CLASSIFICATION OF THE FRAMEWORK OF BOTNET LIFE CYCLE

Mr. Deevi Harikrishna
Research Scholar, Department of Computer Science and Engineering, Sri SatyaSai University of Technology and Medical Sciences, Sehore, Madhya Pradesh, India.
Dr. Neeraj Sharma
Research Supervisor, Department of Computer Science & Engineering, Sri SatyaSai University of Technology & Medical Sciences, Sehore, M.P., India
Dr. B. Bhanu Prakesh
Professor, Department of Computer Science & Engineering, KKR & KSR Institute of Technology & Science, Guntur, A.P

ABSTRACT

Security risks are also rapidly changing in tandem with the development of new systems and technologies. When it comes to eliminating security threats, a lot of time and effort is needed to learn everything possible about a certain one. The greatest danger to the safety of the internet community comes from compromised computers or BOTNETs. Companies are investing more each year in the latest and greatest hardware and software solutions to combat BOTNETs. This article provides a comprehensive overview of the security challenges posed by BOTNETs, including an examination of their potential trajectory, current state of development, and potential vulnerabilities that may be exploited to compromise an organization's most important resource: its data. Systems that have been breached might be compared to viruses in the network, with the potential to do significant damage to the company, including the theft of sensitive information.

Keywords: Malware, Zombie, Attacks, Information, Life cycle
DOI Number: 10.48047/NQ.2022.20.4.NQ22333 **NeuroQuantology2022;20(4): 1092-1097**

I. INTRODUCTION

When anything is done to ensure a network is safe, we say that it is secure. Typically, these measures are taken to ensure the availability, dependability, integrity, and security of the data and the network. Networks with strong operational security are better prepared to deal with and prevent attacks from a wide variety of threat vectors. Network security is under attack from a wide variety of sources. Trojan horses, viruses, worms, spyware, malware, BOTNETs, zero-hour attacks, hacker attacks, DoS (denial of service) assaults, data interception and theft, identity theft, etc.

A "botnet" is a collection of compromised computers that are managed by a single hacker, or "botmaster," from afar. The phrase "botnet" combines the words "robot" and "network," and refers to a group of robots that work together to carry out the botmaster's commands. The botnet's mission is to carry out assaults in accordance with the guidelines set out by the botmaster.

Botnet assaults are a major problem and a major risk to data integrity. There is still an ongoing arms race between botmasters and researchers who are trying to stop malicious botnets. As the stakes are higher, both sides ramp up their preparations for victory. Botnets are effective because of the large number of bots working together to launch coordinated attacks. Another feature that helps improve bots is the botmasters' ability to keep them hidden from any security

system. When it came to the number of infected devices, the Mirai Botnet was one of the most well-known and shocking examples. The Mirai botnet exploited and propagated through Trojans that were installed on IoT devices like webcams and CCTVs that lacked proper security protocols. One hundred thousand Internet of Things (IoT) devices were deployed in the largest Mirai attack, which resulted in a 1.2 Tbps assault.

Simply described, BOTNETs are groups of computers that work together to commit illegal activities by use of malicious software.These bots are commonly used by attackers to infect large numbers of machines simultaneously. The collective of these machines is called BOTNET. These zombies may be used for many malicious purposes, including but not limited to: spam email distribution, malware dissemination, server attacks, and other forms of fraud and criminality.

BOTNET might be either little or rather big, depending on the circumstances. The quantity of bots in BOTNET is proportional to their level of sophistication and complexity. The number of zombies in a big BOTNET can easily reach into the hundreds of thousands. The tiny BOTNET was only made up of a few thousand zombies.

