IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.107103

Botnet Attack and its Detection Techniques

Miss. Shefali Thakare[1], Prof. K. K. Chhajed[2]

PG Scholar, CSE Department, P R Pote College of Engineering and Management , Amravati, India[1]

Assistant Professor, CSE Department, P R Pote College of Engineering and Management , Amravati, India[2]

Abstract: In today's cyber attacks and cyber crimes world Botnet is the severe threat which occurs usually. Botnet are intended to perform predefined functions in an automated fashion, where these malicious actions ranges from online searching of data, accessing lists, moving files sharing channel information to DDoS attacks not in favor of critical targets, phishing. Various types of techniques and approaches have been projected for detection, mitigation and preventation to Botnet attack. This paper discusses in detail about Botnet and related research including Botnet evolution, life-cycle, command and control models, communication protocols, Botnet detection etc. Also an general idea of research on Botnets which describe the possible attacks performed by various types of Botnet communication technologies in future.

Keywords: Bot; Botnet; C&C mechanism; communication protocols; honeynet; passive traffic; attacks; defense; preventaation

I. INTRODUCTION

Botnet is the compilation of bots or collection of compromised computers that are remotely controlled by its BotHerder [1]. Even though Botnets shows the trace of existence for several years ago, recently have only Botnet sparked the interest of the research community. The term ―Bot‟ is term which is derived from ―ro-Bot‖ [2]. which is a common term used to illustrate a script or sets of scripts designed to perform predefined function in automated fashion. Generally Botnet is used to describe networks of infected end-hosts, called bots that are under the control of a human operator commonly known as a Botmaster. Botnets recruit vulnerable machines using techniques utilized by other classes of malware. e.g., remotely exploiting software vulnerabilities, social engineering, etc. [3], these machines produce a C&C infrastructure between them to perform malicious activity. in common the main distinction between Botnet and other kind of malwares is the existence of C&C infrastructure. Hence in the mechanism of detection of Botnet, if we spot the location of C&C then Botnet can be detected, removed and prevented from various types of cyber-crimes.

More specifically on Internet relay chat (IRC) network bot‟s function in channels consist of managing access lists, move files, share users, share channel information, anything else if right scripts are added. IRC bots are automated and controlled by events which could be commands given in a channel by other IRC bot or client with necessary privileges.

In this paper, an summary of current Botnets technology research has been provided. The rest of the paper is organized as follows: Section 2 discusses background of Botnets. Section 3described about literature review, in this section, various botneck detection techniques will be covered in section IV and section V covers key identification and extraction, Classification of bots & also describe about the communication protocols used by Botnet to communicate.

II. HISTORY BOTNECK

Botnets have been in existence for about 10 years [13].Security experts alerting the public about the threat posed by botnets for some time. Still, the depth and density of the problem caused by botnets are underestimated and most users never realize the real threat they pose[13].

A. How Does a Botnetworkwork ?

Most botnets are designed as distributed-design systems, with the main botnet operator (botmaster) issuing instructions openly to a small number of systems. These machines proliferate the instructions to other compromised machines, usually via Internet Relay Chat (IRC) [14]. The ingredient of a typical botnet includes a server program, client program for operation, and the program that embeds itself on the victim's machine (bot). All three of these usually communicate with each other over a network and may use encryption for stealth and for protection against detection or intrusion into the botnet control network. Botnets are efficient in performing tasks that would be impracticable given only a single computer, single IP address, or a single Internet connection. Originally, botnets were used for distributed denial of service attacks. (See Figure 1) Most modern web servers have developed strategies to
combat such DDoS attacks, making this utilization of a botnet less effective [14]. When infecting a computer, the bots connect to IRC servers on a predefined channel as visitors and waited for messages from the botmaster. The botmaster

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.107103

could come online at any time, view the list of bots, send commands to all infected computers at once, or send a private message to one infected machine.

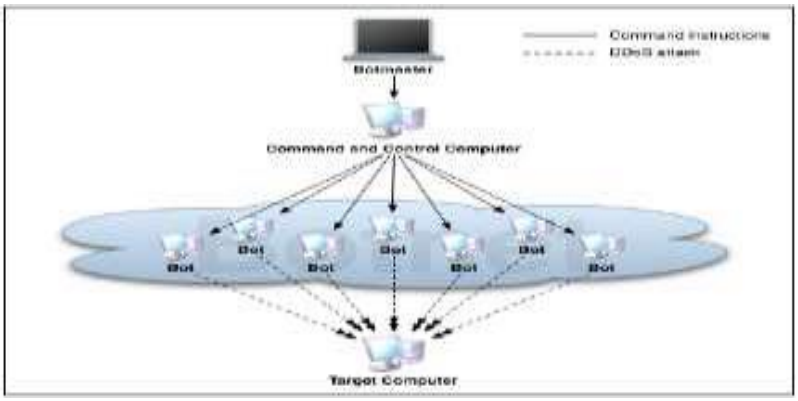

Figure 2 :– Example of Botnet Attack

B. Why are Botnets dangerous today?

Botnets is one of the most dangerous species of network-based attack since they use large, coordinated groups of hosts to carry out both brute-force and subtle attacks. A collection of bots, when proscribed by a single command and control (C&C) infrastructure, forms a botnet [15]. Since the bots work mutually in large groups taking orders from a centralized botmaster, they can cripple a large-scale networks in a petite time. A huge work has been done trying to moderate the efforts of botnets to avoid data and financial loss. However hard the industry works towards patching the known vulnerabilities in hosts and networks, there are always more unpatched or unknown vulnerabilities that malicious developers and cyber criminals may exploit.

