International Journal of Advanced Technology in Engineering and Science
Vol. No.08, Issue No. 03, March 2020
www.ijates.com
ijates
ISSN 2348 - 7550

Botnet Threats/Attacks and Botnet Detection, Prevention Methods

Rajesh Yadav

Department of Computer Science, BML Munjal University, India

ABSTRACT

Today botnets have become one of the biggest risks in the network and security world and have been an infrastructure to carry out nearly every type of cyber-attacks as they provide a distributed platform for different illegal activities like launching the distributed denial of service attacks (DDoS). Recently botnet detection has been a very interesting research topic in the cyber security platform. Botnets are mainly responsible for large scale coordinated attacks. Infected computers also known as an 'Agent' or 'Zombies' perform all kinds of tasks for the bot-master such as phishing campaigns, sending spam, delivering malware or leasing or selling botnet to other hackers or fraudsters. Further, botnets remain a large-scale problem that affects the entire Internet and cyber-security community and requires a significant level of co-operation among operators and providers. Unlike the other types of malwares, botnets are well organized and controlled by skilled bot-masters. They employ various strategies to keep their bots safe and hidden if possible. Therefore, botnet detection is a big challenge in network security management. There are several methods and techniques in detecting and tracking the botnet activities. Each of these techniques has its advantages and disadvantages. In addition, these techniques are designed based on computers and computer networks' specifications and might not be fully applicable for new generations of botnets. As botnets change their C&C communication architecture, these methods will be ineffective. Hence, developing techniques based on data mining and DNS traffic for botnet C&C traffic detection has been the most promising approach to combat botnet threat against online ecosystems and computer assets. This paper reviews overview of current state of bots and botnets, how networks are threatened or attacked by botnets with their detection and the preventiontechniques.

Keywords- **Attacks,** ***Bots, Botnets, Cybersecurity, Darknet, DNS, DDOS, Hacking, IOT, Security, Threats, Vulnerabilities, Zombies.***

1. INTRODUCTION

The definition of denial of service (DOS) attacks isn't limited to a target machine being attacked by another one, nowadays multiple attacker machines send flooding requests to a single target which makes the target machine more vulnerable [1]. Botnets are a genius creation without a doubt but with great power comes great responsibility which makes

them one of the most perilous network-based attacking amid network security threats like viruses and worms [2]. The term "Bot" got its name from "Robots" because they perform in a similar way, mostly pre- programmed to perform specific tasks through an automated approach. Bots are software that reside on the host computer controlled by the bot master allowing them to take over the host computer remotely [3][4].

Based on various researches, it has been found that botnets are not only a threat to computer network but also used for malicious activities such as DDOS attacks, their versatility makes them interesting but dangerous. Due to their nature, botnets can cause disastrous network interference though DDOS, and the cost of this interruption can be hefty for enterprises [5] [6] [7]. Botnets are also programmed to gather personal, corporate, or government sensitive information and sell it for a fair price at an "organized crime market", most spams that we see on the internet today are a result of botnets [8]. Botnets are reliable and reusable which makes them a favorite among attackers hence, determining the source of botnet attacks is a challenge. Therefore, this paper first investigates botnet lifecycle in section two, and thereafter it discusses; Security threats from botnet, Network monitoring with IDS and IPS, Botnet detection technique, Botnet detection tools, and finally Botnet prevention techniques accordingly from section three toseven.

2. BOTNETLIFECYCLE

2.1 InfectionMechanism

Bot-masters use different methods and techniques to infect victim machines like computers and other connected devices and convert the targets into bots. Then the targeted host execute a script known as shell-code. The shell-code draws the image of the real bot binary from the location via FTP, HTTP, or P2P. Once bot binary installs itself on the infected machine which turns the computer turns into Zombie and runs the malicious code. Once the Zombie is rebooted the bot application runs automatically [9]. Some methods that botnet uses to infect is described below.

