IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

3rd-International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2024)

Geetanjali Institute of Technical Studies

Vol. 11, Special Issue 2, May 2024

Botnet and Detection Technique: A Survey

Kamlesh Tiwari

Lecturer, CTAE, MPUAT, Udaipur, India

Abstract: The most pervasive and dangerous type of malware that frequently appears in today's cyber-attacks is the botnet. A botnet is a collection of compromised machines that hackers may remotely manage to carry out different types of network assaults, such as spam, identity theft, DDoS attack and information phishing. A common and effective weapon used in many cyber-attacks is the botnet. The utilization of command and control channels for updating and directing botnets is their distinguishing feature. Malicious botnets have recently evolved from common IRC botnets to HTTP botnets. Characteristics from massive amounts of data can be automatically detected using data mining algorithms, something that was not possible with traditional heuristics or signature-based techniques. The primary problem is: how can these botnets be found? Does cyber-security research grow increasingly intriguing to researchers? This encourages us to investigate botnet architecture and detection methods in our review.

Keywords*:* detection methods, botnet architecture, HTTP Botnet, botnet attacks, bots, botnet, botmaster, Data mining.

I. INTRODUCTION

A botnet is a network of infected computers. Zombies or bots are other terms for compromised computers. Most of this software is written in C++ and C. The primary driver of botnet activity is the introduction of a new type of criminal activity known as cybercrime by the shadowy internet community.

It is commonly acknowledged that network bandwidth and computation, as well as parallel and distributed computing, have improved and advanced. Thus, it is evident that hackers have targeted them [1]. A botnet is a group of computers connected to the internet whose security has been compromised and control has been given to the blackhat community, a malevolent group. One or more attackers going by the handle "Botmaster" are in control of the compromised computer group [2]. The combined strength of numerous bots can be leveraged by botnet operators to significantly increase the impact of those risky acts. While a single bot might not pose a threat to the Internet, a network of bots can undoubtedly cause significant disruptions.

II. BOTNET LIFE CYCLE

There are five steps involved in creating and maintaining a typical botnet: initial infection, secondary injection, connection, malicious command and control, update, and maintenance.

In Fig. 1, this life cycle is shown.
1) Initial Infection: Using various exploitation techniques, the attacker first looks for known vulnerabilities in a target subnet before infecting victim computers. techniques including email attachments, USB autorun, downloading binary files from websites, and some malicious software [11].

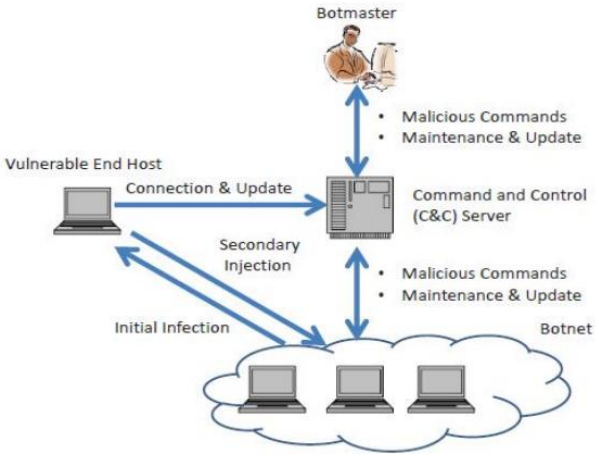

Fig.1 Botnet Life Cycle

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

3rd-International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2024)

Geetanjali Institute of Technical Studies

Vol. 11, Special Issue 2, May 2024

2) Secondary Injection: The compromised hosts run a script that is referred to as shell code. It uses FTP, HTTP, or P2P to download this binary from a specified site. Once the malware is installed, the intended computer turns into a "Bot," also referred to as a "Zombie."

3) Connection: The bot program creates a command and control (C&C) channel and links the zombie to the C&C server during the connection phase. Once the C&C channel is established, the zombie joins the attacker's botnet army.

