Botnets: Security Challenges, Taxonomy and Detection

By **Sumayah Bint Abdullah**

Abstract— **Botnets, a prominent threat to IoT security. 'botnet' this word is the composition of robot and network. A network of robots used to commit cybercrime. A bot means a compromised end-host or a device which is a member of a botnet. [2] Governments have become a popular target for malicious attacks. This is due to them holding mass confidential data on their network.**

Keywords*— *Botnets, Bots, bot controller, botnet detection, network, botnet architecture, botnet attacks, detection techniques

I. Introduction

Botnets are compromised collection of remotely connected computers. Botnets are also known as zombie botnets. This collection can consist of thousands of compromised hosts. These compromised hosts perform a large number of attacks whilst using a high amount of computing power. These machines are under the control of small group of hackers, called herders or botmasters. [3] These herders launch various attacks from spam emails to Denial-of-Service attacks. The activities of botnet attacks are to gather sensitive information from different informational systems. The impact of damage caused by bot herders is massive in comparison to traditional attacks. he elusive and evolving nature of botnets entails research to predict possible topologies. Botnet's harmful ability is becoming more understood, their technological advancement is becoming financially benefitting for hackers.

Although, their host is unaware of it, the botnets are structured to transmit messages to other devices on the network. The machines that develop a botnet can be programmed to relay messages to particular machines. A basic botnet network is applied through the IRC communication approach. Other botnet network types include Centralized, decentralized, HTTP, P2P and HTTP2P Traffic mixed. A botnet network can be commanded with any type of access to the root privileges of machines. This access can be deployed by email access or (SSH) Secure Shell connectivity. [4]

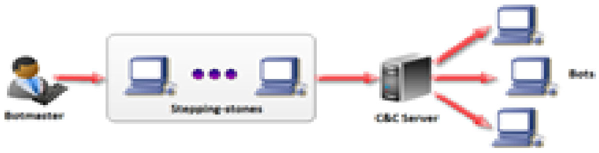

Fig 1. Model of Typical Botnet [15]

II. Background

Botnets are one of the most common ways for malware to propagate, they are mainly responsible for large-coordinated attacks. [10] Botnets are expected to evolve further in the future. Botnet researchers believe further research will be used to reduce the application of botnets. The further research will be beneficial in understanding the botnet behavior and architecture. Since there is not a lot of reliable data on this threat, it is difficult to understand the scale of the issue. The cybercrime industry has prospered due to the productivity of using botnets as a method for extortion [20]. The larger the botnet network the larger its detrimental power. Sophisticated botnets are used to infiltrate the monetary sector and large corporations in this industry are skilled against cyber-attacks. This industry is the most popular target for botnets, initially botnets were constructed for banks. Botnets such as Darkness and black energy have benefited financially from the monetary sector. Since every business on the internet is a target for botnet attacks due to the use of online monetary system. [18] The criminal industry has prospered due to the high efficiency and low cost of using botnets as a method to gain illegal profits. Botnets must connect more machines to its network to evolve and become more vigorous.

III. Botnet History

A. *Traditional Botnets*

This is a botnet containing a compromised class of servers or machines. These zombies are tainted with malware which enables the cyber criminals to control them [22]. Botmasters can control these compromised computers in the botnet because of either the peer-to-peer or the IRC.

B. *IoT Botnets*

This compromised collection of IoT devices: routers, cameras etc which are infected with malware. This malware enables the herder to take control and carry out tasks. Though, these IoT devices intend to spread malware and target more machines to expand their botnet. [16] An IoT botnet is larger in scale than that of a traditional botnet. It contains hundreds of thousands compromised machines. Whereas traditional botnets tend to consist of a smaller range. [16]

IV. Command & Control

- This is crucial to establish an active and operational botnet network. If you cause a disturbance in the communication connection, the bot controllers will be unable to execute coordinated attacks because the communication will be disrupted. C&C communications are similar to file download traffic. Understanding the botnet's command and control operation is significant in combating botnet attacks. [13]

A. *Command & Control architecture*

- There are two types of botnet architecture. The client-server structure and the peer-to-peer structure. In the client-server architecture, a single bot behaves as a central server, controlling the relay of data from the other connected bots. The botmaster uses certain software to create a connection and transfer information among the server and the client. This process is called the command & control. [1]