a. Software Vulnerability*:* Botnet remotely exploit the software used by the victim in their machines. Successful exploitation could lead an attacker to completely take over the host machine. After the attacker takes control of the host machine, they install malicious programs in the machine to create a user account with full administrative privileges. After the completion of this phase the boat launches attack to the infected host machine [10][11].

b. Instant Messaging: An extensive remote-controlled PCs are being used to construct an enormous botnet with the help of a computer worm that can be passed on through instant messaging. In September 2006 Security experts at US Company FaceTime identified the worm as 'W32.pipeline' and warned that it spreads via AOL's instant messenger program. These worms are embedded in a form of jpeg image or a website link[12].

c. P2P file sharing network: P2P is another method for infecting machines. The malware binary makes a copy of itself to the shared folder of popular P2P programs and uses legit names in order to trick a victim into opening the malicious binary. No susceptibilities are abused, but social engineering is used by these malwares binaries to spreadfurther[13].

2.2 Command and Control (C&C)Mechanism

The bot institutes a command and control (C&C) channel, and connects the zombie to the command and control (C&C) server using different models, topologies and different kinds of applications such as HTTP, P2P, IRC etc. The zombie then becomes a part of attacker's botnet army upon the creation of C&C channel. The bot-master uses C&C channel send commands to his bot army [14]. There are three types of botnet command control architectures: centralized, decentralized and hybrid.

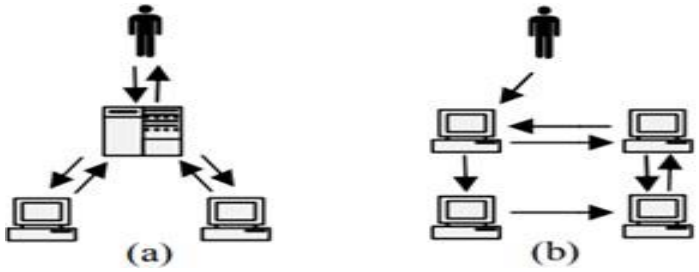

Figure 1: (a) Centralized and (b) Decentralized Mechanisms [15]

a. Centralized C&C:As show in fig. 1(a), Zombies or agents are associated with the central Command and Control (C& C) server to obtain commands and updates. C&C server provide services to register the available bots so that it is easier to track their activities. A bot-master must be connected to the C&C server in order to gain control of the bots and allocate its commands and tasks. However, there's a single point of failure, Centralized C&C are very common as they apply simple steps to create and direct the bots and the response rate is fast. It is divided into two types: Internet Relay Chat (IRC) and HTTP based on the communication protocols they use to establish their connection[15].

b. Decentralized C&C*:* As show in figure 1(b), Decentralized C&C architecture is based on peer-to-peer (P2P) network model. In this type of model, the infected host machines themselves act as bot as well as a C&C server at the same time. In P2P model, each bot acts as a server to send the commands to its nearby bots instead of having a central C&C server. The bot-master sends commands and tasks to one or more than one bot, after the bots receive the command, they then transmit it to the other bots. Unlike centralized bots it is a complex procedure to create and manage P2P botnets and requires high level of expertise[15].

c. Hybrid C&C:As mentioned previously, every C&C mechanism has its own pros and cons regarding the comfort of use and management and effort of desertion and detection. In order to take advantages of each C&C model, different protocols and architectures are used to form a hybrid approach. For example: HTTP2P botnets communicate with HTTP protocol to avoid firewalls over a P2P structure in order to eradicate the central C&C server's traditional shortcomings. This hybrid approach is not just only limited to the use of certain services or architectures. In fact, bot-masters are free to use any applicable protocols to implement this model [15].

3. SECURITY THREATS FROMBOTNET

In today's world the complexity of botnets and highly skilled & organized bot-masters is growing rapidly as a potent threat from viruses, Trojan horses, network intrusion, worms and other familiar cyber/network threats that poses a risk to the internet security and privacy [16] [17]. As bots are tiny applications that slips onto a person's computer in many ways, they often transmit themselves over the internet by searching for vulnerable, unprotected computers are prone to risk. When the bots find an exposed computer, they rapidly corrupt the machine and then report back to their bot master. The main objective of bots here on after is to stay hidden on the host computer until they are requested to carry out a certain task. Although, bot-masters need not to be highly technical and yet some are organized, smart and skilled day by day. They send millions and millions of bots through online games and polls and people easily become the victim to botnets [18]. Because, bot-masters are harder to identify and they can execute attacks such as; DDoS, identity theft, phishing, spamming, and click fraud but not limited to, using numerous strong tools and/or by commanding zombies to carry out various types of attacks[19].