4) Command and Control: At this point, real botnet activity has begun. The Botmaster gives orders to his army of bots over the C&C channel. To prevent a single point of failure, the command communication can be done using P2P protocol, HTTP, DNS, or IRC. Programs known as "bots" take orders from BotMaster and carry them out. The botmaster can remotely command a large number of bots to carry out a variety of illegal operations thanks to the C&C channel.

5) Updating and Maintenance: It is instructed for bots to be active and updated. Therefore, if a new method for finding and controlling is discovered, the control center (Botmaster) can upgrade it by adding new features or new methods. The bots are occasionally moved to a new C&C server by the upgraded binary. Server migration is a highly helpful method that helps botmasters maintain their botnet.

III. BOTNET ARCHITECTURES

Based on their architectural designs, the individual bots that make up a botnet can be divided into three groups. This study presents various techniques for categorizing botnet designs and explains their benefits and drawbacks.

A. Centralized Architecture

The entire document should be in Times New Roman. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.
Recommended font sizes are shown in Table 1.

The centralized design of botnets is the most convenient for the botmaster to administer and control. In a centralized architecture, a command and control server (C&C Server) serves as the single central location from which the botmaster oversees and controls every bot in the botnet. This means that every bot in a centralized botnet architecture receives instructions and reports to a central location known as the C&C server. In centralized botnet architecture, two topologies—star topology and hierarchical topology—are employed. Hyper Text Transfer Protocol (HTTP) and Internet Relay Chat (IRC) are the two main protocols utilized in centralized architecture [6][11] [14]. One central point makes botnet management and monitoring incredibly simple. The botmaster can swiftly and easily communicate directly with the bots. In The centralized design of botnets is the most convenient for the botmaster to administer and control. While message latency and durability are low, the design of the botmaste is less complex in centralized architecture. The C&C server receives commands from the botmaster, and all of the bots in a botnet use these commands. The primary drawbacks of centralized design are its higher failure rate compared to alternative architectures. Due to the central point of control, the botnet as a whole will fail if the C&C server fails[13].

In a similar vein, botmaster identification is quite simple in comparison to decentralized and hybrid infrastructures [8][12].

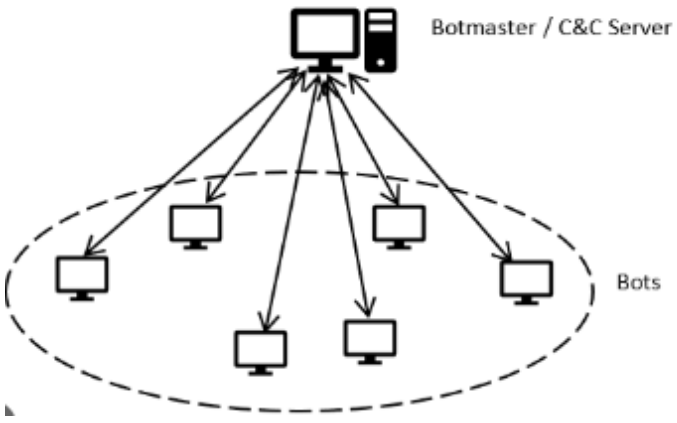

Fig.2 Centralized Botnet Architecture

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

3rd-International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2024)

Geetanjali Institute of Technical Studies

Vol. 11, Special Issue 2, May 2024

B. Decentralized Architecture

A single entity is not in charge of all the bots in a botnet when using a decentralized or peer-to-peer architecture. Multiple C&C servers are in communication with the bots. It is more difficult to detect a botnet with a decentralized architecture than one with a centralized architecture. There is no separate command and control server in a decentralized architecture; instead, every bot functions as both a client and a command and control server[12]. Peer-to-peer protocols form the basis of a decentralized architecture. Peer-to-peer architecture has a more intricate design than centralized architecture, making it more difficult to detect botnets with this type of architecture than others. Likewise, message durability and latency are higher than in centralized botnet design. In decentralized architecture, the likelihood of failure is less as compared to centralized architecture, as two command and control servers can maintain and keep an eye on the botnet in the event of one of them failing.