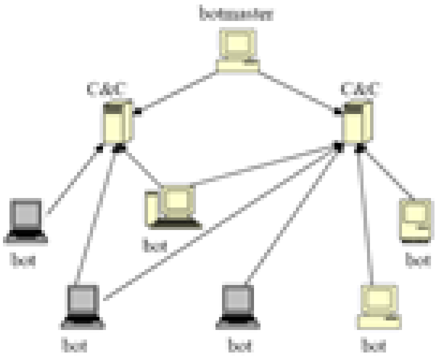

Fig 2. Centralized Model [19]

B. *Client-Server Structure*

- Client-server architecture is suited for preserving control on the bots and is detected easily by security analysts. This architecture can be taken down if the security analysts target the central bot. Early botnets would use centralized architecture [23]. The bot herder would dwell in one of the central servers.
- This architectural design is ineffective because it is connected to a single server. (Figure 2) Security analysts frequently target this single server, and if it is shut down, the entire structure will be rendered inoperable. Bot controllers use the peer-to-peer model to combat this weak structure.

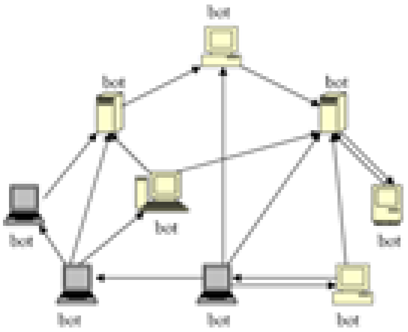

Fig 3. Peer-to-Peer Model [19]

C. *Peer-to-Peer Structure*

- This model is more secure and advanced than the previous model, it does not depend on the centralized C&C server to add new machines to the network. Each bot behaves as both server and client, each bot has a list of infected machines. Permitting each individual bot to create a connection with them. (Figure 3) It is challenging_to detect the source placement due to their being no central server. Removing one bot from this structure won't affect the overall botnet network. [1]
- The C&C communications occur when swapping assets shared by the nodes in the network [25,26]. The bot controller generates a file with bot commands then distributes it to the bots. This file is downloaded and shared again to new compromised devices. [5] Botnet architectures similar to the peer-to-peer model began to arise.

V. Communication Protocols

A. *Internet Relay Chat*

- This is designed for simple client-server and group communication. Developed to link clients with agents. This is an open protocol that uses TCP. The IRC server can expand the IRC network by connecting to other IRC servers. The messages are sent as byte code sequences. [13]

B. *The Hypertext Transfer Protocol*

- This protocol permits the bot controller to hide their activities as normal traffic. This protocol is used to send commands.

VI. Infection Mechanisms

These infection mechanisms are used to find a new machine to join the botnet. [17] Below are different mechanism used to infect victim machines.

A. *Web Download*

This command has two parameters, the file path, and the URL. The URL is used to download, and the file path is operated to collect data. The IP address is acquired through this command. [17]

B. *Mail Attachments*

This attachment is a document which is connected to an email. Usually, sends an spam email with an anonymous sender. A HTTP bot called 'Clickbot' is used to spread operating an email.[17] This bot is controlled by a bot controller.

C. *Automatically Scan*

Recruiting new hosts is important to expand a botnet. This can occur when employing vulnerability scanning. Compromised bots will be operated to find vulnerabilities in host devices. A large amount of IP addresses are being examined for vulnerabilities. [17]

VII. Security Challenges

Botnets which are exploited for cybercrime pose a significant threat to network security. Bots can inspect entire networks and spreads itself employing vulnerable passwords and machines or accessing weaknesses. [5] The attacks include keylogging, sniffing traffic, DoS attacks, extortion, spreading new malware, mass identity theft and password stealer are all examples of universal threats performed by botnets. [10] DoS attacks are disastrous for host networks because they can deplete the network bandwidth. Malicious developers assign devices to commit cybercrimes, the herders have access to thousands of machines. Another infection technique includes injecting a trojan horse etc. The malware infiltrates and spreads into the system using different methods. Like software vulnerability, distribution of emails, instant messaging, and the use of other botnets.

A software vulnerability exploits a flaw in the software running on the victim's computer. This happens remotely. The hacker who has exploited the vulnerability successfully will be able to control the new infected system. It's a dangerous threat due to it infecting any device connected to the internet. A botnet infects a new machine connected to the internet. Then inserts malware using various protocols like HTTP, P2P. The bot controller can activate the malware or malicious programme at any time. [5] The machine is then compromised; the bot herder controls the bot army using the C&C Server. [10] Botnet's compromise around fifty percent of internet traffic.

