IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN OVERVIEW OF BOTNET AND ITS DETECTION TECHNIQUES

Sarath R Mammunni[1] , Sandhya C P[2]
M.Tech. Scholar[1],Assistant Professor[2]
Department of Information Technology[1],Department of Information Technology[2]
Toc H Institute of Science & Technology,Kerala,India[1,2]

Abstract:
Now a days, botnets are intensifying as a serious issue in digital world. Due to the increase in internet usage, the illegal activities like hacking, spamming, phishing, distributed denial of attack (DDoS) , malware dissemination and click fraud are tremendously increasing globally. It's impact affect the personal life and the whole business which causes the worst consequences. Botnets are collection of compromised internet-connected computers under the control of a small number of bot-masters. They create a major threat to Internet's communications and applications. The bot-masters gradually raises the botnet propagation and get away from the latest detection techniques. For communication between its members, botnets relies on command and control (C&C) communication channels. Today botnets are controlled using different protocols such as Internet relay Chat (IRC) , HTTP and P2P for transmission and initiate attacks. Since the botnets are distributed and small, it's very hard to find and destroy it. So, many research works have been proposed different detection techniques and various research works are going on about botnet detection in cyber world, which is a challenge in future. In this paper we are discussing about the botnets, its architecture & characteristics and some of its specific detection techniques in detail.

Keywords*: Botnets, Botnet Architecture, Honeynet, Passive-Netwrok-Traffic-Monitor.*

1. INTRODUCTION

In recent years, botnets are considered as the major threats to the digital world. As our environments are being changing, the securities related to our assets and organizations are becoming very complex. Hackers are using botnets to breach our network securities and making serious threats to our personal life and organizations. Bonet is a collection of internet-connected devices, which is used to perform Denial of Service attacks(DDos) and allows the hackers to get control of other devices. Bonet is defined as a collection of software "robots" that operates on host computers automatically and controlled remotely by a third person/attackers [1]. It is comes from the words "Robert" and "Network". Each devices on the networks acts as a 'bot' and is controlled by an another person for performing some attacks. Bots is sometimes defined as small codes/programs that automatically run on a host device, which perform some illegal activities to damage the system without legal user's knowledge. Since these devices are controlled by some other than its owner, its is also known as Zombie Army[2].

Botnets are the collection of large networks of bots. Botnets are set up by a person/group of persons which controls remotes bots is known as Botmasters. Once the botnet's attack occurred the common tasks executed by bot masters are [3]:

- Spamming emails to millions of Internet users.
- Generating fake Internet Traffics.
- Distributed denial-of-service attacks to other machines.
- Removing/replacing/adding ads in your webpage specially targeted at you.

Many research works showed that botnets are the base of all cyber and malware attacks in this internet world. [4][5]. Using the distinguished communication protocols like IRC,HTTP and P2P, botmaster can take control of other devices according to their desire. Botmasters are using different methods like open an email attachments, downloading hazardous softwares and click on malicious ads to infect the user devices. 6][7]. The detection of botnet are very difficult and complex, various effective approaches are proposed by researchers in various fields.

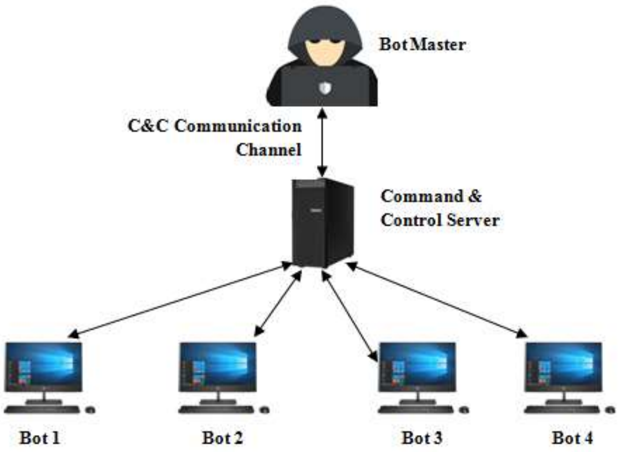

Figure 1: Botnet Netwrok

In this paper, different malware detection approaches are discussed along with its advantages and disadvantages.
The remaining sessions is organized as follows: Section II describes about basic botnet architecture and its structural, technological and behavioral characteristics. Section III discussed about the classification of botnet detection techniques. In this section mainly concentrated on Honey-Based and Passive Network Traffic Monitor methods. Discussion and conclusion included in section IV.