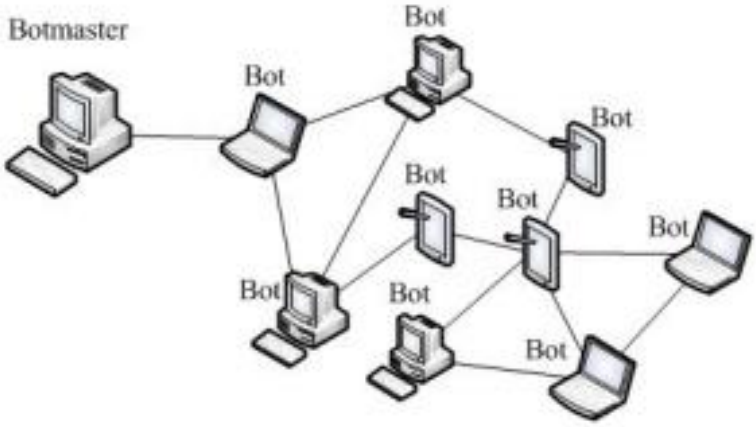

Fig.3 Decentralized Botnet Architecture

C. Hybrid Architecture

The mix of decentralized and centralized architecture is known as hybrid architecture. There are two different kinds of bots in hybrid architecture: client and servant bots [10]. Either as clients or as servants, the bots are linked to the hybrid botnet. tracking and identification of hybrid-architecture botnets are more resilient than botnets with both centralized and decentralized topologies, despite their simple design.

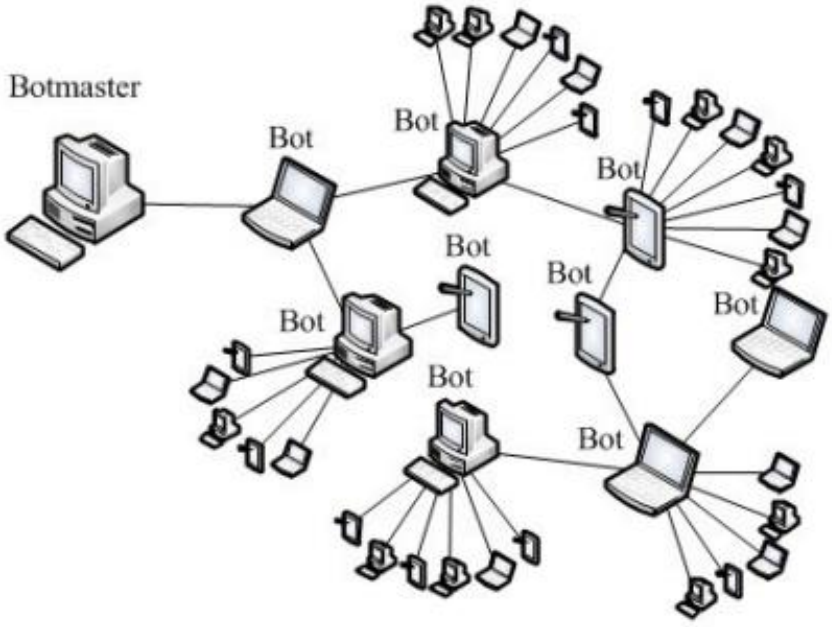

Fig.4 Hybrid Botnet Architecture

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

3rd-International Conference on Muti-Disciplinary Application & Research Technologies (ICMART-2024)

