Botnet Technology: A Persistent Threat to Digital Infrastructure

Devendra Chapagain *, Bindu Aryal, Dinesh Chhetri, Bijay Bastakoti, Pradip Bhusal

Posted Date: 9 December 2024

doi: 10.20944/preprints202412.0660.v1

Keywords: Botnet; Cybersecurity; DDoS; Detection and Mitigation; Network Security

 doi:10.20944/preprints202412.0660.v1

Article

Botnet Technology: A Persistent Threat to Digital Infrastructure

Devendra Chapagain [1,*], Bindu Aryal [1], Dinesh Chhetri [2], Bijay Bastakoti [3] and Pradip Bhusal [4]

[1] Birendra Multiple Campus
[2] Independent Researcher
[3] University of Texas at Arlington
[4] Independent
* Correspondence: devendra.chapagain@bimc.tu.edu.np

Abstract: Botnets are amongst the most prevalent modern day cyber threats spreading advanced attacks which compromise digital infrastructures jeopardizing the data integrity and confidentiality. This research paper elaborates on botnet topologies and subtle organizational structures and communication modalities, which are intrinsic to botnet surreptitious networks. By a controlled taxonomy, botnets are divided into three different categories, which are centralized, decentralized, and peer-to-peer (P2P) architectures, each with different operational paradigms and resilience profiles. This paper looks further at the communication protocols and covert mechanisms in place with botnets that cloak their presence and manage to stay hidden. Synergistically, this article also documents thorough research on all measures currently in place and designed to prevent botnet proliferation and further reduce its impact. These comprise various forms, from network monitoring and intrusion detection systems to orchestrated takedown operations that are scrutinized for efficacy and ethical repercussions.

Keywords: botnet; cybersecurity; DDoS; detection and mitigation; network security

Introduction

A botnet is a network of compromised devices, such as computers, smartphones, or IoT devices, which are controlled by a malicious actor. Botnets are networks of compromised devices, such as computers, smartphones, or IoT devices, controlled by a malicious actor [1]. These devices, known as "bots," are infected with malware that allows the attacker to remotely control them. Botnets are a serious threat to cybersecurity due to their ability to launch large-scale attacks and cause severe damage. A user's computer network may be compromised and remotely controlled by a third-party intruder without the user's knowledge [2]. This compromised computer, often referred to as a "zombie," is controlled by a hacker to perform various malicious activities on the internet, such as sending spam, launching attacks, or stealing data. Many IoT devices have been attacked in the past because they were not secure enough [3]. Some of these attacks have even put people's lives in danger. Botnet C&C servers are used by cybercriminals to control infected devices. These devices, including computers, smartphones, and IoT devices, can be used to launch attacks like spam, ransomware, DDoS attacks, and cryptojacking. Command and Control (C&C) is the critical communication channel between a botnet's operator and the infected devices (bots) [4]. It allows the attacker to issue commands to the botnet and receive information about the botnet's status.

The rapid growth of IoT devices, often manufactured with weak security practices, has made them prime targets for cyberattacks [5]. Many devices come with default, easily guessable credentials and lack essential security features. This vulnerability makes them susceptible to botnet formation, where large numbers of compromised devices are controlled remotely to launch malicious attacks.