2. BASIC BOTNET ARCHITECURE

The basic Botnet architecture consists of Botmaster, C&C architecture, Malicious activities and Victims (Figure 2).

Botmaster: Botmaster is a person/group of persons who remotely controls the botnets and issuing commands to C&C servers and bots with in a network. He is also called as botnet controller or bot herder.

Bot: Bot is an internet-connected individual devices within botnet network. It can be a personal computer, laptops, smart phones, tablets or IoT devices and so on are infected by a backdoor programs/softwares. It receives commands directly from botmaster through C&C servers. Another name for bot is Zombie. A botnet is also called as Zombie army.

Command & Control Server: It comprises of several servers and other technical components which issue the commands from botmaters to bots and receive the information back from the bots. It normally be abbreviated as C&C servers.

Malicious activities : The illegal activities in botnet attacks includes spam generation, distributed denial of attacks (DDoS),unauthorized access, phishing, credentials leaks, and data theft.

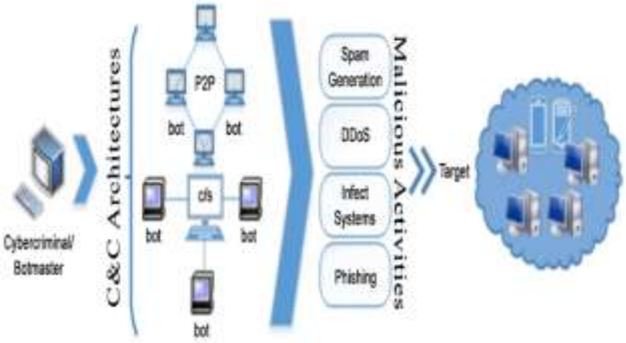

Figure 2[8] : Basic Botnet Architecture

2.1 How Botnets does works?

Step 1: The botmaster sends out malware through suspicious email attachments, ads/links in social medias, downloads to infect targets.

Step 2 : Theses bot malwares will make use your system software's vulnerabilities and entering through backdoor access via your outdated plug-in or an out of date operating system.

Step 3: Once the botmaster gets the whole control of the system he/she sends instructions to the bots through command & control server. In this stage the bot herder starts carrying out malicious activities.

Step 4: In the meantime, botmaster will try to expand the botnet by adding more and more zombies without the knowledge of legal users.

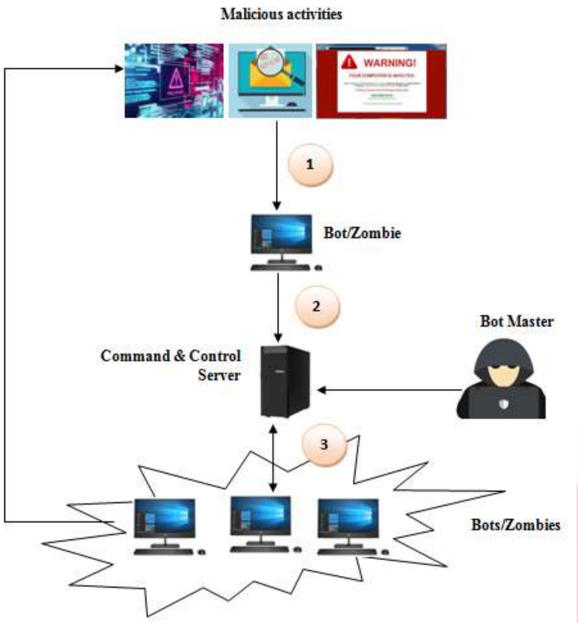

Figure 3: Working Of Botnet

III. CHARACTERISTICS OF BOTNETS

The characteristics of botnets can be classified on the basis of their structure/topology, technology and behavior.