3.1 DDoS (Denial ofService)

DDoS is a malicious attack to disrupt the computer attacks which are often infected with a Trojan to target a system. Attackers attempt to use number of hosts to overwhelm a server with a flood of internet traffic. They take control over online machines and overwhelm a server sending number of hosts and compel a website to experience a complete crash. An attacker starts the process by taking advantage of vulnerability in a computer system. Using a single command, the attacker instruct the zombies to pass the several flood attacks towards a target. They infect the device with malware turning one into a bot. When the botnet targets the IP address of a victim, each bot will respond by sending request to the target which results in a denial of service [19] [20].

3.2 Phishing and identitytheft

Phishing is a form of fraud where attackers spoof emails and other technical tools to learn the sensitive information's such as security number, login credentials, bank information. The attackers send victim a fraud email which looks extremely professional and realistic where victim is compelled to enter their personal and sensitive information's. It is one of the popular crimes among the attackers. It just needs spoofed link and organizational logo to fool the victim. There are two types of phishing; one is targeted to online identity where attacker target the company and second target towards their customer. These days the attackers are targeting the banking and online company. It is easy to fool the victim by sending the phishing links to hack their information's. Bot-master designed the emails that look professional with company logos, colors, graphics, and font styles to proof the sender. When the recipients of email clock on the email the hacker enter their account and get their id, password, social security number and other important personal information [17] [19].

3.3 ClickFraud

Click fraud is an illegal internet crime when a person clicks the automated internet ads. It is one of the biggest threats to the online economy. Criminals set up the automated scripts on some of the websites to register clicks on person per clicks.

The one clicks per person counts the number of people who visited the website. It is hard to detect the fraud related botnet. These days bot masters are using large number of geographically dispersed IP address and quick register click links. Click fraud activity generates large volumes of revenue for attackers and their customers but at the same time poses a great threat to both the advertisers and the content providers and thus is considered as an emerging threat to e-commerce[20].

3.4 IllegalHosting

A computer or server with high bandwidth connection and larger storage to the internet can become a target for a bot-master to gain control and use for file sharing and illegal hosting. Botnet programs and hosting services are available for sale or rent for the malicious purposes in any required duration [19].

4 BOTNET DETECTIONTECHNIQUE

Detecting botnet is not easy, it is designed to operate while user is still unaware about it. The increase in botnet activity has attracted the most of the people's attention in cyberspace. It can be a difficult task to detect bot without the knowledge of the botnet. The bot master is rapidly involving in the propagation of the detecting bots. They uses several current techniques to implement and get better information about the type of attack. Detecting a botnet needs advanced evaluating capabilities which should be tracked, and certain characteristics of issues needs to be performed. The paper presents categorization of the botnet detection techniques as follows:

4.1 Initial sign andsymptoms

If we look carefully on system, we can notice some common signs that a network may be infected with a botnet virus such as when the machine starts and shows several symptoms of botnet infiltration. Awareness of these symptoms can aid in early botnet detection. Another sign occurs when there is a problem with internet access and it sends the outbound messages such as instant messages, email, social media etc. There are spikes in traffic for Port 1080 (used by proxy servers), port 25 (used in email spamming), and port 6667 (used for IRC). Computer run slow and uses high CPU. There are unexpected high pop ups in the websites. It shows high outgoing SMTP, multiples machines on a network making identical DNS requests. Botnets and bot masters use IRC for communication. There are connection attempts with known C&C servers. These are evidence shown in individual, compromised workstationsnetwork.