 doi:10.20944/preprints202412.0660.v1

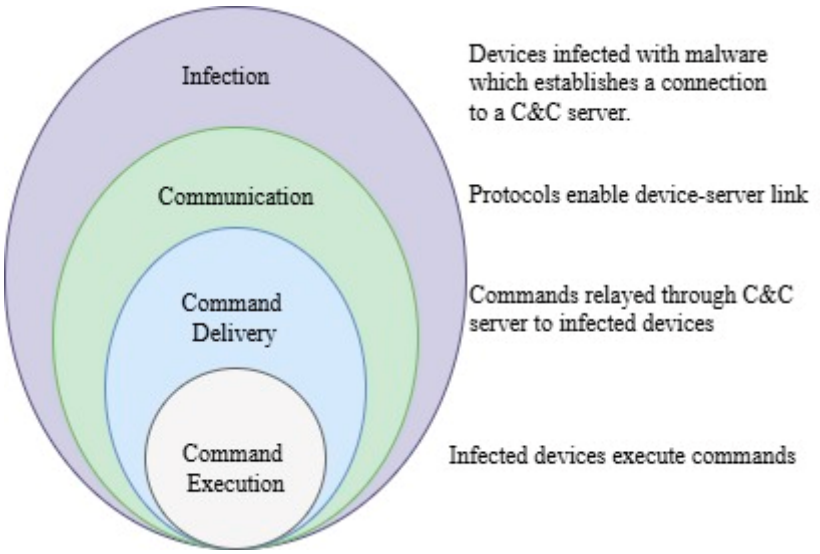

Figure 1. C&C in botnet attack.

The paper by Gaonkar et.al [6] utilized the UNSW-NB15 dataset (a comprehensive network intrusion detection dataset designed to benchmark the performance of intrusion detection systems) for creating and analyzing models before proceeding with active data collection. This dataset is commonly used for training and testing various network intrusion detection systems, including those focused on IoT botnet detection. From the sample data [6], it is observed that passive traffic monitoring is more frequently used than active monitoring. The architectures and techniques vary widely, indicating a diverse approach to botnet detection. Notably, the accuracy is predominantly 'High', suggesting effective detection methods. However, there is an inconsistency in the spelling of 'High' as 'Hign', which may need correction. The dataset provides a comprehensive view of the current landscape in botnet detection methodologies, highlighting the variety of tools and techniques employed in the field.

Mobile botnets, networks of compromised mobile devices controlled by malicious actors, pose a significant threat to cybersecurity [7]. These devices, often smartphones and tablets, are infected with malicious software that allows attackers to remotely control them. The increasing prevalence of mobile devices, coupled with their diverse operating systems and vulnerabilities, makes them attractive targets for cybercriminals. Mobile botnets can be used to launch various attacks, including distributed denial-of-service (DDoS) attacks, data theft, spam campaigns, and click fraud. To mitigate the risks associated with mobile botnets, individuals and organizations must adopt robust security practices, such as keeping software up to date, using strong passwords, and being cautious of suspicious apps and phishing attacks.

Significance of the Study

Various topologies of botnets need to be understood to devise effective strategies against the ever-evolving cyber threats managed by them. It is crucial to protect devices with strong security measures like up-to-date antivirus software, firewalls, and regular software updates to prevent them from becoming part of a botnet. Adaptation, evasion, and scalability include all various architectures like centralized, decentralized, and hybrid botnets. The paper intensively reviews such topologies with a view to extract more comprehensive knowledge about the way of functioning, communication, and evolution pattern of botnets. This knowledge is the government standard in finding the natural vulnerabilities within the various botnet structures that must be tapped to damp their effects. Besides, mitigation on cybersecurity improves such that it can protect people, organizations, and critical infrastructures from damage brought about by this class of activity that may include DDoS attacks, data breaches, and financial fraud. This is expected to contribute toward the elaboration of proactive defense mechanisms capable of neutralizing botnet threats before they reach their critical mass, thereby improving the overall resilience of cybersecurity systems. The

 doi:10.20944/preprints202412.0660.v1

resultant benefit will therefore not only aid in the operations of cybersecurity practitioners but also help guide appropriate policy-thinking and researchers in the formulation of robust, adaptive, and forward-looking cybersecurity strategies. Understanding the command-and-control structure of botnet attacks is essential for cybersecurity professionals. [8] By recognizing how attackers orchestrate their operations through C&C servers, organizations can better prepare their defenses against such threats.

Literature Review

Lack of standardization and the complexity of managing multi-vendor environments can lead to vulnerabilities and inefficiencies in network management, which could indirectly relate to network threats. [9] Shingo Yamaguchi [10] proposed Botnet Defense System (BDS). The proposed Botnet Defense System (BDS) is a multi-component approach designed to counter malicious botnets. It comprises a Monitor component to identify threats like the Mirai botnet, a Strategy Planner to devise a counterstrategy, a Launcher to deploy white-hat worms, and a C&C Server to orchestrate the white-hat botnet's actions. This strategic approach leverages the power of botnets themselves to combat malicious activities, offering a proactive defense mechanism for IoT systems.