3.1 Structural Characteristics:

It means the architecture/topology on which the boot master controls the victims through C&C servers. It allows the connection between boots and botmasters and other members. Actually botnet topology refers to the way in which C&C server is organized in between zombies and a botmaster. Based on the C&C communication, there are two possible sophisticated ways for the bots to receive their orders. (i) Centralized and (ii).Decentralized.

3.1.1 Centralized architecture: A centralized architecture enables the communication between all bot agents and bot controller via centralized server. Each bot agent is issued new instructions directly from the central C&C point [9].
Different centralized topologies used in botnets are Star, Multi-Server & Hierarchical.

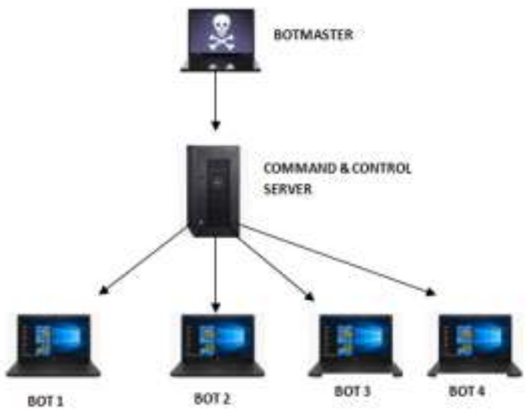

Figure 3: Centralized Architecture

In star topology, direct communication between centralized server and bots.

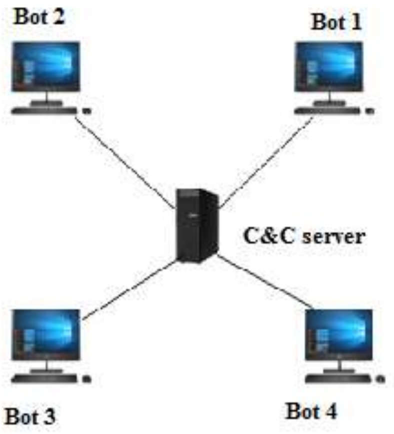

Figure 4: Star Topology

Instead of one server, multiple servers are used to give commands to bots in multi-server topology.

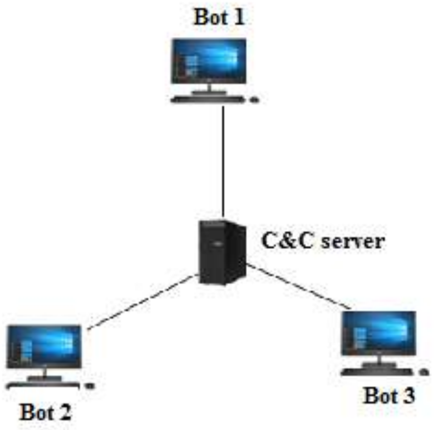

Figure 5: Hierarchical Topology

In hierarchical topology, bots are not awareness of the location of servers

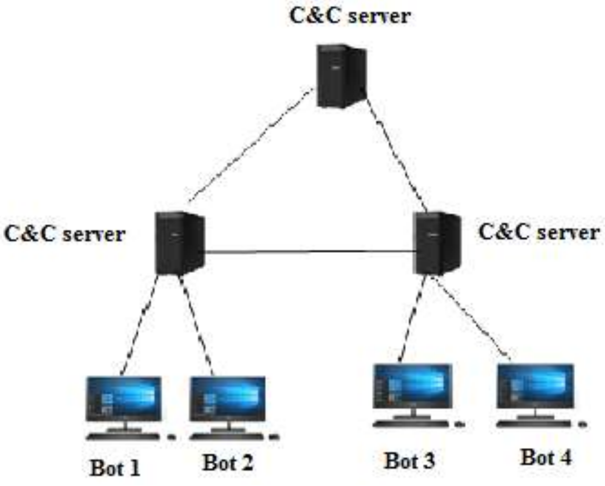

Figure 6: Multi-Server Topology

3.1.1.1 Proxy architecture: In some cases finding the C&C server is very harder. In this case bot creators uses proxies as intermediate machines that serves to connect to individual bots. These proxies either act as a bootmaster servers or malicious machines themselves. The main advantage of this architecture is (i). Making the infrastructure more resilient and (ii) analyzing of defenders making easy for finding C&C server.[10]

