A Study on BOTNET Attacks and Detection Techniques

Yogita Barse[1], Dr. Sonali Tidke[2]

[1]M.Tech. Scholar Department of CSE Indore Institute of Science and Technology (IIST) INDORE (M.P.), India
[2]Professor Department of CSE Indore Institute of Science and Technology (IIST) INDORE (M.P.), India

Abstract:*A Bot is a type of malware that allows an attacker to take control of infected machine. The Botnet is a network of bots. A Bot infected machine is often called as zombie and cybercriminals who control these bots are called Botherders or Botmasters. Bots are often spread themselves across internet by searching for vulnerable machines to expand. The way the bots are controlled depends upon architecture of botnet Command and Control (C&C) mechanism which may be based on Internet Relay Chat (IRC) or HTTP or Peer to Peer(P2P). Botnet is widely used to carry out malicious activities like Distributed Denial of Service(DDoS) attacks, sending spam mails and click frauds.Botnet detection techniques are broadly based on either setting up of a honeypot tocollect bot binaries or developing intrusion detection system. The intrusion detection system (IDS) identify botnet traffic by monitoring network and system logs. It can be based on anomaly behavior or signature or DNS. In this paper discussion over different tools are given such as Snort, Suricata, Ntop, Bothunter, etc. This paper is mainly focused on honeypot-based botnet detection technique.*

Keywords:*Distributed Denial of Service Attack, Botnet,Botnet detection, Lifecycle.*

Date of Submission: 22-05-2020 Date of Acceptance: 09-06-2020

I. Introduction

A Bot is an autonomous program automatically perform task without knowing to areal user. A collection of machines which run such autonomous bot is called as botnets. Bot is remotely controlled by command and control server. The black-hat developers created highly sophisticated malwares that are difficult to detect and remove. Bot program is stealthy during its whole life cycle. They had generated relatively small network footprint and most of time remains ideal for stealing information. The concept of remote-controlled computer bot originated from Internet Relay Chat (IRC). It provides one to many communications channels and support very large number of concurrent users. Eggdrop was first bot developed in 1993 [1][2].

As internet connects billions of computers, tablets, smart phones together to share the information across the globe, peoples are relying on these technologies to share their personal as well as business information. The black hat hackers used its vulnerabilities to perform attacks. The initial intention of these cyber criminals was just to gain fame but over the period they are doing criminal activities to earn money [3]. Theterm botnet isderived from the words robot and network.A bot in this case is a device infected by malicious code, which then becomes part of a network, or net, of infected devices controlled by a single attacker or attack group. A bot is sometimes called a zombies and a botnet is sometimes referred to as a zombie army [4].

Both names (bot and zombie) imply the mindless automatic propagation of something malicious (malware) by agents that are possessed in some way (by the threat actor).The botnet malware typically looks for vulnerable devices across the internet, rather than targeting specific individuals, companies or industries. The objective for creating a botnet is to infect as many connected devices as possible and to use the computing power and resources of those devices for automated tasks that generally remain hidden to the users of the devices [5].

For example, Fraud botnet that infects a user's PC will take over the system's web browsers to divert fraudulent traffic to certain online advertisements. However, to stay concealed, the botnet won't take complete control of the web browsers, which would alert the user. Instead, the botnet may use a small portion of the browser's processes, often running in the background, to send a barely noticeable amount of traffic from the infected device to the targeted ads [6].

On its own, that fraction of bandwidth taken from an individual device won't offer much to the cybercriminals running the ad fraud campaign. However, a botnet that combines millions of devices will be able to generate a massive amount of fake traffic for ad fraud, while also avoiding detection by the individuals using the devices [7] [8].

II. Elements Of A Botnet

A bot network mainly comprises of three elements to initialize and to carry out a malicious activity successfully, as shown in Fig. 1.

*The Attackers:*The attackers are the ones who are responsible for the initialization of attacks and gives out commands to the bots present in the botnet to carry out some malicious activity.

The Bots: The vulnerable computers which are infected with malicious code and thus are recruited as part of the botnet to carry out some malicious activity.

The Handlers: These are used as means of communication to the bots, by the attackers. By this the attacker communicates indirectly with the bots for commands dissemination purpose [9].