4.2 Botnet Detection at the endpoint

There is another way to detect botnet on host- based that start with client-side anti -viral solutions. It is mainly infiltration itself with malware. Antiviral technology could not pinpoint the spot an infection. In this situation the administrator should look for other additional issues. There are couple of Host -based botnet detection. We can see unexpected pop ups while browsing over HTTP, rootkit installations, any sudden change to the Windows Hosts file that used to restrict outbound server access. If there is modified on default DNS server the traffic will go to another way, where it should not go..

4.3 Botnet Detection on theNetwork

It is difficult to detect botnet on network-based. However, there are some way we can detect by monitoring IRC (Internet relay chat) traffic as it is no longer exist on a company at all. Packet sniffer is used to detected IRC traffic encrypted keywords. At endpoints there are sudden and frequent hit by one or more external sites which is the sign of bot-driven DDOS attack that comes from network. There is a huge outbound traffic happens on SMTP that shows spam-mail is an issue.]. A new approach for detecting and characterizing botnets on a large-scale Wi-Fi ISP network is proposed by Wei Lu and Ali A. Ghorbani.. They first classified the network traffic into different applications by using payload signatures and a novel clustering algorithm and then analyzing the specific IRC application community based on the temporal-frequent characteristics of flows that leads the differentiation of malicious IRC channels created by bots from normal IRC traffic generated by human beings. They evaluated their approach with over 160 million flows collected over five consecutive days on a large-scale network and results showed that the proposed approach successfully detects the botnet flows from over 160 million flows with a high detection rate and an acceptable low false alarmrate.

4.4 Botnet Detection viaHoneypot

Security personal creates a trap known as honeypot to collect valuable information about malicious activity. In below picture a honey pot is outside the external firewall. It is useful for tracking to scan or attack the internal network. The good thing about it that it does not increase the risk for the internal network. It also reduces the alerts issued by the firewall. A honey pot can also be deployed in different location such as in DMZ, internal network alongside with servers and workstations [18][19]. The general structure of honeynet based method consists of honeypot and honey wall. Honeypot denotes an end host which is very vulnerable to malicious attacks and is often successfully compromised in a very short time span. Honeywell denotes software which is used to monitor, collect, control, and modify the traffic through the honeypot, such as Snort. The idea behind this methodology is to lure in attackers such an automated malware and then study of them in detail. Honeypots have proven to be very effective tools in learning more about Internet crime like botnets.

5 BOTNET DETECTIONTOOLS

5.1 Net Flow analyzer: Normally, antivirus software uses dynamic codes and sometimes it is difficult to detect worms with it. In that situation, DDOS attack can be detected using Cisco NetFlow analyzer. At first, Cisco NetFlow analyzer finds out the spikes in the overall flow of all the routers. After identifying the spikes originating from the router, it digs more into the origin of these anomalies and finds out where the destination of these flow goes. This explains whether the transfer from router is occurring to an unplanned host.

5.2 Ntop: It is a powerful network sniffing and statistics gathering tool which can be used along with Darknet. It analyzes and detects botnets. The Darknet refers to public and private chunk of a network that is void of any servers. The idea of Darknet is influenced from honeypots and usually underestimated. The setups are showing in below diagram. Those

packets that are marked blocked are inspected instead of just discarded. All the packets in a Darknet are not the legitimate packets. There are options provided in Ntop, they are network usage graphs, sorting packets by hosts and ports, detect host OS, vendor and other details about the hosts.