II. APPLICATION OF BOTNETS

Whenever a computer is infected by BOTNET, the legitimate user loses access to all of the system's data and resources, which has devastating effects on both business and personal security. The vast majority of people keep sensitive data on their personal computers.All of that private and sensitive information may be stolen from this computer if its security were breached. In the past, bot herders would rent out or sell their BOTNETs to hackers looking to conduct illicit operations. BOTNETs, with their formidable penetration and strength, allow attackers a growing foothold in the cyber realm. As the number of BOTNETs grows, the herder is able to exert more control over infected machines, allowing them to carry out increasingly sophisticated and common attacks.The following are examples of BOTNETs more serious uses:

- **Click Fraud**

  It is possible to commit Click Fraud with BOTNETs. In this con, bot software is used to search the web and click on ads without any human intervention. Let's say a herder manages to set up a botnet of several thousand machines and steals a sizable sum of money from ad networks that pay a nominal sum per click. An enormous network means that even a little investment of a few clicks per user might provide substantial earnings. There's no way for investigators to figure out that it's a fraud if the clicks are coming from all over the world, on different computers.

- **Distributed Denial of Service (DDoS)**

By entirely entrapping and overwhelming its bandwidth and other resources, BOTNETs are utilised to remunerate confrontation on several machines across the network accessing the internet. Such distributed denial of service assaults can prevent users from accessing websites for extended periods of time. When the financial infrastructure is taken into account, the delay in accessibility exerts a tremendous load on the financial institutions that are unable to serve their clients.DDoS also include attacks in which the perpetrators demand money before releasing the resources they've blocked and resuming normal network activity. Extortion attacks are a specific form of cybercrime. Figure 1 provides a reference for the entire diagram.

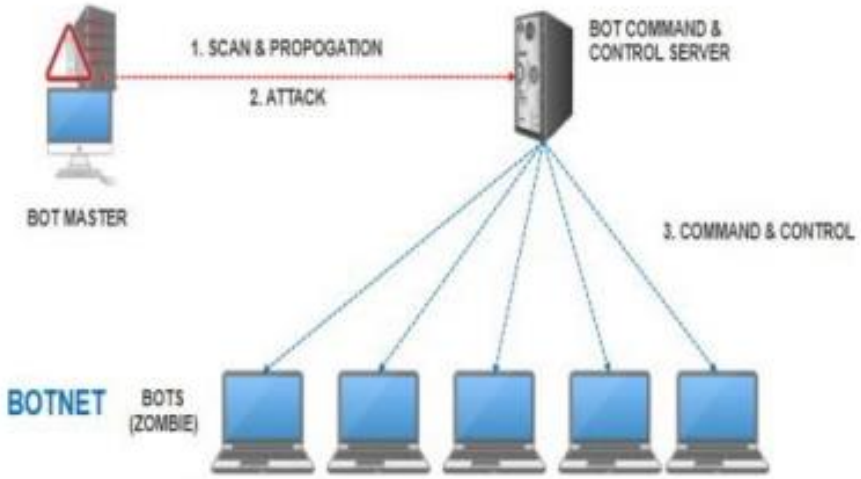

Figure 1: Distributed Denial of Service (DDoS)

- **Key logging and Mass Identity Theft**

The process of recording the succession of keys pushed is called "key logging." A key logger programme installation will allow you to accomplish this. The user's keystroke sequence can be gathered with this encryption software. The user's identity and any relevant passwords are part of this. For this and other reasons, this has been a major catalyst for the vast amount of PayPal account theft that has occurred over the previous few years.Anattacker can use a bot as a front in a massive identity theft scheme. This includes "phishing" techniques, when an individual poses as a corporate representative in order to trick a victim into divulging sensitive information (such as a password or credit card number). Spam emails are commonly used to apply the phishing tactic, which involves tricking a user into submitting personal information by using a link that seems to go to a legitimate banking or online transaction website.

Many bots provide the herder full access to the file system, even if they record all keystrokes. The herder can then alter and transmit any file, access any private data saved on the user's computer, and upload hazardous files.

- **Traffic Monitoring and Spamming**

TCP/IP proxy protocols are used in BOTNETs for a variety of network applications. After a computer's IP has been hacked, bot commander may utilize it to send out phishing, fraud, and other malicious emails in enormous quantities. To do this, the bot commander steals the IP address of another bot and uses it to send out a flood of spam messages.By using infected computers, a zombie can operate as a packet sniffer, keeping tabs on network traffic and activity. Most commonly, these sniffers attempt to collect usernames and passwords for various accounts that a bot commander may then utilize for its own ends.

