Xournals

Academic Journal of Information Security

ISSN UA | Volume 01 | Issue 01 | January-2019

Botnet and Botnet Detection Techniques

Devendra Sharma[1] and Aman Sharma[2]

Available online at: www.xournals.com

Received 12th September 2018 | Revised 8th October 2018 | Accepted 13th December 2018

Abstract:

Botnet is currently the most emerging risk to the internet safety needs much attention as it have made already a big impact. In criminal activities such as DDoS, click fraud, phishing spamming, sniffing and spreading new malware, botnets are used by the attackers. It is worst when peer-to-peer technology underlying exchanges files and botnets become much tougher to identify and lock down due to which it becomes one of the biggest danger to internet constancy and safety. Hence, botnets are becoming more highlighted for the topic of research. Botnet attacks can be prevented, detected and mitigated by various types of proposed techniques hence, the current trend of botnet techniques and different criterias has beend discussed in this review study.

Keywords: *Bots, Botnet, Botmaster, Detection Techniques, Botnet Architecture, Botnet Attacks*

Authors:

1. *MB Khalsa College, Indore, Madhya Pradesh, INDIA*
2. *Maharaja Ranjit Singh College of Professional Sciences, Indore, Madhya Pradesh, INDIA.*

Introduction

Internet becomes a vital need for everyone in this current scenario. This fast and sharp increase of internet have increase the growth of online attacks. There are many sophisticated attacks are being launched by many cyber criminals towards the network organization through several universally secluded hosts and it is done with the determination of the misuse and is certainly enthused by political and financial intentions.One of the most emergent threat of online attack is Botnet attack which had previously made a huge effect and need much attention. Rapid botnets require uninterrupted work to make sure the detection methods of botnets and have bad impact. Therefore the basic criterion has been selected for the success of botnet detection.

Botnet

Nowadays, botnets are the serious manifestation of advanced malware. An assortment of computers infested by the malevolent software to make drones, bots and zombies, are called botnets. This have been integrated into a massive collective through a centralized expertise and controlled set-up. Botnets act as army for cyber attack by exploiting and recruiting computer and can be used for fake websites, spamming, DDoS attacks, worms, and viruses. Widespread security analysis and safety issues are created by the malicious behaviours of botnets that propagating the cyber crimes.

Peer 2 Peer (P2P) Botnet

Botnet systematizes their concealed tactics within a gentle presentation through the combinaing with the current technology like Peer to Peer, IRC, and HTTP. Through network monitoring analysis, several researches has been done for the detection of the IRC and HTTP Botnet. Each and every of the bot are remain joined to a control server and central command therefore most of the activities are easy to beat. P2P Botnets are one the most recent phenomenon which hindered the traditional methods of intrusion detection therefore cyber defence requires new Computational Intelligence (CI) **(Abdullah *et al*., 2013)**.

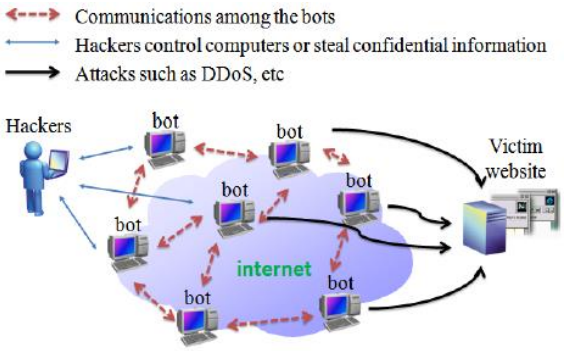

Figure: P2P Botnet Operation (Abdullah *et al*., 2013)

Botnet Life Cycle

Botmaster have to go through proper phases such as initial infection, secondry injection, connection, sending malicious code and maintaenance and updating during infecting another victim device. Botmaster infects new device first, which are connected to the internet, then using different protocols such as Hyper Text Transfer Protocol (HTTP), FTP and P2P, it injects some malicious code. After that victim device automatically makes connecftion with existing command and control server after the completion of successful injection of the malicious code and it become zombie. Then through the command and control server botmaster sends the bot army which performs malicious activities according to the receiving commands of the victim devices. Maintenance and updating of the zombie by sending the updated to the zombie device time to time is the last step **(Anwar *et al*., 2015)**.