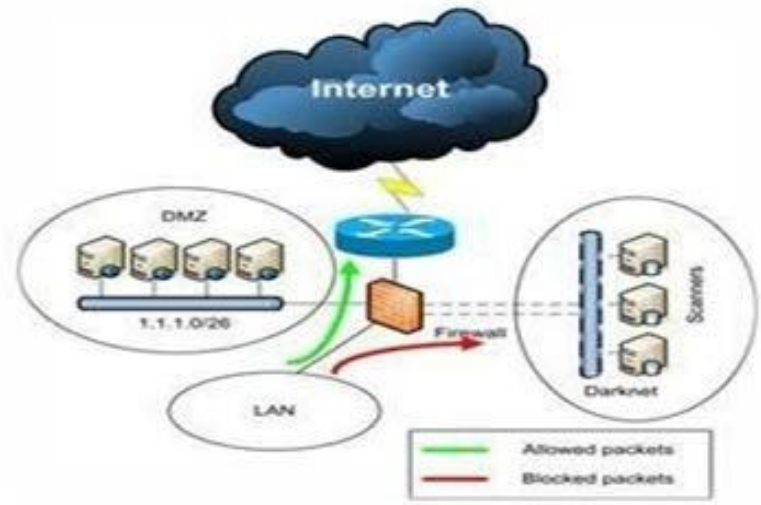

Figure 3: The Ntop Model

5.3 *Snort*:It is used along with Darknet and Ntop to log alters. Basically, snort is used for detecting botnets based on their signatures. Configuration of snort.conf is important. An alter is recorded in the file after the traffic matches any of these botnet signatures and those packets can be further analyzed in Wireshark for more details. There is also a facility for writing your own signatures for making snort customizable for botnet detection.

5.4 Wireshark:Wireshark is a powerful tool with wide-ranging applications. Here, we are going to use the tool for DNS traffic analysis. DNS-based botnet detection technique is based on domain name system (DNS) information generated by a botnet. The Wireshark is to create a CSV file using a GUI tool like logparser or 'tshark -r Myfile -t fields' command to do this. Once we are done, we can recover the DNS name and the respective IP information from the CSV file.

6 BOTNET PREVENTION TECHNIQUES

There are several measures that users can take to prevent botnet virus infection. Since bot infections usually spread via malware, many of these measures focus on preventing malware infections. Some of the recommendation for botnet prevention are as follows:

6.1 Install anti-virus andanti-spyware

To prevent from the botnet, we should install antivirus and antispyware programs from the trusted sources. These programs help to scan and monitor viruses and spywares. When programs find anything suspicious on the computer, they warn us, and we must act. There are lots of good antivirus and antispyware program available in the market such as

Notron, Mcafee, Kaspersky, Intrusta.

6.2 UpdateSoftware

Software update improved security, performance, and stability of the machine. In our devices when we see any warning saying it needs to update, we need to do that on time. It saves significant amount of time and trouble in the future. If possible, set the automatic update.

6.3 UpdatePassword

Computer stores and provides access to lots of important and sensitive data. Computer and data security are always the top priority in any organization. Some people can try to hack the computers and to prevent it we should change the password of devices regularly. The password should me strong and secret.

6.4 Firewall

Firewall puts a protective barrier between computer and the internet, it should always turn on. Only a few minutes turnoff increases the risk of computer being infected by viruses.

6.5 Disable Universal Plug (UPnP) onrouters

UPnP is a set of network protocols. It has the feature to automatically connect configure network devices. After the connection was started from the local network, it automatically forwards to the port. It trusts the Local area network outgoing requests by default. This makes the router vulnerable and chances for hackers to change DNS setting on router. That is why we should disable UPnP on router to stay safe.

7 CONCLUSION

The criminal minded people are increasing which poses the potential threat every legitimate user, infrastructure of the internet and timeless service provided as the internet user are increasing. The aim of this paper is to pass message towards people about the current state of bots and botnet and its malicious activities that are hamerping people. It is affecting the almost every single individual and business. The boaster are well oragnzed and have knowledge of controlling the network. Therefore, botnet detection has been a biggest challenge currently. There are various tools and techniques being used to detect the malicious activities and still need to pay more attention to save our network being hacked or attacked by the attackers. All the techniques are being used might not be fully applicable for new generations of botnets. Hence, discovering new techniques based on data mining and DNS traffic for botnet C&C traffic detection can be a good approach to control the threat against online ecosystems and computerassets.

REFERENCES

[1] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs." In Companion Conference of the Supercomputing-2018 (SC18),2018.

[2] Hoque, Nazrul, Dhruba K. Bhattacharyya, and Jugal K. Kalita. "Botnet in DDoS attacks: trends and challenges." IEEE Communications Surveys & Tutorials 17, no. 4 (2015):2242-2270.