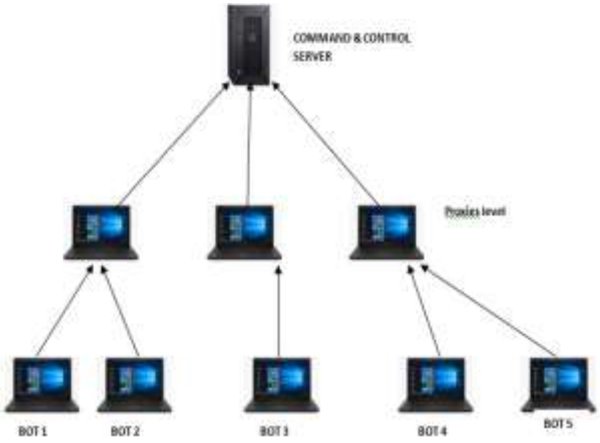

Figure 7: Proxy Architecture

3.1.2 Decentralized architecture: If the C&C server crashes in centralized architecture, the bot master fails to communicate with the bots. Hence decentralized architecture is used by the botnet to pass commands to its zombies. In decentralized architecture every devices in the network are communicate each other. Botnet uses P2P decentralized architecture as a better choice for its purpose.

3.1.2.1P2P Architecture

In P2P architecture bots are directly contact each other instead of C&C server. Here a node can acts as a client as well as a server and there is no centralized point of communication. Bots itself propagating Information and control commands in the network. For maintain control over the botnet, its master only needs to be able to contact any infected machine. In this architecture, no coordination among the bots are needed and if any node crashes, the network still handled by the attacker itself.

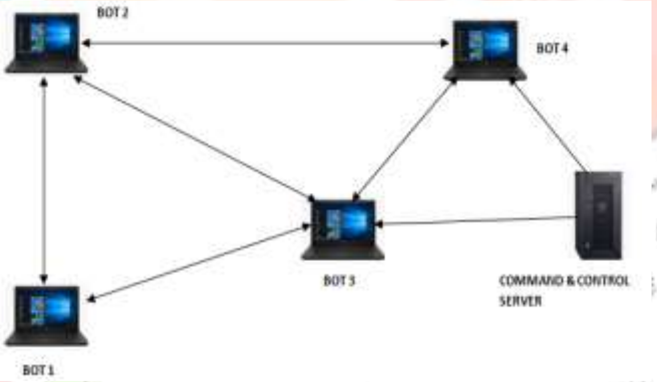

Figure 8: P2P Architecture

3.2 Technological Characteristics

The data’s and commands are carrying through channels. The bot controllers in a botnet are able to give commands to infected computers through a communication channels formed by standards-based network protocols, such as IRC, Hypertext Transfer Protocol (HTTP) and P2P[11][12].

3.3 Behavioural Characteristics

The behavioural characteristics of botnet include the attack behavior and operational behavior. The main attack behaviour of botnets are e-mail spamming, phishing, Distributed Denial of attacks, Financial fraud, Data exfiltration, Bitcoin mining and so on. The operational behavior includes the characteristics of C&C servers and communication methods, botmaster behaviour and intention

IV. BOTNET DETECTION METHODS

We can say that bots are the platform for the sharing of different threats like Trojan, backdoors etc. The bots is designed to perform the activities without users knowledge. This make the Botnet detection become very difficult. However, there are some signs for the infected computers with botnet malwares include IRC traffic, identical DNS request ,slow computing /high CPU usage, outbound messages, problems with Internet access [13] .Basically various Botnet detection methods can be used to detect botnets illegal activities. In this paper we explained about the following detection methods:

(i) Honeynet-based approach
(ii) Passive network traffic monitor / Intrusion and detection (IDS) method.