- **Warez**

Warez is another use case for BOTNETs. Warez is a term used in the hacking community to refer to a method of stealing software licenses. BOTNETs are prone to stealing, storing, or spreading Warez. Infected computers' hard drives can be scanned for licensedprograms and apps. After locating the license, the herder can copy it and disseminate it widely online, in violation of the software's copyright. Figure 2 is an example of Warez.

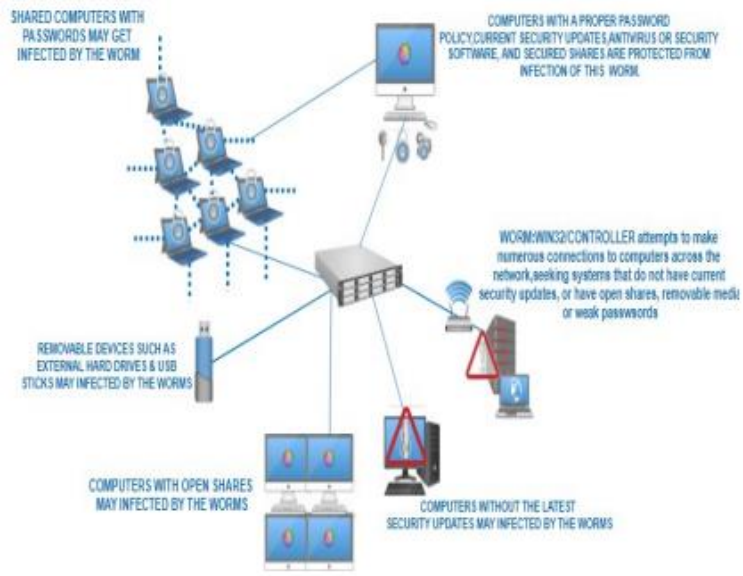

Figure 2: Illustration of Warez

III. BOTNET LIFE CYCLE

Botnets' basic life cycle is seen in Figure 3. There are some procedures it must go through before it can begin functioning as a bot for the host system. To begin communication amongst bots, the botmaster must first perform the "initialization" phase of the botnet life cycle. Afterwards, the botmaster registers with the distributed domain name system (DDNS), which gives the botmaster a permanent Internet Protocol (IP) address. The standard infection technique begins with an injection stage, where infections can take many forms (such as viral propagation, unsolicited downloads, downloading and executing malicious attachments from emails, or infected external disc drives).

In the following phase, bots construct their networks and plant harmful software. The compromised host makes network-based database queries, installing malicious programs. Once these malicious programs are installed on a host, it begins behaving like a true bot. Moreover, HTTP, FTP, or P2P protocols are typically used throughout the downloading procedure.

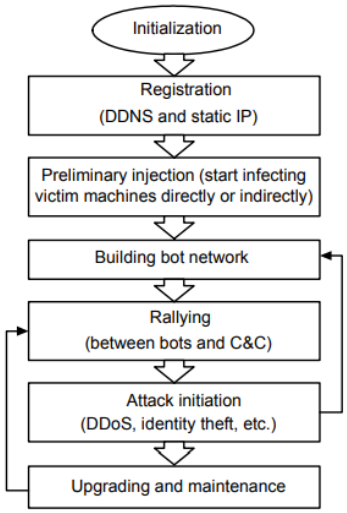

Figure 3: Botnet flow diagram

Some scholars refer to what happens next as the "connecting phase," although the term "rallying" has become more widely used. Indeed, this procedure is always carried out whenever a bot restarts, guaranteeing the connection setup status between the botmaster and bots, allowing the bots to

participate in the botnet process and receive directions for carrying them out.

