally make use of file sharing networks. In decentralized models the botherder has freedom to choose any bot to distribute commands in the botnet. All bots can act as clients as well as servers. This type of botnet cannot be taken down by simply attacking at one point because there is no central server to control entire botnet. If one bot is attacked and taken down then other bots of the botnet will keep on working. P2P botnet is more dynamic and robust than the centralized one. Each bot maintains some collaboration to the other bots of the botnet. The P2P botnet is quite hard to be monitored, taken down and hacked.

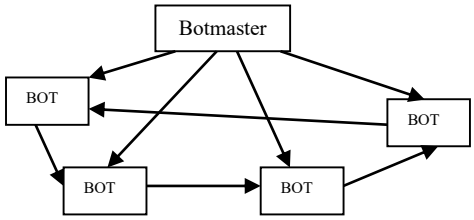

Figure.3: Peer to Peer bonet architecture

IV. BOTNET DETECTION

Many researchers have worked on the detection techniques of botnets and followed various approaches to identify C&C channels or analysis of the network traffic. Various techniques have been designed for Botnet detection from time to time. As per the researchers there are three major techniques of botnet detection:-

a) Host based detection
b) Honeynets based detection
c) Network based detection

A. Host based detection

In hosts based detection techniques the analysis of machine responses is done on the basis of certain terms. The general behavior of the machine is observed and tried to locate any type of abnormality. System taking too long to respond to even small actions, taking too long to resolve the call sequences, any suspicious entry in the registry, abnormal changes in the file systems, antivirus not responding or turning off on its own, changes observed in network connections etc may point fingers in the direction of presence of bot. Host based detection methods are not treated as very successful methods because such methods are capable for only one machine and may vary machine to machine.

B. Honeynets based Detection

Honeynets are sometimes referred to as Honeypots . Honeynets are mainly used to study and understand botnet features and techniques but are not always useful in detecting bot infection. Honey nets are normally employed to discover the intentions of botmasters or attackers. This technique is useful for detecting the known bots. The unknown bots and even known bots with slight change in the bot binaries are not detected by this method.

C. Network based detection

The network based detection technique is based on monitoring and analyzing the passive network traffic. This approach is quite helpful in identifying the presence of botnets in the networks. In this approach the network data is continuously monitored, network based communications are observed. Any abnormal trace may indicate the presence of some malicious activity. Now a days the botmasters are very smart and apply multitude of code obfuscation techniques. Even though the malicious code is obfuscated and bypassed by malware detection software, the packets are still present in the network that can be further traced by applying other techniques. The network based detection technique can be classified into four categories:-

a) Signature based detection
b) Anomaly based detection
c) DNS based detection
d) Mining based detection

a) Signature based detection

For signature based botnet detection technique there must be a dataset containing information about existing botnets. Using the bot binaries of existing botnets the bots behavior can be studied. A very good example of an Intrusion detection system that is based on signature based detection is Snort. In [21] it is being discussed about Snort and it is openly available for anyone on Internet. It has the capability of tracing out the signs of malicious activity when it is placed to monitor the network traffic. But we may consider its limitation that it can only detect the bots with known signatures and is proved to be useless for newly introduced bots.

b) Anomaly based detection

Anomaly based botnet detection techniques work on the basis of some flaws found in networks and such flaws may be high amount of network latency(High reaction time), sudden flow of massive amount of network traffic, presence of data traffic on unusual ports, abnormal behavior of computer system or network devices. All these reasons sufficiently give indication of bot activity. Even though it has the capability to detect unknown botnets but is incapable to detect that IRC network which has not yet been used for attack purpose. In [25] the author mentions about Botsniffer software which works on the basis of anomaly detection.

c) DNS based detection

The DNS based approach is a kind of passive detection technique. In such techniques there is full transparency but are not known to botherders. DNS based approach is based on the property that in order to access the C&C server, bots carry out DNS queries to locate the particular C&C server that is typically hosted by DDNS(Dynamic DNS) provider. So DNS monitoring will be easy approach to detect Botnet DNS traffic and detect DNS traffic anomalies. This is most famous and easy technique of botnet detection [22].

d) Mining based detection

The data mining based technique helps in recognizing the useful patterns to find out certain type of regularities and irregularities in available datasets. Data mining techniques can be used for the purpose of optimization. In this method the sufficient amount of data is obtained from the network log file to work upon and analyse. The various data mining methods are correlation, classification, clustering, statistical analysis and aggregation for extracting the useful information from the available data[22].