VIII. Malicious Botnet Behavior

A. *Denial-Of-Service Attack*

A DoS attack is utilized, which sends a dos attack to flood a website. Though, the majority of compromised machines are home-based. The bot herder will command bots to access either an IP address or web application at the same time. This influx of traffic overpowers the site and affects the sites' ability to function [28]. The bot herders are capable of transmitting the surge of the machines by sending a single command from an IRC Site and disrupting a server.

B. *Malicious Spam*

Using thousands of bots to send spam emails to millions of recipients. The attachments or links in these fraudulent emails are dangerous. They have the potential to be used to download malware. Email distribution includes spreading malicious codes onto networks using emails. [13]

IX. Botnet Evolution

Researching the evolution of bots creates an insight into their current abilities. The original purpose of bots was to aid the IRC. Botnets used to operate in the background but now they are commonly operated by criminals. The PrettyPark worm was created in 1999. It would connect to remote IRC server and gain access to private system information, this botnet was not as harmful as new botnets, its attacking capability was lacking. Though this benefited botnet evolution due to its ability to permit the botmaster to remotely access a large group of infected machines using the IRC. The PrettyPark technique to utilize the IRC as a extensive and discrete technique for the command and control was then implemented by the black hat society [2].

This technique has improved newer botnets Behavior and made them sophisticated and have more vicious attack methods. Modern botnets tend to have robust attack mechanisms that are adopted from the command-and-control systems. GT Bot, or Global Threat Bot, was first released in the year 2000. This was a new botnet version that could produce custom scripts in response to IRC commands. [18] This botnet had access to sockets for the UDP and TCP protocols, allowing it to launch DDoS assaults. There are hundreds of variants of this bot. [6]

The CutWail botnet released in the year 2007. This botnet operated a concealment technique, hiding its activity on the network. This technique benefited botnet evolution by aiding cybercriminals in concealing their botnet activity. This bot also created the idea of backup connections. Mirai, a notorious botnet operated in the year 2016. Its shutdown a network, affecting large corporations, such as amazon and Netflix etc. Since then, a new Mirai variant arose targeting vulnerable business machines.

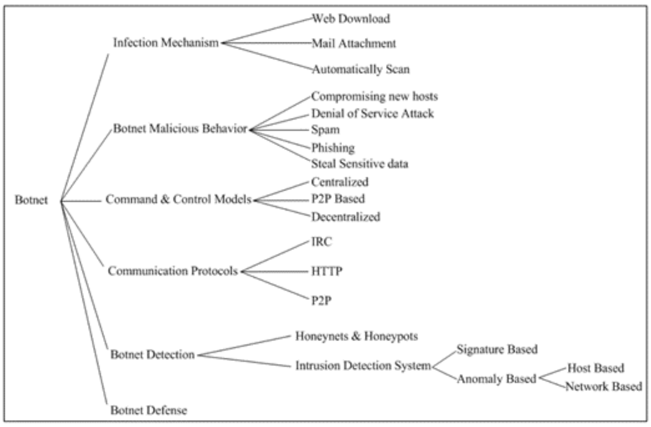

Fig 4. Botnet Taxonomy [10]

X. Botnet Taxonomy

The discussion on botnet taxonomy studies the classification of; infection mechanism, botnet Behavior, Command & control model, communication protocols and botnet detection as shown in Figure 4. Analyzing botnets and their malicious Behavior and architecture. It is needed to classify threats in more detail that are related to defence measures.[17] The goal is to determine the most efficient way to classify and treat botnets based on their strong traits.

XI. Botnet Detection

Botnets have become more advanced and more complex. The botnets have become stealthier_against intrusion detection bypassing the infection identifications. [14] The majority of detection methods rely on network traffic analysis. This is done to define the possible existence of the C&C communications with the botmaster and bots. Botnet detection is crucial in cybersecurity as it is effective against various cybercrime. Botnet detection methods can be classified intro intrusion detection techniques and honeypots detection techniques. [5] The intrusion detection split further intro more categories. [10] To evade detection, the bot controller can use proxy bots called Stepping-Stones. These proxy machines are located amongst the botmaster and C&C server (Figure. 1).In previous studies the botnets change their signatures frequently to avoid detection.