III. LITERATURE REVIEW

Initially we identify the motivations behind building and operating botnets and how these motivations have evolved over time. Then, we talk about the current research on how to track and disable botnets.

A. Botnet Life cycle

B. A typical Botnet can be created and maintained in five phases. This is depicted in Fig. 2.

C. In first phase, initially Botmaster infect victim host with Bot via the social engineering, mail attachments, automatic scan, exploit and compromise etc mechanisms.

D. In second phase, Bot connected to command and control channel

E. In third phase, Botmaster send command through IRC/HTTP/P2P C&C Channel to bots

F. In fourth phase, repeat, soon the Botmaster has a large number of army bots to control from a single point.

G. And in last phase, bots are updated with a new version or new business functionally through their operator which issue payload command. therefore the above conversation explained all five steps about how a bot is infected to other hosts. In count it also gives insight into how the Bot increase their quantity means its capacity on a network to perform malicious activity and harm the users.

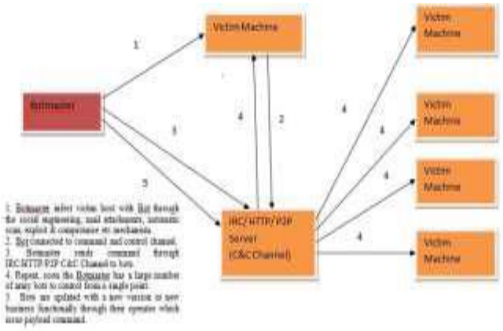

Figure 2 :– A Typical Botnet Life-cycle

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.107103

IV. CLASSIFICATION OF BOTNECK

1. On the basis on Network Protocols For a Botmaster to send commands to a bot, it is necessary that a network connection must be established between the zombie machine and the computer transmitting commands to control it. In this all network connections are stand on protocols that define rules for the communication between computers on the network. Botnets can be classified according to network protocols follow as:

a. IRC-oriented: This is one of the types of Botnet in which bots are restricted via IRC channels. Every infected computer connected to the IRC server (master) indicated in the body of the Bot program, and stay for commands [48] from its master on a certain channel (eg-IRC Botnet).

b. IM-oriented: This type of Botnet is not mostly common. It varies from IRC-oriented Botnets only in that it uses communication channels given by IM (instant messaging) services such as AOL, MSN, and ICQ etc and because of the complexity of creating individual IM accounts for each bot. The principal problem in this, Bots should be connected to the network and must stay online all the time [4] and each bot needs its own IM account to perform malicious activity. As result, owners of IM oriented Botnets only have a limited number of registered IM accounts at their disposal, which limits the number of bots that can be online at any one time.

Web-oriented: This is a relatively new and speedily evolving type of Botnet designed to controlling zombie networks over the World Wide Web. A bot connects to a predefined web server (master), receives commands from it and transfers data to it in response. And wait to get a signal from its master to perform some activity for eg-HTTP Botnet.

d. Other: In this, there are other types of Botnets that communicate via only their own protocol that is only based on the TCP/IP stack, i.e., they only use transport-layer protocols such as TCP, ICMP and UDP.

V. BOTNECK DETECTION TECHNIQUES

Here, We present our Pebbletrace scheme for the traceback to the botmaster. In the beginning it identifies cryptographic keys of the botnet communications for configuring botnet operations and then traces back to the botmaster. First recognize the cryptographic key of the botnet communications for figuring out the botnet operations. We then compromise the botnet entities for tracing back to the botmaster across the stepping-stones.

A. Key Identification

A major difficulty for analyzing botnet attack traffic is that communication between bots and C&C servers are typically encrypted, and the encryption keys are to be recognized first. conventional memory forensic key identification problem was studied (e.g. [15]), however, we have to meet the following new challenges:

a. **No source code**.

conventional key identification schemes typically inspect source code, e.g. [16]. on the other hand, it is tough to obtain bot source code — often not even the bot binaries. Static analysis on source code and binaries cannot be conducted as in memory forensic.

b. Abnormal code pattern

Attackers do not follow the standards to employ their encryption schemes even though they are mathematically equivalent. Identification schemes based on standard key.