4.1 Honeynet-based botnet detection

A honeynet is a network that focuses for potential attackers and diverts them from their production network. Here, attackers will not only find vulnerable services or servers but also find vulnerable routers, firewalls, and other network boundary devices, security applications, and so forth. Honeynet-Based again divide into two

(i) Honeypot
(ii) Honey-well

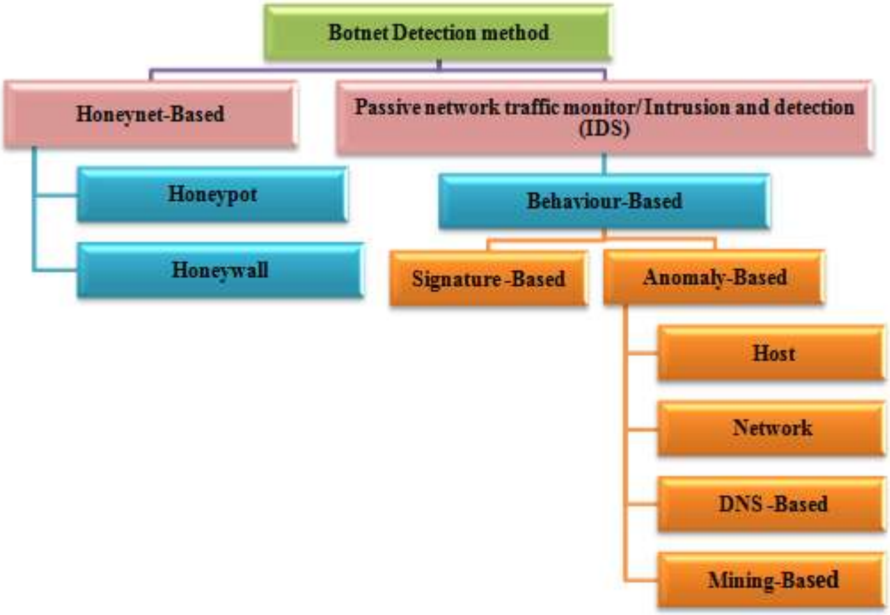

Figure 6: Botnet Detection Methods

4.1.1 Honeypot

Honetpot is the security mechanism to detect the unauthorized usage of information systems. It collects more information's about bots illegal activities and study about bots characteristics and botmasters intensions. They are vulnerable systems always waiting for attacks. Based on the design criteria, honeypots can be classified as :

(i) Pure Honeypots
(ii) Low-Interaction Honeypots
(iii) High-Interaction Honeypots.

Pure Honeypots is a full-fledged production system where no installed software is needed for monitoring the communication between honeypot and the network. But still there is a risk of attack by hackers by making honeypot as attacking platform.

Low-interaction honeypot provides only limited services or operating systems with a low level of interaction[14]. The advantage of this is ease of installation and configuration with low risk. And also easy to detect by expert attackers which may lead to more aggressive attacks against our network.

In High-interaction honeypots allowing the attacker to interact with a real system. This type is more difficult to organize and configure, also the risk is higher here since attackers can take full manage over the machine and may use it to start other attacks that may go through our production network or to take it as a zombie to generate attacks on the internet. The risk of deploying tends to be higher, so it is required to establish precautions and special provisions to prevent attacks against the system, more complex to setup and maintain. The main intention is to understand the attack scene, concerned that the attacks on the process, it requires a strong ability to interact with the attacker. The most common setup for this kind of honeypots is a GenII Honeynet[15].

Advantages:

- Any node can be used as honeypot systems.
- Always monitoring the traffic and illegal activities makes the investigation easier.
- Gathering the information about attacks that may happen in future.

Disadvantages:

- Honeypots fails to identify the attacks, when attacks occurring in other bots.
- It’s very easy for an experienced hacker to attack the honeypot systems.
- Honeypot can be used as other bots to collect information about others in the network.

4.1.2 Honey-Wall

Honeywall approach is the easiest way to protect the honeypots from malicious abuses by an attacker. It can be considered as the gateway in Honeypot. It collects the complete to and from traffic information of the Honeynet system. The Honeywall enables the following task of a honeynet.