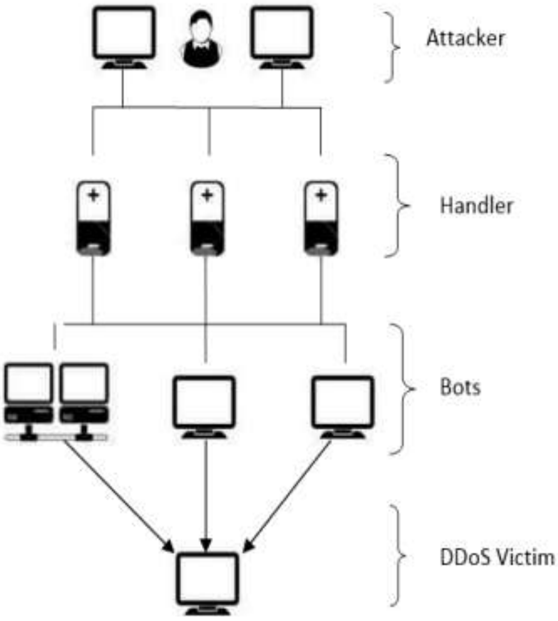

Figure 1: Elements of a Botnet

III. Botnet Life-Cycle

Creation: Firstly, botmaster develop his software mostly by extending previous code or by adding new features. This is very well tested in isolated environment.

Infection: There are many ways for infecting victims machine through software vul-nerabilities, email attachments and trojan horse. Once victims machine is infected by this software then it is called zombie.

Rallying: After infection, zombie machine attemptsfirst and try to contact com-mand and control machine. This process is called Rallying. In centralized botnet topology, this could be IRC or HTTP servers whereas in P2P topology zombie tries to locate peer machine and join the network. Bot program contains multiple addresses of servers. Some C&C servers are configured in such a way that it immediately reply to bots initial request [10][11].

Waiting: After joining to network, bot waits for command from C&C server. During this phase very little traffic is found between bot and its master.

Executing: Once the bot received command from its master, it starts executing it.After execution it sends result to bot master via C&C network. Typical commands are: scanning for new victims, sending spam, and sending DoS. There are two main botnet topologies: centralized and peer to peer (P2P). In centralized botnets, IRC is still pre dominant protocol of C&C channel.

The bot lifecycle consists of following phases shown in figure 2.

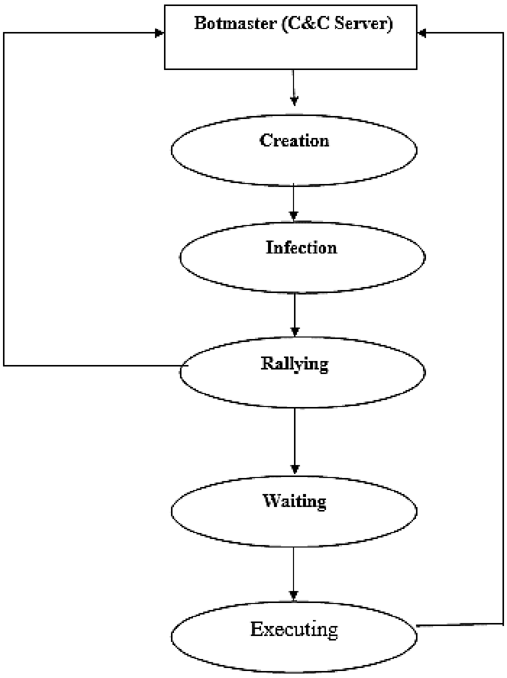

Figure 2: Bot Lifecycle[1]

Internet users are getting infected by bots and any times corporate andend users are trapped in botnet attacks.Now a day 16-25% of the computers connected to the internet aremembers of a botnet. In this network bots are located in various locations [12].

It will become difficult to track illegal activities. This behavior makes botnet an attractive tool for intruders and increase threat against network security.

A Bot is an autonomous program automatically perform task without knowing to a real user. A collection of machines which run such autonomous bot is called as botnets.Bot is remotely controlled by command and control server. The black-hat developers created highly sophisticated malwares that are difficult to detect and remove.