B. Key Identification and Extraction

When the traceback server receives traceback requests with the desirable information, initially it identifies the encryption key of attack traffic for: (i) Decrypting the attack traffic and figure out the needed information for trackback; and ( ) Embed Pebble ware in the botnet traffic and traceback botmasters from side to side stepping-stones. This scheme works exclusive of source codes and with vague traffic patterns only, is time proficient, and has low false positives. Given a memory image of victim machines, network traffic (ciphertext) and the type of botnets, we propose a three phase detection scheme that consists of (i) a pattern filter; ( ) an entropy analyzer; and (i) a verifier for identifying the symmetric keys used by bots. Figure 4 is an overview of the key identification scheme.

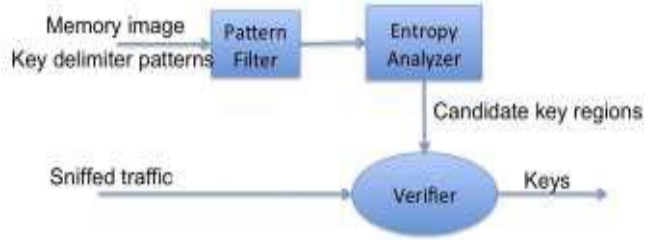

Figure 2 :– An Overview of Key Identification Scheme

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 7, July 2021
DOI 10.17148/IJARCCE.2021.107103

Figure 3 shows an general idea of our Pebbletrace scheme for cloud-based botnets. The trackback starts from the receiver, i.e. C&C server, or from the victim. A local network administrator put forward a request to traceback server providing sniffed traffic, memory image and basic information of victim. Traceback server then take out encryption key of botnet communication by our key identification algorithm. After that traceback server creates a Pebbleware and encrypts it with the detected botnet key.

VI. ONCLUSION

Botnet have evolved from the beginning assistant tool to the predominant threat in modern internet and as discussed in this paper, focused on the attacks that a botmaster attempts to steal sensitive data from the victim machines and we can spread our tracing pebbles along with the stolen data all the way back to the botmaster. Asymmetric key identification is a challenging research topic in general. However, our results on symmetric key identification and the specific botnet application environment may shed light on future investigation.

REFERENCES

[1] Hossein Rouhani Zeidanloo, Azizah Bt Manaf, Payam Vahdani, Farzaneh Tabatabaei, Mazdak Zamani, "Botnet Detection Based on Traffic Monitoring" IEEE transaction,2010.
[2] SANS Institute InfoSec Reading Room provided a description on "Bot & Botnet: An overview" research on topics in information security, 2003. Johny Antony P & Selvadoss Thanamani Antony., "A Survey on Privacy Preservation in Big Data", International Journal of Engineering Science Invention Research and Development (IJESIRD) Vol 3, Issue 3, October 2016, ISSN 2349-6185
[3] Generation of a robust Botnet capable of maintaining control of its remaining bots even after a substantial portion of the Botnet population has been removed by defenders.
[4] S. Nagendra Prabhu, Kemal Sultan Abdo & Gashaw Bekele Kabtimer, „Introducing Proxy Cloud Storage Using Internet Information Services in University and Utilization Of ItsResources in the Academic Institution" in Journal of Network communications and Emerging Technologies, Volume 8, issue 2 February 2018.
[5] Hossein Rouhani Zeidanloo, Farhoud Hosseinpour , Farhood Farid Etemad, "New Approach for Detection of IRC and P2P Botnets" , International Journal of Computer and Electrical Engineering, Vol.2, No.6, December, 2010, 1793-8163.
[6] Prabhu S, Chandrasekar V & Shanthi S, Improving the performance of IDS using Arbitrary Decision Tree in NetworkSecurity, International Journal of Advanced Science and Technology Vol. 29, No. 3, (2020), pp. 3453 - 3462
[7] Hossein Rouhani Zeidanloo, Azizah Abdul Manaf,"Botnet Command and Control Mechanisms", IEEE transactions, 2009.
[8] Nagendra Prabhu, S & Shanthi, D „A Survey on Anomaly Detection of Botnet in Network" published in Volume 2, Issue 1 of International Journal of Advance Research in Computer Science and Management Studies in the year of 2014.
[9] Robert F. Erbacher, Adele Cutler, Pranab Banerjee, Jim Marshall,"A Multi-Layered Approach to Botnet Detection", IEEE conference, 2010.
[10] Nagendra Prabhu, S & Shanthi Saravanan, D, 2017, „An Efficient Botnet Detection System in Large Scenario Networks Using Adaptive Neuro Fuzzy Inference System Classifier", Journal of Computational and Theoretical Nanoscience Vol. 14, 1–5, 2017
[11] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," in Proc. In Workshop on Hot Topics in understanding Botnets, 2010.
[12] Prabhu, SN & Shanthi, D , „Cloud Computing Defense Threats and Responses against DDOS Attack", published in Volume 5, Issue 4 in International Journal of Science, Engineering and Technology Research (IJSETR) in Vol. 5, 1–4, April 2016.
[13] http://www.kaspersky.com/reading_room?chapter=207716701