- *Data Capture:* All actions within the honeynet and the entering and leaving data’s of the honeynet should be captured without attackers knowing they are monitored.
- *Data Control:* The main goal of data control is to protect the internet from compromised honeynet systems. It controls suspicious traffic entering or leaving the honeynet.
- *Data Analysis:* It analysis all the captured data and help us to analysis the network malwares.[16]

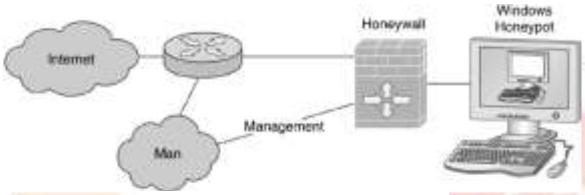

Fig 7 [16] : Honeywall Setup

Advantages:

- It is a device which acts as a gateway through which the network traffic are passing. So its very easy to analysis the network traffics.
- It control, capture, analysis the network traffic and alerting about the same.

Disadvantages:

- It needs firewall to validate the authenticity of users [17].

4.2Passive Network Traffic Monitor

The monitoring of network traffic plays an significant role for the detection in Passive Network Traffic Monitor,. Monitoring can be done either in active or passive mode. By observing the rate of packets injected into the malicious network helps to decide whether the bot or human is in charge of the session[18]. In this technique, the individual bots are detected by checking the traffic patterns or content that can reveal the command and control (C& C) server or malicious in bots-related activities. If the result of the traffic analyzing process indicates two or more hosts with similar patterns means the bots react the same function.

4.2.1 Behaviour Based detection Methods

We can classify the behaviour based detection techniques as Signature-based as well as anomaly-based detection techniques. Anomaly is again classified as Host and Network detection methods.

4.2.1.1 Signature-based detection

Signature-based detection is the simplest form of detection which uses the signatures/specific pattern such as byte/instruction sequences in network traffic for botnet detection. In these methods, it compares the network traffic with the signature database. If the comparison result of signature is match then the alert is generated, if not the traffic flows without any problem. This technique learns and gains knowledge from the signatures or behaviours from existing botnets [19]. This method is useful for detecting on well-known botnets accurately but the unknown bots. Signature database needs to be updated constantly. If not the IDS systems will fail to detect some of the intrusion attacks.

Advantages :

- Detect zero possibility towards fake or false positive immediately.
- Requires less amount of system resource for detection.
- Detect well known botnets.

Disadvantages:

- Unknown botnet's can't be detect.
- Have very little information about previous requests when processing the current ones.

4.2.1.2 Anomaly-based detection

In this technique, each behaviour or anomaly of botnets are compared with a created model of trustworthy. It is also used to detect intrusion and misuse of network and computer by monitoring the network traffic anomalies. The anomalies includes high network latency, high volume traffic, traffic on unusual ports and unusual system behaviour that can indicates any presence of malicious bots in the network[20].It mainly focuses on normal behaviour to overcome undetected unknown attack. It is capable of detecting the unknown botnets and previously unknown attacks, which overcomes the disadvantage of Signature-based detection method. .

Advantages:
Detect unknown botnets.

Disadvantages:

- High false positive alarm rate.
- Efficiency of the system depends how the protocols are implemented and tested.

Anomaly –based detection can be divided into following categories :

- Network-Based
- Host-Based
- DNS-Based
- Data- Minig-Based.

4.2.1.2.1 Network-Based IDS

Network intrusion detection systems (NIDS) attempt to identify attacks of cyber, malware, denial of service (DoS) attacks on a computer network or a computer itself. They are very easy to secure and can be more difficult for an attacker to detect. It identifies the suspicious activities from the network reported either to an administrator or collected centrally using a security information and event management (SIEM) system. SIEMS system works with the help of a multiple collection agents to gather security related information's and raise security issues faced by the network. By giving a large amount of data that NIDS have to analyze, they do have a somewhat lower level of specificity.

4.2.1.2.2 Host-Based IDS

It operates similar to the NIDS, but it capable for monitoring the internals of a system and network packets on a network. It is an application monitoring a computer or network for suspicious activity, which can include intrusions by external actors as well as misuse of resources or data by internal ones. Host-based intrusion detection systems (HIDS) help organizations to identify threats inside networks by monitoring host devices for malicious activity that, if left undetected, could lead to damage and disruption. It consists of a log and all suspicious activities are recorded in the log and report to administrator. It is also called as automated detection tools.

4.2.1.2.3 DNS-Based IDS

The Domain Name System (DNS) is the directory of all the device names of a network, including the huge network. Every host having IP address through which its serving the contents to the users.