V. PROPOSED BOTNET ANALYSIS FRAMEWORK

The meaning of the word detection is to detect any abnormal activity and take measures to prevent it. The proposed framework presents the comparative analysis of the models presented by different researchers and suggests the useful measures in the direction of botnet detection.

The proposed model divides the process of bot detection into series of steps which starts from pre identification phase.

There are three major steps involved in the proposed model :-

5.1 Pre Identification

The pre Identification means the steps that can be taken before starting the botnet detection process. It includes :

- Security tools Preprocessing
- Reorganization
- Collection
- Preservation
- Retention

In security tools preprocessing the installed security tools are analysed and the problem is identified. In reorganization step, a setup is prepared, various networking tools are arranged and organized to make an environment ready to generate the network traffic. An available tool may be used to collect the network packets from the traffic flown in the network. The packet or dataset collection is done and the dataset is preserved safely. Once the dataset preservation is performed, it must be retained in the form of backup and its safety is ensured so that no one should tamper or harm the collected data. The various steps are shown through figure 4.

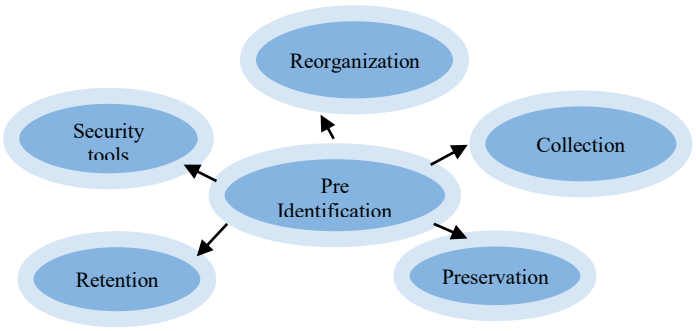

Figure 4. Pre Identification Phase

5.2 Identification Phase

In identification phase or process the data is identified and captured by using the available tools. The figure 5 shows identification phase.The various tools that may be used for data capturing may be Wireshark, NS2, Tcpdump, Botnet Simulator(BoNeSi). Then begins the detection phase in which the classification of data is performed. The different types of methods are employed such as machine learning, clustering, regression and association etc and then the next step is for mitigation of the problem and forensics analysis. Machine learning focuses on the development of such computer applications that can train themselves to grow and change when exposed to new form of information. Clustering is the unsupervised classification of patterns (observations, data items, or feature vectors) into groups (clusters). The regression analysis is used to find the relationship between the dependent variable (target field) and one or more independent variables. The dependent variable is the one whose values you want to predict, whereas the independent variables are the variables that you base your prediction on. *Association* rules are those

statements that help unveil relationships between seemingly unrelated *data* in a relational database or other information datasets.

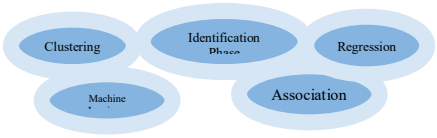

Figure 5.I dentification Phase

VI. CONCLUSION AND FUTURE CHALLENGES

In this paper we have tried to review the current state of botnets and to understand how botnet works and propose a detection framework to develop the efficient botnet detection system. The proposed process model or framework is a complete model that can be used for detecting the bots and analyzing them. The test bed environment consists of series of steps that can be easily implemented and fruitful result may be obtained from them. The method is quite simple and useful.

Several botnet studies are based on botnets detection techniques. There is hardly any methodical study about botnet anticipation and alleviation. More studies on botnet prevention are required that can extend support to spot botnets in their early stages. On the other hand, more studies about how to mitigate and respond after finding trails of an infection. Therefore, prevention and mitigation are striking challenges in this field.

VII. REFERENCES

[1] A. Bijalwan and E. S. Pilli, "Understanding botnet on Internet," in Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on, 2014, pp. 1-5.