The detection of botnet is reliant on signature, Behavior, and the command-and-control structure [29]. Botnet communication can be utilized for detection, because during bot communication the data is carried between them. This communication can mix with normal traffic, making it hard to distinguish malicious traffic from normal traffic. [4]

A. *Honeynets*

Honeynets are utilized to comprehend these botnet properties. In the honeynets detection method, the honey wall is crucial for analyzing, collecting, controlling communication, and modifying. [5]

B. *Intrusion Detection System*

This detection system is used to analyse traffic flow for malicious signatures. IDS are divided into two categories: anomaly based, and signature based. The system administrator will be notified if malware activity is discovered in the system. The IDS have the potential to block the malicious traffic from a compromised system.[10] Bot Behavior system works by analyzing the Behavior of a single bot with information from another bot. [5]

C. *Anomaly-Based Detection*

This can identify unknown intrusion depending on similar Behavior of previous attacks. This is done when comparing normal traffic logs against malicious traffic. [10] The network traffic is restricted by the system administrator. In comparison to other approaches, this process is expensive. However, it is more secure than signature-based detection. [9]

D. *Signature-Based Detection*

This detection operates by searching for specific patterns, like the number of bytes in the network traffic. The detected pattern is called signatures. [10] This detection is effective in detecting existing malware signatures but not so great at detecting new malware signatures.

E. *Challenges in Detection*

The network traffic is too big to monitor, which makes detection difficult. The amount of malware on the network is quite low. Botnet Behavior is constantly changing, rendering their signatures more difficult to detect.

XII. Security challenges faced when evaluating botnet detection system

A. *Internet Heterogeniety*

Networks are different to each other and have distinctive characteristics.

B. *Multiple Administrative Domains*

Many organizations regulate the internet, each with its own set of rules and purposes.

C. *Privacy Concerns*

Network traces contain confidential data about users on the network. The data includes their communication and actions. It will be difficult to share this data with third parties.

D. *Controlled Environment*

Live honeypots provide a realistic report on traffic produced from bots. It's an artificial setting, therefore it's not the same as a real-time traffic report.

XIII. Conclusion

The amount of internet consumers is increasing massively, increasing the quantity of cyber-attacks and cybercriminals. Botnet characteristics and signatures are evolving, botnet is the largest cyber threat. The distribution of spam emails remains the most common infection technique for botnets. [15] The centralized architecture is the most common botnet, due to its easy development. The botnets are using different methods to remain undetected [13], like using camouflaging techniques. Around, half of the internet connected smartphones devices and machines are apart of a botnet causing cybercrime without even knowing. [10] Security on all devices is required to prevent a system or device from becoming a compromised host. Other botnet prevention methods include, updating your system regularly, avoid suspicious emails from anonymous sources, utilize anti-virus software, disabling unused ports.

XIV. Future Research

Botnets will recruit new kinds of connected devices in the future. For instance, the use of IoT consumer gadgets. Botnet networks will get smaller and become more complex to avoid detection and be more resistant to cybersecurity takedown operations. The proposed taxonomy includes different aspects and Behaviors of botnets [31]. This contributes to a better understanding of the threat. Future research will concentrate on analyzing characteristics from the viewpoint of network providers, as well as developing and implementing mitigating techniques.

References

[1] Rodríguez-Gómez, R., Maciá-Fernández, G., García-Teodoro, P., Steiner, M. and Balzarotti, D., 2014. Resource monitoring for the detection of parasite P2P botnets. Computer Networks, 70, pp.302-311.

[2] Citeseerx.ist.psu.edu. 2007. TREND MICRO: TAXONOMY OF BOTNET THREATS. [online] Available at: <https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.127.1845 > [Accessed 9 December 2021].

[3] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, “Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat.” International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.

[4] Ullah, I., Khan, N. and Aboalsamh, H., 2013. Survey on botnet: Its architecture, detection, prevention, and mitigation. 2013 10th IEEE INTERNATIONAL CONFERENCE ON NETWORKING, SENSING AND CONTROL (ICNSC)

[5] I. Ghafir, M. Husak and V. Prenosil, “A Survey on Intrusion Detection and Prevention Systems,” IEEE/UREL conference, Zvule, Czech Republic, pp. 10-14, 2014.

[6] Oujezsky, V., Horvath, T. and Skorpil, V., 2017. Botnet C&C Traffic and Flow Lifespans Using Survival Analysis. International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems, 6(1), p.38.