Bot program is stealthy during its whole life cycle. They had generated relatively small network footprint and most of time remains ideal for stealing information. The concept of remote-controlled computer bot originated from Internet Relay Chat (IRC). It provides one to many communications channels and support very large number of concurrent users [13][14].

IV. Literature survey

Deshpande et al. [8] discussed classification and predictive models for anomaly detection are built by using machine learning classification algorithms namely Random Forest.

Pratik et al. [9] detected bots by using signal processing techniques and achieved high detection accuracy. In this work no DPI required and can detect malicious hosts from the monitored network only. Computational Complexity was high.

Huy et al. [10]proposed a proactive detection approach Entelecheia. This approach detected bots in waiting stage but not able to stealthy botnets.

Zhao et al. [11] discussed that the bots are detected by identifying malicious fast-flux service traffic Low computational complexity. In this paper, more discriminators required for classification of malicious and non-malicious FFSNs.

Yuhui and Ning [12]performed off-line analysis and on-line monitoring for detection Combine advantages of off-line and on-line detection. In this system they cannot detect bots if they are not in attack stage.

Rafael et al. [13]analyzed resource sharing behavior for which no traffic analysis required.

Priyanka and Dave [14] proposed a detection approach PeerFox based on intensity and consistency of search packet.

V. Honeypot-based botnet detection

A honeypot is an information system resource,which value lies in unauthorized or illicit use ofthat resource; they are vulnerable systems waitingfor attacks. The idea behind this methodology is tolure in attackers such as automated malware andthen study them in detail. Honeypots have provento be very effective tools in learning more aboutInternet crime like botnets.

There are two generaltypes of honeypots:The first one is Low-interaction honeypots: Theyemulate services or operating systems with a low level of interaction.Implementing this type ofhoneypots tends to be low risk, the main intentionis to capture harmful code samples, anddeployment and maintenance tend to be easy.

Apopular example of this kind of honeypots isNepenthes.we used the low-interaction honeypot“nepenthes”todetectbotnets.A distributedframework of Nepenthes honeypots was built tocollect as more as possible malware samples.

TheconfigurationofNepenthes to improve the capture efficiency. Later,theyhave analyzed thesesamplesfirstlybyfeatures viaantivirus scan, then bybehavior viatwo different online sandboxes in different periods and multiple times for obtaining accurate behavior.Thesecondtypeis High interactionhoneypotsallowing the attacker to interact with a real system. The risk of deploying tends to be higher, so it isrequiredtoestablishprecautionsand specialprovisions toprevent attacks against the system,more complexto setupandmaintain.

The mainintentionistounderstandtheattackscene,concernedthattheattacksontheprocess,itrequiresastrongabilitytointeractwiththeattacker. The most common setup for this kind ofhoneypotsisa GenII Honeynet.

The Honeynet, forexample,has doneextensive workon capturinglive bots and characterizing botnet activities, and agroupofwhite-hatvigilantesisscouringtheInternetlookingforevidenceofbotnets.

VI. Proposed System

In this System a system has to be setup using Honeypot and to detect botnet attack in network.For this PENTBOX TOOL is used for identifying botnet activities in our system.

As network security has become integral part of our life and botnets have become the most serious threat to it.

A. Proposed System Architecture

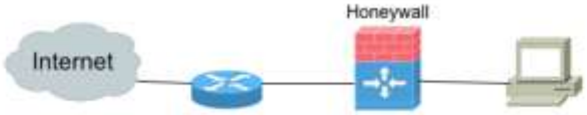

Figure 3: Botnet Detection : Setting up Honeynets[6]

B. Honeywall Responsibilities

DNS/IP-address of IRC server and port number(optional) password to connect to IRC-server.

Nickname of bot.

Channel to join and (optional) channel-password.

Main objective of this paper is to do research on botnets from their origin until today and to develop botnet analysis and detection techniques on one of the latest botnet using most advanced techniques.

Initially an idea is developed to learn some botnet development and to develop a botnet and then develop software to detect it and as conclusion to understand what flaws could be in current botnets and how they could be detected.