For this reason, the rallying phase of a bot's development is an ongoing one. In the attack phase, when the C&C channel has been successfully established with the bots, the bots wait for orders from their C&C before beginning their harmful operations. The ultimate goal of botnets is to carry out harmful actions such as Distributed Denial of Service (DDoS) assaults, traffic analysis, resource theft, malware distribution, system vulnerability scanning, identity theft, document exploitation, game manipulation, and survey manipulation.

Botnet maintenance and upgrades occur in the latter phase of the life cycle. The botmasters and their robotic armies require regular upkeep to ensure that they are ready for any future coordinated strikes. The binary code for the bot army is often updated for a variety of reasons, including protecting itself from new forms of detection, preventing itself from behaving in the same way, and incorporating additional feature sets to facilitate communication over multiple C&C channels. It is the sole responsibility of the botmaster to ensure that the modifications are reflected as fast as possible, as this is typically regarded a vulnerable period in which the botnet may be recognized by analyzing comparable network activity.

IV. CONCLUSION

When it comes to network security, BOTNETs are a major concern. This study discussed some of the most notable features of BOTNETs and offered an explanation for why these networks pose such a serious threat to network safety. Accordingly, educating end users on the dangers posed by viruses like this is crucial. Since botnets now pose a threat on a worldwide scale, it is imperative that many actors (network operators, governing bodies, etc.) work together to eradicate this menace. In a similar vein, establishing global regulations and negotiating potential international legislative issues to comprehensively address the concerns posed by the botnet phenomena are crucial.

REFERENCES: -

1. P. Wainwright and H. Kettani, “An analysis of botnet models,” in ACM International Conference Proceeding Series, New York, New York, USA, 2019, no. March, pp. 116–121.
2. X. D. Hoang, “Botnet Detection Based On Machine Learning Techniques Using DNS Query Data,” pp. 1–11, 2018.
3. R. Chen, W. Niu, X. Zhang, Z. Zhuo, and F. Lv, “An Effective Conversation-Based Botnet Detection Method,” Mathematical Problems in Engineering, vol. 2017, 2017.
4. Chen, C.M., Huang, M.Z., Ou, Y.H., 2013. Detecting webbased botnets with fast-flux domains. Advances in Intelligent Systems and Applications, Volume 2. Springer, p.79-89. [doi:10.1007/978-3-642-35473-1_9]
5. Tartakovsky, A.G., Polunchenko, A.S., Sokolov, G., 2013. Efficient computer network anomaly detection by changepoint detection methods. IEEE J. Sel. Topics Signal Process., 7(1):4-11. [doi:10.1109/JSTSP.2013. 2241912]
6. Ge, L., Liu, H., Zhang, D., et al., 2012. On effective sampling techniques for host-based intrusion detection in MANET. IEEE Military Communications Conf., p.1-6.
7. Jian, G., Zheng, K., Yang, Y., et al., 2012. An evaluation model of botnet based on peer to peer. IEEE 4th Int. Conf. on Computational Intelligence and Communication Networks, p.925-929.
8. Aviv, A.J., Haeberlen, A., 2011. Challenges in experimenting with botnet detection systems. USENIX 4th CSET Workshop, p.1-8.
9. François, J., Wang, S., Engel, T., 2011. BotTrack: tracking botnets using NetFlow and PageRank. NETWORKING, p.1-14.
10. Zeidanloo, H.R., Shooshtari, M.J.Z., Amoli, P.V., et al., 2010. A taxonomy of botnet detection techniques. 3rd IEEE Int. Conf. on Computer Science and Information Technology, p.158-162.
11. Bailey, M., Cooke, E., Jahanian, F., et al., 2009. A survey of botnet technology and defenses. IEEE Cybersecurity Applications & Technology Conf. for Homeland

Security, p.299-304. [doi:10.1109/CATCH.2009.40]

12. Feily, M., Shahrestani, A., Ramadass, S., 2009. A survey of botnet and botnet detection. IEEE 3rd Int. Conf. on Emerging Security Information, Systems and Technologies, p.268-273.