Geetanjali Institute of Technical Studies

Vol. 11, Special Issue 2, May 2024

IV. BOTNET DETECTION TECHNIQUES

Advanced analytical skills related to the chosen data for analysis track and the features of issues executed are frequently required for the detection of botnets. The primary classification can be carried out using used data and network behavior (flow based). Botnet detection in the behavioral method can be achieved by both passive and active analysis. These methods were employed in the early stages of detection, however they are no longer relevant. Krugel et al. detected using data that was used. "The process of identifying and responding to malicious activities targeted at computers and network resources" is the definition of intrusion detection. The Intrusion Detection System (IDS) distinguishes between legitimate system usage and intrusion attempts. IDS-based detection needed additional bandwidth and payload. Well-known tools like Snort and Bro use a lot of resources when handling the massive payload data that modern high-speed networks carry. Often referred to as behavior-based IDS, anomaly-based IDS compares input data to the anticipated behavior of the system. Because unknown assaults are anomaly (irregular) based, the system can identify them; these attacks may produce false positive alerts. Intrusion detection systems are less comfortable than flow-based alternatives. Specialized accounting modules, which are often installed in network routers, keep an eye on flows. Netflow data, also known as Cisco Netflow (n.d.), makes up between %0.1 and %0.5 of all network data consumed [9].

1) Honeypots and Honeynet:
According to Pouget and Dacier (2004), a honeypot is a "environment where vulnerabilities have been deliberately introduced to observe attacks and intrusions." It is a computer system that is meant to serve as a trap to get people to attack it. Every Honeypot has a different idea. These computer systems are worthless for production [9]. Every Honeypot has a different idea. They are very skilled at identifying security risks, gathering malware signatures, and deciphering the intent and method of the threat's perpetrator. For instance, you may place a honeypot web server within your network's demilitarized zone. The restrictions are Small-scale exploitation operations that are able to follow but not capture the bots that are use a propagation technique other than scanning. We can therefore draw the conclusion that, in order to track or examine a machine while utilizing a honeynet for botnet detection, we must first wait for one bot on the network to infect our system.

2) Intrusion Detection System (IDS): There are two primary ways to describe it [9].
a. Signature Based Botnet Detection: Known malware signatures are used by rule-based intrusion detection systems, such as Snort, to detect botnet activity. They keep an eye on network activity and look for indications of intrusions. It is clear that the payload data from network traffic is converted and incorporated into the rule or signature. When malicious traffic fits the communication parameters specified by the rule, the IDS identifies it. A framework called "BotHunter" is proposed by Gu et al. (2007) to correlate IDS-based detection warnings.
b. Botnet Detection Based on Anomalies: This method seeks to identify botnets based on the quantity of anomalous network traffic. Such as high traffic volumes, excessive network latency, and traffic on peculiar ports and peculiar system activity that might indicate the presence of bots on the network. This method can identify unidentified botnets. It falls within the host-based category and Detection Based on Networks. A detection mechanism that is used in host-based detection techniques observes and evaluates a computer system's internal components rather than the traffic on its exterior ports from networks. This system's high false positive rate is a limitation.

A network-based technique is a method of detection that watches network activity in an attempt to find Botnets. Network-based methods can be divided into two groups: active monitoring and passive monitoring. In active monitoring, test packets are injected into the network to gauge its response and generate additional traffic. So it have suggested Botsniffer, which locates Botnet C&C channels in a local area network using network-based anomaly detection.

3) DNS-based detection method: Bots use DNS queries to find the specific C&C server, which is usually hosted by a DDNS (Dynamic DNS) provider, in order to gain access to the C&C server. Thus, DNS monitoring will be a simple method for identifying DNS traffic anomalies and botnet DNS traffic. Although this is the most well-known and straightforward method for detecting botnets, it will be difficult to identify more current, sophisticated botnets using this method.

4) Data Mining Based Detection Technique: Data mining looks for patterns that can be utilized to identify regularities and anomalies in massive amounts of data. Although it comes in a huge file format, packet flow offers all of the flow data information. The majority of anomaly-based approaches are predicated on anomalies in network behavior, such as high latency and activity on unutilized ports [9]. The process of data mining can be used for optimization. It makes it possible to extract from the network log file enough data for analysis. For effectively learning about network flows, the most helpful data mining techniques are correlation, classification, clustering, statistical analysis, and aggregation [12].