[2] K. Singh ,S. Chandra Guntuku , A. Thakur , C. Hota "Big Data Analytics framework for Peer-to-Peer Botnet detection using Random Forests" , Information Sciences 278 (2014) 488–497, March 2014

[3] M. Cremonini and M. Riccardi, "The Dorothy Project: An Open Botnet Analysis Framework for Automatic Tracking and Activity Visualization." , University of Milan Milano, Italy

[4] H. Rouhani Zeidanloo, A. Bt Abdul Manaf, R. Bt Ahmad, M. Zaman, "A Proposed Framework for P2P Botnet Detection", IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April 2010

[5] M. Riccardi, D. Oro and J. Luna, "A Framework For Financial Botnet Analysis" Barcelona Digital Technology Centre Barcelona, Spain jluna@bdigital.org

[6] H. Rouhani Zeidanloo, A. Bt Manaf, P. Vahdani, F. Tabatabaei, M. Zamani ," Botnet Detection Based on Traffic Monitoring", 2010 International Conference on Networking and Information Technology"

[7] Alden W. Jackson, D. Lapsley, C. Jones , SLINGbot: A System for Live Investigation of Next Generation Botnets, BBN Technologies ,10 Moulton Street Cambridge, MA 01845, USA

[8] C. Mazzariello ,University of Napoli Federico II, "IRC traffic analysis for botnet detection", The Fourth International Conference on Information Assurance and Security

[9] H. Rouhani Zeidanloo, A. Bt Abdul Manaf, "Botnet Detection by Monitoring Similar Communication Patterns", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, 2010

[10] W. Lu, M. Tavallaee and A. A. Ghorbani, "Automatic Discovery of Botnet Communitieson Large-Scale Communication Networks" University of New Brunswick Fredericton, NB E3B 5A3, Canada

[11] A. K. Soodn, R. J. Enbody, "Crimeware-as-a-service—A survey of commoditized crimeware in the underground market", Internation al journal of critical infrastructu protection vol - 6(2013) p 28 – 38

[12] D. Zhao , I. Traore , B Sayed , W. Lu , S. Saad ,A.Ghorbani , D. Garant, "Botnet detection based on traffic behavior analysis and flow intervals", computers & security, 39 (2013) 2 -16

[13] T. Ormerod, Lingyu Wang, Mourad Debbabi," Thomas Ormerod, Lingyu Wang, Mourad Debbabi", National Cyber-Forensics and Training Alliance CANADA

[14] E. Stalmans, "A Framework for DNS based detection and mitigation of malware infections on a network", Security and Networks Research Group Department of Computer Science Rhodes University Grahamstown,South Africa

[15] L. Mendonça, H. Santos," Botnets: A Heuristic-Based Detection Framework", Centro ALGORITMI University of Minho Braga, Portugal

[16] N. Paxton, G. Ahn, B. Chu, "Towards Practical Framework for Collecting and Analyzing Network-Centric Attacks", University of North Carolina at Charlotte

[17] R. Ahmed, R. V. Dharaskar, " Study of Mobile Botnets: An Analysis from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices", National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012)

[18] U. Wijesinghe, U. Tupakula, V. Varadharajan, "An Enhanced Model for Network Flow Based Botnet Detection" , Proceedings of the 38th Australasian Computer Science Conference (ACSC 2015), Sydney, Australia, 27 - 30 January 2015

[19] L. Yeh, Y. Tsai," An Automated Framework for Command and Control Server Connection and Malicious Mail Detection" ICNS 2015 The Eleventh International Conference on Networking and Services

[20] R. Shirazi, "Botnet Takedown Initiatives: A Taxonomy and Performance Model", Technology Innovation Management Review, January 2015

[21] P. Sharma, S. Tiwari, A. Bijalwan, E. Pilli, "Botnet Detection Framework", International Journal of Computer Applications (0975 – 8887) Volume 93 – No.19, May 2014

[22] H. Singh and A. Bijalwan, "A survey on Malware, Botnets and their detection," International Journal of Advanced Engineering Research and Science (IJAERS), vol. 03, no. 03, 2016.

[23] B. Anchit and S. Harvinder, "Investigation of UDP Bot Flooding Attack," Indian Journal of Science and Technology, vol. 9, no. 21, 2016.

[24] A. Bijalwan, M. Wazid, E. S. Pilli, and R. C. Joshi, "Forensics of random-UDP flooding attacks," Journal of Networks, vol. 10, no. 5, pp. 287-293, 2015.

[25] Sultan, M. Shahid. Monitoring HTTP based Command and Control Botnets in Network Traffic using Bot-Sniffer. Diss. Texas A&M University-Corpus Christi, 2015.