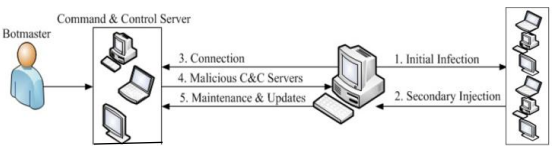

Figure: Life Cycle of Botnets (Anwar *et al*., 2015)

Botnet Architectures

Botnet architecture is the way through which the individual bots form a botnet and are classified into three categories. There are some methods of classifying the botnet architecture discussed in this paper.

A. Centralized Architecture
B. Decentralized Architecture
C. Hybrid Architecture

A. **Centralized Architecture:** Botmaster can easily manage and control the centralized botnet architectures. The Botmaster control and supervise all the bots in a botnet in the centralized architecture from a single circle pint which is called command and control server. Hierarchical topology and Star topology are the two topologies used in the integrated botnet architechture and the key proprieties used in integrated botnet architecture are Hyper Text Transfer Protocol (HTTP) and Internet Relay Chat (IRC). In this architecture, disaster chances is greater than the supplementary architecture and this is the main disadvantage of this architechture.

B. **Decentralized Architecture:** The entities responsible fro controlling the bots in a botnet is absent in the decentralized botnet architecture or peer to peer architecture. The C and C server needed for the communication with bots are more than one in this architecture.

C. **Hybrid Architecture:** It is the combination of both the centralized as well as the decentralized architecture. Servant and client are the two kinds of bots present in the hybrid architecture. The connected bot with hybrid bots are remain either servant or client bot. The botnets having hybrid architecture is harder to monitor than the botnet having centralized and decentralized botnets.

Classification of Botnet Detection Techniques

As many cyber attacks are occurring nowadays in internet, botnet detection is one of the essential task to advance the cyber security. Botnet detection methods can be categorized into two categories according to the previous studies which are honeynets detection techniques and intrusion detection techniques where intrusion detection techniques are additionally divided into sub groups.

1. Honeypots and Honeynets Based Detection System

Both these Honeyhnets and Honeypots are signifying to the end user devices which are best to assemble critical info about the cyber attacks. Botmaster can easily attack and compromise by this end user PC. Botnets changes their signature timely because of their security purpose it is proved by the previous researches and for understanding these properties of botnets, honeynets are very important. Honeywalls are very important in the honeynets detection technique for observing, gathering, altering and regulating communication over the honeypotys.

2. Intrusion Detection System (IDS)

Traffic flow for the malevolent happenings of a network is monitored by the intrusion detection system. It openly informs the computer system or the manager of the system if any malicious attacks has is found during the traffic. These malicious activities also can be prevented by the IDS to block the traffick which are coming from the virus infeted systems. IDS have two types: Signature based and Anomaly based

a. **Signature Based Detection:** In this technique of detection, the knowledge of network performance being find makes the signature very simple to grow and this is the main advantage of this detection technique. The technique is easy to develop and understand and is very simple. For making the botnet attack more secure from bot infected machines, every attacks's signature changed by the botmaster with time to time.

b. **Anomaly Based Detection:** The network activities which in advance are specified by the administrator or which are feed by the administrator or both only accepted by anomaly based botnet detection techniques. The rules for each protocols in this practice should be well-defined in progress and should be established for their precision. The proceedings which are not linked with the feed or recognized model of performance only detected by this technique. This technique is much more secure than the signatutre based detection technique and is expensive with respect to the computation. This technique has a disadvantages also in which the main disadvantages is that the definition of rules is very difficult. Anomaly based detection technique is again divided into two subcategories ie. Network and Host-based detection technique.

i. **Network Based Detection Techniques:** Network based approach mainly focuses on two factors of Monitoring network trafficking ie., detection of individuals bots that can expose the control and command server or malevolent in bot related activities by testing for traffic forms or content and the other is to analyze the traffic that designate two or more hosts behaving in similar arrangements as bot to respond in the same functionality.

ii. **Host Based Detection Techniques:** It monitors the linkage trafficking for suggestions of bot infected machines. When bot had been triggered, the host leads the variations on system files and system registry and become worse.

Review of Literature

Zhao *et al.*, (2009) implemented a novel system for the detection of new kind of botnet spamming attacks that targets the chief web email providers is termed as Botgraph. Both their implimentations and graph based approach are generally applicable to wide class of security are believed by them to analyze large datasets.