In the paper [21] the author proposed an anomaly-based detection system by considering the common activities in DNS traffic called BotGAD (Botnet Group Activity Detector). In his work migration of C&C server is detecting using this detector. The drawback of this method is that it requires more computational power to monitor the enormous amount of network traffic adequately [22]. In another work[23] the author has proposed two different approaches to identify the C&C server through the analysis of DDNS (Dynamic DNS) traffic. The first approach depends on the filtering all domains, which has abnormally high DDNS query rate. It indicates that the botmaster is frequently migrating the C&C server to different IP. In the second approach, the author is trying to decontaminate the unusual recurring DDNS replies. The query indicates that the bot is trying to connect with the C&C server, which has already been taken-down using sink-holing techniques [24].

Advanatges:

- Identify the C&C botnets.
- Irregular and common DNS traffics are separed [24].
- Detect botnets from large scale networks.

Disadvantages:

- Detection method is complex.
- Increase the number of bots.
- Large processing time.

4.2.1.2.4 Data Mining-Based IDS

Data mining refers to the extraction/mining of data from a large amount of data. The main reason for incorporating data mining with IDS are the datasets are very huge, constructing IDS manually is very expensive and slow and frequent updating requires. Some of the datamining techniques used that have been applied for IDS are Feature selection and Machine Learning. Feature selection, also known as subset selection or variable selection, is a process commonly used in machine learning, wherein a subset of the features available from the data is selected for application of a learning algorithm. Machine Learning is the study of computer algorithms that improve automatically through experience. Applications range from data mining programs that discover general rules in large data sets, to information filtering systems that automatically learn users' interests. In his work different categories of techniques – Statistical techniques, Clustering Techniques, Neural Networks, Support Vendor Machine, Immunological based Techniques are proposed for enhancing IDS via Datamining. [25].

In the paper [26],the authors proposed robust and effective flow-based botnet traffic detection by mining multiple log files. They introduce multiple log correlation for C&C traffic detection. They classify an entire flow to identify botnet C&C traffic. This method does not impose any restriction on the botnet communication protocol and is therefore applicable to non- IRC botnets. Furthermore, this method does not require access to payload content. Hence, it is effective even if the C&C payload is encrypted or is not available.[27]

Advantages: [28]

- Botnet detection for large amount of data.
- Effective method for internal patterns.
- Network filtering is possible.

Disadvantages:

- Response time and time duration not considering.
- Filtering process is not implemented for dynamic environments.
- Source and destination ports are not considered.

V. CONCLUSION

This paper has presented an overview of Botnet and its architecture and characteristics .We focused mainly on the classification botnet detection methods with its advantages and disadvantages As mentioned in this paper, the main highlight of botnets is the ability to provide anonymity through the use of a multitier command and control (C&C) architecture. In this paper botnet detection techniques based on passive network traffic monitoring are classified into four classes including Signature-Based, Anomaly-Based, DNS Based, and Data-Mining Based. Signature-based techniques can only detect already known botnets, whereas the other classes are able to detect unknown bots. However, most of the current botnet detection techniques depends on specific botnet C&C communication protocols and structures. As a result, as botnets change their C&C communication architecture, these methods will not be effective.

REFERENCES

[1] Zhaosheng Zhu, Guohan Lu, Yan Chen, Zhi Judy Fu, Phil Roberts, and Keesook Han. 2008, Botnet research survey. 32nd Annual IEEE International Computer Software and Applications Conference, pages 967–972,

[2]. https://blog.eccouncil.org/botnets-and-their-types/

[3]. https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

[4]. "Botnets The New Threat Landscape White Paper [Threat Control] - Cisco Systems." .

[5]. M. Zahid, A. Belmekki, and A. Mezrioui, May 2012 ,"A new architecture for detecting DDoS/brute forcing attack and destroying the botnet behind," 2012 Int. Conf. Multimed. Comput. Syst., pp. 899–903,

[6] W. Paper, "Anatomy of a Botnet."

[7] "Microsoft Security Intelligence Report," vol. 15, 2013.