[3] Tyagi, Amit Kumar, and G. Aghila. "A wide scale survey on botnet." International Journal of Computer Applications 34, no. 9 (2011):10-23.

[4] Mailewa, Akalanka, and Jayantha Herath. "Operating Systems Learning Environment with VMware." In The Midwest Instruction and Computing Symposium. Retrieved from http://www.micsymposium.org/mics2014/ProceedingsMICS_2014/mics2014_submission_14.pdf. 2014.

[5] Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. "DDoS in the IoT: Mirai and other botnets." Computer 50, no. 7 (2017):80-84.

[6] Alomari, Esraa, Selvakumar Manickam, B. B. Gupta, Shankar Karuppayah, and Rafeef Alfaris. "Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art." arXiv preprint arXiv:1208.0403(2012).

[7] Hoque, Nazrul, Dhruba K. Bhattacharyya, and Jugal K. Kalita. "Botnet in DDoS attacks: trends and challenges." IEEE Communications Surveys & Tutorials 17, no. 4 (2015):2242-2270.

[8] Elliott, Claire. "Botnets: To what extent are they a threat to information security?." Information security technical report 15, no. 3 (2010):79-103.

[9] Li, Chao, Wei Jiang, and Xin Zou. "Botnet: Survey and case study." In 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC), pp. 1184-1187. IEEE,2009.

[10] Tyagi, Amit Kumar, and G. Aghila. "A wide scale survey on botnet." International Journal of Computer Applications 34, no. 9 (2011):10-23.

[11] Mailewa, Akalanka, Jayantha Herath, and Susantha Herath. "A Survey of Effective and Efficient Software Testing." In The Midwest Instruction and Computing Symposium. Retrieved from http://www.micsymposium.org/mics2015/ProceedingsMICS_2015/ Mailewa_2D1_41. pdf.2015.

[12] Hachem, Nabil, Yosra Ben Mustapha, Gustavo Gonzalez Granadillo, and Herve Debar. "Botnets: lifecycle and

taxonomy." In 2011 Conference on Network and Information Systems Security, pp. 1-8. IEEE, 2011.

[13] Saad, Sherif, Issa Traore, Ali Ghorbani, Bassam Sayed, David Zhao, Wei Lu, John Felix, and Payman Hakimian. "Detecting P2P botnets through network behavior analysis and machine learning." In 2011 Ninth Annual International Conference on Privacy, Security and Trust, pp. 174-180. IEEE,2011.

[14] Zeidanloo, Hossein Rouhani, and Azizah Abdul Manaf. "Botnet command and control mechanisms." In2009SecondInternationalConferenceonComputerandElectricalEngineering,vol.1,pp.564-568. IEEE, 2009.

[15] Rahimipour, Maryam, and Shahram Jamali. "A Survey on Botnets and Web-based Botnet Characteristics." International Journal of Science, Engineering and Computer Technology 4, no. 11 (2014):282.

[16] Caglayan, Alper, Mike Toothaker, Dan Drapeau, Dustin Burke, and Gerry Eaton. "Behavioral analysis of botnets for threat intelligence." Information systems and e-business management 10, no. 4 (2012): 491-519.

[17] Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. "Secure NoSQL Based Medical Data Processing and Retrieval: The Exposome Project." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99-105. ACM,2017.

[18] Freiling, Felix C., Thorsten Holz, and Georg Wicherski. "Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks." In European Symposium on Research in Computer Security, pp. 319-335. Springer, Berlin, Heidelberg,2005.

[19] Banday, M. Tariq, Jameel A. Qadri, and Nisar A. Shah. "Study of Botnets and their threats to Internet Security." Sprouts: Working Papers on Information Systems 9, no. 24(2009).

[20] Thing, Vrizlynn L., Morris Sloman, and Naranker Dulay. "A survey of bots used for distributed denial of service attacks." In IFIP International Information Security Conference, pp. 229-240. Springer, Boston, MA,2007.