Karim *et al.*, (2014) presented a widespread analysis of techniques of modern state of the art for botnet detection and therefore, figure out the developments of previous and current research. The highlighted the future recommendations for refining the systems that largely span the complete research field of botnet detection, and also suggested to recognize the prominent and persistent research trials. The criminal activities such as click fraud, distributed denial of service attacks, spam emails, malware distribution, phishing, and building machines used for the illegal interchange of data or supplies is supported by the botnet phenomenon.

Lin, Chen and Hung, (2014) used proposed method to recognize the perilous structures that define the configuration of botnets and worked on botnet detection by using support vector machines with artificial fish swarm algorithm and effects showed that the methods can be used for recognizing the important botnet features and that the enactment of the planned method was superior to that of the genetic algorithms.

Prabhu and Shanthi, (2014) in their paper, they distinguished their survey into three parts such as Anomaly detection- Botnets, Botnet attacks and latest botnet behaviours and techniques for defending against botnets. They also summarized the existing research in their paper and recommend future path for botnet research. The major threat of the internet is the botnet attack. The main source of excecution of all the cyber malicious activities is botnet.

Alzahrani and Hong, (2017) surveyed both traditional and modern mechanisms, practiced in distinguishing cloud based DDoS attacks. They said the requirement to safeguard the data in the cloud from any system of attack. The techniques against DDoS explained in this paper is greatly plagiarized from the already tried customary techniques. Although for the complete recognition and inhibition of the DDoS attacks, no techniques has proven to be perfect.

Kaur and Gupta, (2017) discussed the Botnet threats in cloud based infrastructures and also reviewed some current detection techniques to defend against such threats. This paper also presents the state of art models for botnet detection in cloud environment and at last the architectural view of the models of botnet threat detection which are based on the outbound DNS traffic monitoring and said the essential need to apply subject knowledge of data mining.

Thangapandiyan and Anand, (2017) studied and analyzed different detection techniques based on user data and behavior of the distributed computing environment. Also represented an overview on the recent botnets types, botnet detection techniques and botnets impact reducing techniques. They compared different types of botnets and found low latency communication of IRC botnet and botmasters have a real control over the bots. They also found that the bots gets easily collapsed by shutting down the IRC.

Conclusion

The number of internet users are growing day by day by the passage of time. Number of usage of internet is diretly proportional to the cloud computiong that is increase in the user of internet will also increase the cloud computing while the cloud computing is directly proportional to the cyber attacks that is, cyber attacks will be increase with the increase in cloud computing. Botnets propagates and change its shape and signature itself from time to time. Here in this paper, details of botnets, its attacks, life cycle and its detection techniques is presented. It is recommended for future work to research on the anomaly based botnet detection and high network latency as a base.

References:

Abdullah, Raihana Syahirah, *et al*. "Revealing the Criterion on Botnet Detection Technique." *IJCSI International Journal of Computer Science Issues*, vol. 10, no. 2, Mar. 2013, pp. 208–215.

Alzahrani, Sabah, and Liang Hong. "A Survey of Cloud Computing Detection Techniques against DDoS Attacks." *Journal of Information Security*, vol. 09, no. 01, 2018, pp. 45–69.

Anwar, Shahid, *et al*. "A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing." *IEEE Symposium on Computers & Informatics, At Kota Kinabalu, Sabah, Malaysia*, Sept. 2014.

Karim, Ahmad, *et al*. "Botnet Detection Techniques: Review, Future Trends, and Issues." *Journal of Zhejiang University SCIENCE C*, vol. 15, no. 11, 2014, pp. 943–983.

Kaur, Parneet, and Anuj Gupta. "A Study on Botnet Detection in Cloud Network." *International Journal of Computer Science Engineering*, vol. 6, no. 11, Dec. 2017, pp. 225–229.

Lin, Kuan-Cheng, *et al*. "Botnet Detection Using Support Vector Machines with Artificial Fish Swarm Algorithm." *Journal of Applied Mathematics*, vol. 2014, 2014, pp. 1–9.

Prabhu, S. Nagendra, and D. Shanthi. "A Survey on Anomaly Detection of Botnet in Network." *International Journal of Advance Research in Computer Science and Management Studies*, vol. 2, no. 1, Jan. 2014, pp. 552–558.

Thangapandiyan, M., and P. M. Rubesh Anand. "Botnet Detection Techniques in Cloud Computing Environment: A Survey." *International Journal of Pure and Applied Mathematics*, vol. 118, no. 22, pp. 929–939.

Zhao, Yao, et al. "BotGraph: Large Scale Spamming Botnet Detection." *Symposium on Networked Systems Design and Implementation*, pp. 321–334.