Problem with this method was it needed quite comprehensive study to learn botnet development techniques and it was not a surety that the botnet developed is “up to standard” accordingto latest botnet such as Zeus, Torpig or Hlux.

VII. Conclusion

Botnet is a major security threat and difficult to discover its existence. We reviewed different botnet tools and detection techniques. The intrusion detection system is widely used for botnet detection. There are anomaly based and signature based tools to detect botnet like Net ow, Snort, Suricata, Ntop, Wireshark. The other category of tools are based on mining like Botminer, Botsni fer, Bot under. Bothunter is driven by Snort. It monitor two way communication between internal asset and external entity. Zeus Toolkit is most popular in hacker community for understanding botnet internals. It is publicly available, so many variant of Zeus malware exists in internet domain.Mostof thecurrentbotnet detectiontechniques work only on specific botnet C&Communicationprotocols and structures. Consequently, as botnetschangetheirC&Ccommunicationarchitecture,these methodswill be ineffective.

References

[1]. Ping Wang, Baber Aslam, Cliff C. Zou, “Peer to Peer Botnets”, Handbook of Information and Communication Security(Springer), 2010, pp. 335-350.

[2]. Hossein Rouhani Zeidanloo, Azizah Abdul ManafJ, “Botnet Command and Control Architectures”, in Second International Conference on Computer and Electrical , 2009, pp. 564-568.

[3]. David Dittrich, Sven Dietrich, “P2P as botnet command and control: a deeper insight”, In 3rd International Conference on Malicious and Unwanted Software (MALWARE) IEEE, 2008, pp. 41-48.

[4]. http://www.computerweekly.com/news/450303601/More-IoT-botnetsconnected-to-DDoS-attacks

[5]. Saman Taghavi Zargar, James Joshi, and David Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”, In IEEE Communications Surveys & Tutorials, Fourth Quarter 2013, vol. 15, no. 4, pp. 2046-2069.

[6]. Maryam Feily, Alireza Shahrestani, Sureswaran Ramadass “A Survey of Botnet and Botnet Detection”, In Third International Conference on Emerging Security Information, Systems and Technologies IEEE, 2009, pp. 268-273.

[7]. T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, “Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm”, In LEET 08: First USENIX Workshop on LargeScale Exploits and Emergent Threats, 2008.

[8]. A. Deshpande and R. Sharma, “Anomaly Detection using Optimized Features using Genetic Algorithm and MultiEnsemble Classifier”, ojssports, vol. 5, no. 6, p. 7, Dec. 2018. Retrieved From https://ijosthe.com/index.php/ojssports/article/view/79. https://doi.org/10.24113/ojssports.v5i6.79.

[9]. Pratik Narang, Vansh Khurana, Chittaranjan Hota, “POSTER: Machinelearning Approaches for P2P Botnet Detection using Signal-processing Techniques”, In ACM-DEBS, May 26-29, 2014,, pp. 338-341.

[10]. Huy Hang, Xuetao Wei, Michalis Faloutsos, Tina Eliassi-Rad, “Entelecheia: Detecting P2P Botnets in their Waiting Stage”, IFIP Networking Conference, 2013, pp. 1 – 9.

[11]. David Zhao, Issa Traore, “P2P Botnet Detection through Malicious Fast Flux Network Identification”, IEEE Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2012, pp. 170- 175.

[12]. Yuhui Fan, Ning Xu, “ A P2P Botnet Detection Method Used On-line Monitoring and Off-line Detection”, International Journal of Security and Its Applications, 2014, Vol.8, No.3, pp. 87-96.

[13]. Rafael A. Rodríguez-Gómez, Gabriel Maciá-Fernández, Pedro GarcíaTeodoro, Moritz Steiner, Davide Balzarotti, “Resource monitoring for the detection of parasite P2P botnets”, in Computer Networks, Elsevier 2014, pp. 302-311.

[14]. Priyanka, Mayank Dave, “PeerFox: Detecting Parasite P2P Botnets in their Waiting Stage”, In International Conference on Signal Processing, Computing and Control ISPCC, IEEE, 2015, pp. 350-355.

Yogita Barse, et. al. “A Study on BOTNET Attacks and Detection Techniques.”*IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)*, 15(3), (2020): pp. 01-05.