A recent report by DataDome [11] reveals a concerning trend: 65% of businesses are still susceptible to simple bot attacks, and only a small fraction (8%) has robust security measures in place. The report highlights the alarming rise of advanced threats like account and payment fraud, often carried out by highly sophisticated fake Chrome bots that are difficult to detect.

Several methodologies have been explored in the literature to detect botnet activities. Traditional approaches often rely on signature-based detection, which is limited in its ability to identify new or evolving threats. In contrast, machine learning techniques have gained traction due to their adaptability and effectiveness in recognizing patterns in network traffic. For instance, Dollah et al. [12] utilized a machine learning approach to detect HTTP botnets, demonstrating that the k-NN algorithm outperformed others in terms of detection accuracy. However, this study did not account for the specific behaviors and scenarios of bot activities.

M. A. R. Putra et al [13] research investigates the detection of botnets by examining their communication patterns. His proposed model involves three key steps: identifying bot activity, extracting crucial information, and analyzing their communication behaviors. By understanding the connection between bot actions and their communication patterns, Yamaguchi's research aims to significantly improve the accuracy of botnet detection. Recent trends indicate a growing number of cyberattacks, fueled by the rapid proliferation of insecure IoT devices [14]. Among the most prevalent threats are botnets and distributed denial-of-service (DDoS) attacks, which have seen a significant increase in both frequency and intensity over the past decade.

Evolution of Botnets

Botnet operators are constantly evolving their techniques to improve the resilience and effectiveness of their botnets. This includes adopting more sophisticated topologies, using encryption to protect communication, and employing advanced anti-detection measures. Understanding botnet topologies is crucial for security professionals to develop effective defense strategies. By analyzing the communication patterns and infrastructure of botnets, researchers can identify vulnerabilities and develop countermeasures to disrupt their operations.

The bot, discovered in August 1988 by Jarkko "WiZ" Oikarinen from the University of Oulu, Finland, was one of the earliest examples of automated software agents [15]. At that time, most bots utilized Internet Relay Chat (IRC) as their primary control protocol [16]. IRC, initially designed for connecting to chat rooms and facilitating real-time text-based communication, was widely used during the early days of the internet. The rise of so-called “zombie networks” peaked in the mid-2000s. A central command and control (C&C) server operated remotely over a network of infected machines [17].

 doi:10.20944/preprints202412.0660.v1

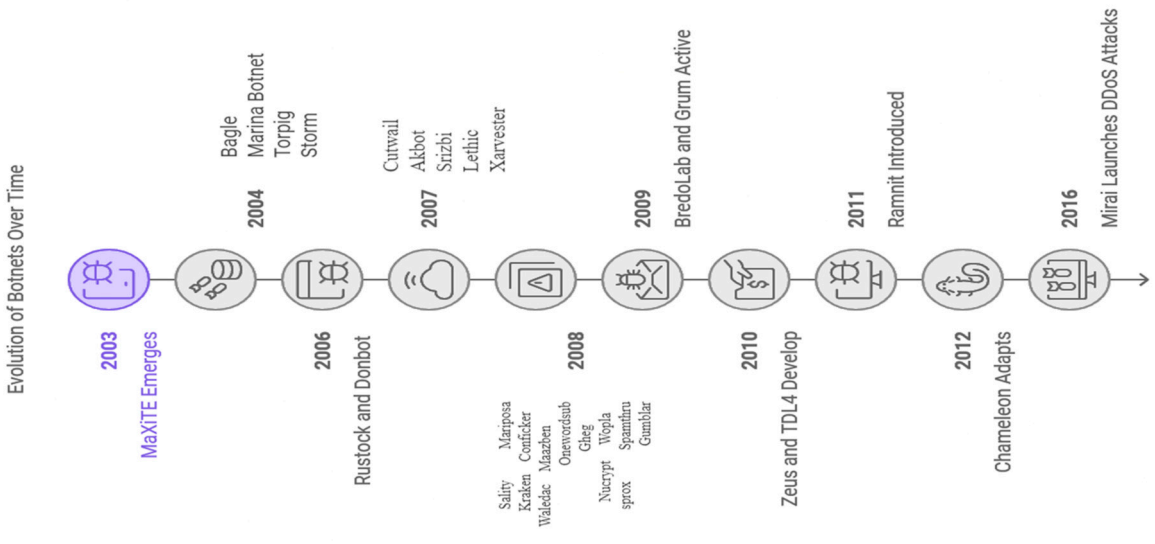

Figure 2. Evolution of Botnet.

