International Interdisciplinary Virtual Conference on
'Recent Advancements in Computer Science, Management and Information Technology'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

A Study on Botnets

H. J. Kharat*[1], P. A. Ghuge[2], S. K. Devade[1], R. K. Shirsat[1], D. V. Petkar[2]
*[1]Department of Physics, Shankarlal Khandelwal College, Akola, Maharashtra, India
[2]Department of Computer Science, Shankarlal Khandelwal College, Akola, Maharashtra, India

ABSTRACT
In this age of digital technology, internet has become an integral part of our life. It is the global system of interconnected computer networks which links the devices into one entity. It carries and provides an extensive range of information useful for all types of users. However some of the people identify and then exploit the weaknesses in a computer system through internet and gain unauthorized access to personal or organizational data. This negative approach mostly called as hacking. Hackers use the various software's or programs such as RAT (remote access Trojan), Botnet etc for gaining the unauthorized data from unknown users and becomes cyber criminals. In the present study we have described the working of botnet and preventive measures against the hacking of the systems.

Keywords: Software, Botnets, BotnetTypes, Hackers

I. INTRODUCTION

Internet is being a basic need of every one. Increase of speed and use of internet provides opportunity for hackers to perform the criminal activities [1]. Hackers used different softwares for illegal access of personal data. A botnet is basically a software that is being used by hackers on a very large scale. Botnets are networks of compromised computers, also known as "bots" or "zombies," that are under the control of a single attacker.[2].
Botnet includes two terms, Bot stands for Robot and net stands for Network. This software works in two places server side and client side. In this, hackers create a malicious application or software in exe format and send it to their target. And once it gets into the target's system, the hackers get remote access to that system. Botnets are networks of hijacked devices infected by a common type of malware and used by malicious actors to automate widespread scams and massive cyberattacks, It can be used for sending spam emails, launching distributed denial-of-service (DDoS) attacks, stealing sensitive information, and spreading more malware to other computersThey can also be used for political purposes, such as launching cyber-attacks on government websites or disrupting critical infrastructure. [3].
Each individual device on a botnet is known as a "bot". Individual threat actors or small teams of hackers can use botnets to execute much larger attacks than previously possible [4]. With little cost and time investments, botnets are both widely accessible and more efficient than traditional attack methods. By commanding every computer on its botnet to simultaneously carry out the same instructions at the same time, a malicious actor

can successfully launch attacks designed to crash a target's network, inject malware, or execute CPU-intensive tasks [5].

1. Working of Botnet

A botnet is automated computer software. Server side is the hacker's side on the server side an application or software is created in exe format which will work on the client side. While creating it, it has different features like it will not be uninstalled, admin access such features are turned on by hackers and make it. Once built, it needs to be deployed on the client side. Now normally people don't install any application or software. But a botnet that has a bot means this bot or this software is automatically on the silent side installs and assigns its remote access to the server side and thus a system is accessed and monitored. In this, hackers can take advantage of the hacked system[6]. It has a feature in which hackers bind the malicious app to another file and deliver it to the client side.ie from behind PDF or image, video. So that the target will not understand anything.When a bot-herder has successfully infected a sufficient number of bots, the next step is data collecting. The bot-herder sends commands o to the infected devices, and the bots carry out the orders [7].

The working of a botnet can be studied in a stepwise and simple manner as follows:

a. **Infection:** The attacker infects computers with malware, often through phishing emails, malicious websites, or exploiting vulnerabilities in software.
b. **Recruitment:** The infected computers are then added to the botnet and become part of a network of compromised devices under the control of the attacker.
c. **Command and Control:** The attacker uses a command and control (C&C) server to send instructions to the bots in the network. The C&C server can be located anywhere in the world, making it difficult to track down the attacker.
d. **Malicious Activities:** Once the bots receive instructions from the C&C server, they carry out various malicious activities, such as sending spam emails, launching DDoS attacks, stealing data, and spreading malware to other computers.
e. **Concealment:** Botnets are designed to remain hidden from the user of the infected computer, and often use techniques such as encryption and obfuscation to avoid detection by anti-virus and anti-malware software.
f. **Persistence:** Botnets are designed to be persistent and difficult to remove. They often have mechanisms in place to evade detection and removal, such as periodically changing their C&C server or using multiple servers.

Botnets are a significant threat to computer and internet security, as they can be used to launch large-scale attacks that are difficult to trace back to their source.

2. Types of Botnets

There are basically two types of botnets. First one is client-server model and second one is peer to peer model [8].

A. Client-Server Model

First generation botnets usually operate on a client-server model, which means one command-and-control (C&C) server is used to operate the entire botnet. However, centralized models are more susceptible to a single point of failure due to the simplicity of
their structure.(Fig.1)[9]

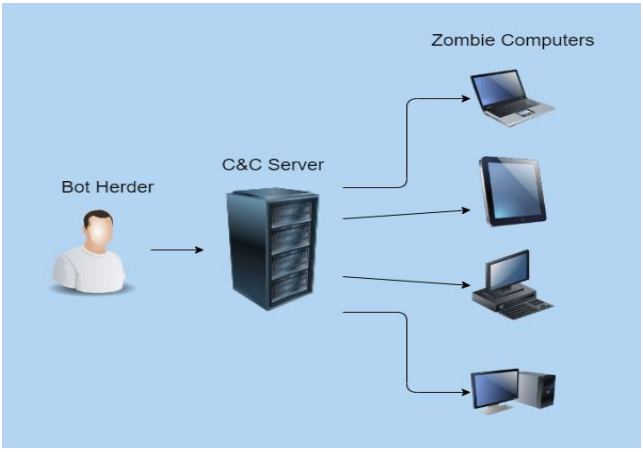

Figure1. Client Server botnet

B. Peer - Peer (P2P) Model

New generation botnets use predominantly peer-to-peer (P2P) models which allow bots to share commands and information with each other and without direct contact with C&C servers. P2P botnets are more reliable because they don't rely on a single centralized server.In a P2P model, each bot shares and updates information between devices by working as both a client and a server. (Fig.2)