[7] García, S., Zunino, A. and Campo, M., 2013. Survey on network-based botnet detection methods. Security and Communication Networks, 7(5), pp.878-903.

[8] I. Ghafir, J. Svoboda and V. Prenosil, “Tor-based malware and Tor connection detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-6, 2014.

[9] Li, C., Jiang, W. and Zou, X., 2009. Botnet: Survey and Case Study. 2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC),

[10] Silva, S., Silva, R., Pinto, R. and Salles, R., 2013. Botnets: A survey. Computer Networks, 57(2), pp.378-403.

[11] I. Ghafir and V. Prenosil, “Advanced Persistent Threat Attack Detection: An Overview,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 4(4), pp. 50-54, 2014.

[12] Aviv, A. and Haeberlen, A., 2011. Challenges in experimenting with botnet detection systems. In: Proceedings of the 4th conference on Cyber security experimentation and tes. [online] ScholarlyCommons, p.6. Available at: <https://core.ac.uk/download/pdf/214173606.pdf> [Accessed 11 December 2021].

[13] I. Ghafir and V. Prenosil, “DNS traffic analysis for malicious domains detection,” International Conference on Signal Processing and Integrated networks. Noida, India: pp. 613 - 618, 2015.

[14] Sandip Sonawane, 0, A Survey of Botnet and Botnet Detection Methods, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 07, Issue 12 (December – 2018),

[15] Anwar, Shahid & Mohamad Zain, Jasni & Zolkipli, Mohamad & Inayat, Zakira. (2014). A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing.

[16] I. Ghafir and V. Prenosil, “Advanced Persistent Threat and Spear Phishing Emails.” International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

[17] Joshi, C., Bharti, V. and Ranjan, R., 2021. Botnet Detection Using Machine Learning Algorithms. Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences, pp.717-727.

[18] Lee, S., Abdullah, A., Jhanjhi, N. and Kok, S., 2021. Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning. PeerJ Computer Science, 7, p.e350.

[19] Hachem, N., Ben Mustapha, Y., Granadillo, G. and Debar, H., 2021. Botnets: Lifecycle and Taxonomy.

[20] Tiirmaa-Klaar, H., Gassen, J., Gerhards-Padilla, E. and Martini, P., 2013. Botnets, Cybercrime and National Security. SpringerBriefs in Cybersecurity, pp.1-40.

[21] S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and S. A. Khayam, "A Taxonomy of Botnet Behavior, Detection, and Defense," in IEEE Communications Surveys & Tutorials, vol. 16, no. 2, pp. 898-924, Second Quarter 2014, doi: 10.1109/SURV.2013.091213.00134.

[22] Bertino, E. and Islam, N., 2017. Botnets and Internet of Things Security. Computer, 50(2), pp.76-79.

[23] I. Ghafir and V. Prenosil, “Blacklist-based Malicious IP Traffic Detection,” Global Conference on Communication Technologies (GCCT). Thuckalay, India: pp. 229-233, 2015.

[24] Lashkari, A., Ghalebandi, S. and Reza Moradhaseli, M., 2011. A Wide Survey on Botnet. Communications in Computer and Information Science, pp.445-454.

[25] Waheed, S. (2012). Implementation and evaluation of a botnet analysis and detection method in a virtual environment. (Thesis). Edinburgh NapierUniversity.http://researchrepository.napier.ac.uk/id/eprint/5667

[26] Wang, P., Aslam, B. and Zou, C., 2010. Peer-to-Peer Botnets. Handbook of Information and Communication Security, pp.335-350.

[27] I. Ghafir, J. Svoboda, V. Prenosil, “A Survey on Botnet Command and Control Traffic Detection,” International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 75-80, 2015.

[28] S. Eltanani and I. Ghafir, "Aerial Wireless Networks: Proposed Solution for Coverage Optimisation," IEEE Conference on Computer Communications Workshops”, IEEE, 2021.

[29] M. Hammoudeh, I. Ghafir, A.Bounceur and T. Rawlinson, “Continuous Monitoring in Mission-Critical Applications Using the Internet of Things and Blockchain,” International Conference on Future Networks and Distributed Systems. Paris, France, 2019.

[30] I. Ghafir and V. Prenosil, “DNS query failure and algorithmically generated domain-flux detection,” International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-5, 2014.

[31] U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, “An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes,” International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.