[8]. Ahmad Karim1*, Rosli Salleh1, Muhammad Khurram Khan2, "SMARTbot: A Behavioral Analysis Framework Augmented with Machine Learning to Identify Mobile Botnet Applications", 2016, Article in PLoS ONE, DOI: 10.1371/journal.pone.0150077

[9]. Botnet Detection Literature Review, Benoit Jacob, Edinburgh Napier University School of Computing 2008

[10] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets

[11].*Ramneek, Puri (8 August 2003). "Bots &; Botnet: An Overview" (PDF). SANS Institute. Retrieved 12.*

[12]. *Putman, C. G. J.; Abhishta; Nieuwenhuis, L. J. M. , "Business Model of a Botnet". 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP): 441–445. arXiv:1804.10848. Bibcode:2018arXiv180410848P. doi:10.1109/PDP2018.2018.00077. ISBN 978-1-5386-4975-6.2018*

[13] https://www.veracode.com/security/botnet

[14]. A. Jakalan, G. Jian, and L. Shangdong,"DISTRIBUTED,2011,LOW-INTERACTION HONEYPOT SYSTEMTO DETECT BOTNETS,"InternationalConference on Computer Engineeringand Technology, 3rd (ICCET 2011).

[15] "The Honeynet Project. Know YourEnemy : Learning about Security Threats.Addison-Wesley Professional; 2 edition(May 17, 2004),.

[16].http://books.gigatux.nl/mirror/honeypot/final/ch02lev1sec5.html

[17] S. Nagendra Prabhu, S. Shanthi, R. Nidhya June 2019," A Virtual Honeynet Based Botnet Detection (Vhbd) Architecture for Cloud", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5,

[18]. Rishikesh Sharma, Abha Thakral," Identifying Botnets: Classification and Detection", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-9S,

[19] Feily, M., A. Shahrestani and S. Ramadass, 2009 . A survey of botnet and botnet detection. Proceedings of the 3rd International Conference on Emerging Security Information, Systems and Technologies, June 18-23, 2009, Glyfada, Athens, Greece, pp: 268-273.

[20]. Zeidanloo, H.R. and A.B.A. Manaf2010.,. Botnet detection by monitoring similar communication patterns. Int. J. Comput. Sci. Inform. Secur., 7: 36-45. Direct Link,

[21]. H. Choi, H. Lee, and H. Kim, 2009, "Botgad: detecting botnets by capturing group activities in network traffic," in Proceedings of the Fourth International ICST Conference on COMmunication System software and middlewaRE. ACM, p. 2.

[22] M. Feily, A. Shahrestani, and S. Ramadass, 2009,"A survey of botnet and botnet detection," in 2009 Third International Conference on Emerging Security Information,System and Technologes,IEEE,pp. 268-273.

[23] R. Villamar´ın-Salom´on and J. C. Brustoloni, "Identifying botnets using anomaly detection techniques applied to dns traffic," in 2008 5th IEEE Consumer Communications and Networking Conference. IEEE, 2008, pp. 476–481.

[24] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna,2009, "Your botnet is my botnet: analysis of a botnet takeover," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, pp. 635–647.

[25]. E.Kesavulu Reddy, Member IAENG, V.Naveen Reddy, P.Govinda Rajulu, July 6 - 8, 2011" A Study of Intrusion Detection in Data Mining".proceedings of the World Congress on Engineering 2011 Vol III WCE 2011, , London, U.K

[26]. M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, K. W.Hamlen, 2008," Flow-based identification of botnet traffic by miningmultiple log file," in Proc. International Conference onDistributed Frameworks & Applications (DFMA), Penang,Malaysia.

[27]. Mr. Sandip Sonawane, -2018" A Survey of Botnet and Botnet Detection Methods", International Journal of Engineering Research & Technology (IJERT)http://www.ijert.org ISSN: 2278-0181IJERTV7IS120024, Vol. 7 Issue 12, December".

[28]. M. Thangapandiyan1 , P. M. Rubesh Anand2*," BOTNET DETECTION TECHNIQUES IN CLOUD COMPUTING ENVIRONMENT: A SURVEY", International Journal of Pure and Applied Mathematics, Volume 118 No. 22 2018, 929-939 ISSN: 1314-3395 (on-line version) url: http://acadpubl.eu/hub Special Issue