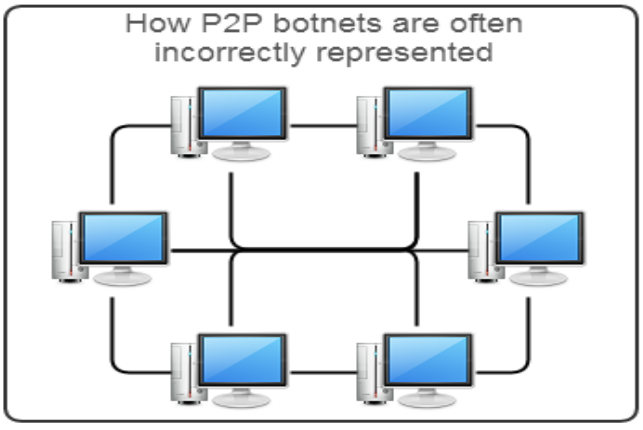

Figure 2.Peer - Peer (P2P) botnet

3. Common Types of Botnets

There are several types of botnets, each with different characteristics and purposes. Botnets are constantly evolving, and new types of botnets may emerge as attackers develop new techniques and strategies [10]. Following are some common types of botnets studied in this work:

1. **Spam Botnets**: These botnets are used to send large volumes of spam emails, often promoting scams or fraudulent products.
2. **DDoS Botnets:** These botnets are used to launch distributed denial-of-service (DDoS) attacks on websites or servers, causing them to become unavailable to legitimate users.
3. **Banking Botnets:** These botnets are designed to steal financial information, such as credit card numbers and bank account credentials.
4. **File-sharing Botnets:** These botnets are used to distribute pirated software or media files, often without the user's knowledge or consent.
5. **Click Fraud Botnets**: These botnets generate fraudulent clicks on online advertisements, allowing the attacker to earn money from ad networks.
6. **Ransomware Botnets:** These botnets are used to distribute ransomware, which encrypts the victim's files and demands payment in exchange for the decryption key.
7. **IoT Botnets:** These botnets are composed of compromised Internet of Things (IoT) devices, such as routers and security cameras, and are often used for DDoS attacks or cryptocurrency mining.
8. **Credential Stuffing:** Botnets can be used to test a large number of stolen usernames and passwords to gain unauthorized access to user accounts or sensitive data.
9. **Information theft:** Botnets can steal sensitive information, such as credit card numbers, login credentials, or personal data.

II. CONCLUSION

Internet users are increasing surprisingly, thereby increasing the possibility of cyber-attacks by using many software's. Amongst botnet is frequently and morely used software by the hackers. Botnet propagates itself time to time and changes its shape with time and increases criminal activities without knowing end users. Different types of botnets attacks and general solution as preventive measures have been presented. Any file received have to scan first before to open and if it is found infected should have to delete and block the person. Preventative measures include keeping software up-to-date, using strong passwords, and using anti-virus and anti-malware software.This reduces the possibility of botnet attacks.

III. ACKNOWLEDGEMENT

Authors are thankful to the head of the department of Physics and department of Computer Science for their kind support and guidance for understanding the topic and preparing the paper.

IV. REFERENCES

[1]. Sarath R Mammunni, Sandhya C P, "AN OVERVIEW OF BOTNET AND ITS DETECTION TECHNIQUES" in International Journal of Creative Research Thoughts (IJCRT) ISSN 2320-2882, Value 8 Issue , March 2020.

[2]. YogitaBarse ,Dr. Sonali Tidke "A Study on BOTNET Attacks and Detection Techniques" in IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 15, Issue 3 Ser. II (May – June 2020), PP 01-05.

[3]. Moheeb Abu Rajab Jay Zarfoss Fabian Monrose Andreas Terzis, "A Multifaceted Approach to Understanding the Botnet Phenomenon"

[4]. A. Deshpande and R. Sharma, "Anomaly Detection using Optimized Features using Genetic Algorithm and MultiEnsembleClassifier", 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.

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

[6]. 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.

[7]. Mr. Sandip Sonawane, -2018" A Survey of Botnet and Botnet Detection Methods", International Journal of Engineering Research & Technology (IJERT)http://www.ijert.org ISSN: 2278-0181IJERTV7IS120024, Vol. 7 Issue 12, December".

[8]. M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, K. W.Hamlen, 2008," Flow-based identification of botnet traffic by miningmultiple log file," in Proc. International Conference onDistributed Frameworks & Applications (DFMA), Penang,Malaysia.

[9]. J. H. Lee, "Rise of Anonymous Crypto currencies: Brief Introduction," IEEE Consum. Electron. Mag., vol. 8, no. 5, pp. 20–25, 2019, doi: 10.1109/MCE.2019.2923927.

[10]. Rishikesh Sharma, AbhaThakral," Identifying Botnets: Classification and Detection", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-9S