Algorithms for flow correlation are helpful for comparing flow objects according to a feature other than packet material. This method works particularly well when the content of packet is unavailable or encrypted; for example, one may compare arrival time. These algorithms make use of the distinctive values as inputs into a function or functions provide a metric for determining if the flows are associated [12]. Algorithms for classification presume that incoming packets will correspond to a prior pattern.

Consequently, it's not a suitable method to identify fresh assaults [12]. One popular data mining method is clustering, where data points are grouped together according to the values of their features and a measure of resemblance. In contrast to classification, clustering that the clustering process lacks a target variable. Grouping algorithms separate all of the data into groups or clusters with features that are essentially the same. Consequently, Clustering offers several noteworthy benefits in comparison to the categorization methods, as they don't need a labelled training data set [14]. To identify a certain pattern from a vast dataset is referred to be an aggregation approach, which gathers and examining various record kinds from various channels concurrently.

V. CONCLUSION AND FUTURE WORK

Over the past few years, the number of internet users has nearly doubled. Users who use the internet more frequently are drawn to cloud computing, while cloud users who use it more frequently are drawn to cyber-attacks. One of the most common cyber-attacks nowadays is the botnet. It sets itself apart from conventional malware by being able to compromise other machines for a cyber-attack (Botnet Taxonomy [12][13]). A botnet will occasionally spread itself and will also alter its signature and form over time. Even now, 25% of all internet-connected PCs and cell phones are part of botnets that engage in various illegal activities without the end users' knowledge. This study provides an in-depth analysis of botnets, attacks, and their various forms. Architectures as well as methods of detection. The detailed descriptions of the three distinct architectures show which protocols are used in each. Botnet identification is still in its infancy; further study is required in this field. In the future, though, the researcher can focus on anomaly-based botnet detection, which uses factors like excessive network latency and communication on uncommon and regular ports to identify malware.

REFERENCES

[1] E. Alomari, “Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers : Classification and Art,” vol. 49, no. 7, pp. 24–32, 2012.
[2] Chung-Huang Yang , Kuang-Li Ting. Fast Deployment of Botnet Detection with Traffic Monitoring, Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pages 856-860, 2009.
[3] M. Thapliyal, N. Garg, and A. Bijalwan, “Botnet Forensics : Survey and Research Challenges,” no. April, 2013.
[4] Haritha S. Nair, Vinodh Ewards S E A Study on Botnet Detection Techniques, International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012
[5] F. Carpine and S. Maria, “Online IRC Botnet Detection using a SOINN Classifier,” pp. 1351–1356, 2013.
[6] Botnet scams are exploding, 2008 http://usatoday30.usatoday.com/tech/news/ computersecurity/2008-03- 16-computer-botnets_n.htm.
[7] Nicholas Ianelli, Aaron Hackworth. Botnets as a Vehicle for Online Crime - CERT and CERT Coordination Center are registeredin the U.S. Patent and Trademark Office. 2005
[8] R. A. Rodr, I. Omez, G. M. A-fern, and P. Garc, “Survey and Taxonomy of Botnet Research through Life-Cycle,” vol. 45, no. 4, 2013.
[9] J. Govil, J. Govil, C. Science, and A. Arbor, “Criminology of BotNets and their Detection and Defense Methods,” pp. 215–220, 2007.
[10] Oregon Man Cops Plea in eBay DDOS Attack, http://www.internetnews.com/security/ article.php/ 3574101
[11] S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and S. A. Khayam, “A Taxonomy of Botnet Behavior ,” vol. 94085, pp. 1–27, 2013.
[12] Zeus botnet steals $47M from European bank customers,2012. http://news.cnet.com/ 8301-1009_3-57557434-83/zeus-botnet-steals- $47m-from-european-bank-customers
[13] C. Li, W. Jiang, and X. Zou, “Botnet: Survey and Case Study,” 2009 Fourth Int. Conf. Innov. Comput. Inf. Control, pp. 1184–1187, Dec. 2009.
[14] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and A. Arbor, “A Survey of Botnet Technology and Defenses,” 2006.