The modern botnets have also adapted to use the vulnerabilities in the growing landscape of IoT to their advantage, as was witnessed with the Mirai botnet, which utilized poorly secured IoT devices for laying massive DDoS attacks. This reflects an older view of the race that continuously goes on between botmasters, who seek to widen their control, and cybersecurity professionals who strive to mitigate such threats. The evolution of botnets poses a significant threat to cybersecurity. As technology advances, it is crucial to stay informed about the latest trends and adopt robust security measures to protect against these malicious attacks.

According to a 2023 report by NSFOCUS [18], botnet threats significantly escalated, with over 1,400 large-scale attacks targeting critical infrastructure. Prominent botnet families like Mirai, XorDDoS, Gafgyt, and HailBot exploited vulnerable IoT devices, primarily routers, to form extensive botnets. These botnets served as the foundation for more intricate attacks, creating complex attack chains. The US and China emerged as primary targets, facing numerous UDP Flood attacks. The report also highlighted the rise of Linux/IoT-based botnets and the increased use of the Go programming language. Looking ahead to 2024, experts predict a further intensification of attacks on critical infrastructure, enhanced botnet group coordination, and more sophisticated concealment techniques.

Botnet Topologies

Star Topology: The most popular and quickly infecting type of botnet is the centralized botnet, often known as star topology [19]. A star botnet topology is a centralized botnet architecture where a single command-and-control (C&C) server coordinates the activities of all infected devices. This topology is relatively simple to manage but is also highly vulnerable to attacks. If the C&C server is compromised or taken down, the entire botnet can be disrupted.

Multi- server: A multi-server botnet topology is a type of botnet architecture that employs multiple C&C servers to coordinate the activities of infected devices. This design enhances the botnet's resilience by distributing control across multiple servers. If one server is compromised or taken down, the botnet can still function through the remaining servers. This topology can also be used to evade detection and takedown efforts, as attackers can switch between different C&C servers to avoid detection.

Hierarchical: Hierarchical botnets pose a significant threat due to their robust structure and evasive nature, making them difficult to detect and disrupt [20]. A hierarchical botnet topology is a multi-tiered structure where infected devices are organized into a hierarchical structure. This topology typically involves multiple layers of botnet nodes, with each layer controlling the layer below it. The top layer consists of a small number of highly privileged nodes, often referred to as

 doi:10.20944/preprints202412.0660.v1

"botmasters" or "herders," who control the entire botnet. These botmasters issue commands to lower-level nodes, which in turn relay these commands to the devices they control.

Peer to Peer:

Peer-to-peer (P2P) botnets are decentralized networks of infected devices that communicate directly with each other without relying on a central server. This decentralized structure makes them highly resilient to attacks and difficult to detect and disrupt [21]. Botnets can leverage P2P networks to launch large-scale attacks like DDoS attacks, data theft, spam campaigns, and cryptocurrency mining.

Table 1. Comparison of botnet topologies.

Feature	Star Topology	Multi-Server Topology	Hierarchical Topology	Peer-to-Peer Topology
Centralization	Highly Centralized	Moderately Centralized	Moderately Centralized	Decentralized
Resilience	Low	Medium	High	High
Detection Difficulty	Easy	Medium	High	High
Control	High	Medium	High	Low
Scalability	Moderate	High	High	High
Complexity	Low	Medium	High	High
Examples	Early botnets like Storm Worm	Zeus, Conficker	Mirai, Gbot	Cryptojacking botnets

The Future of Botnets

Botnets are networks of infected devices controlled by a malicious actor. They operate as distributed networks, allowing attackers to launch large-scale attacks, posing a significant threat to modern computing systems [22]. The future of botnets is likely to be characterized by increased sophistication and adaptability. Botnets could leverage AI and ML to automate attacks, target IoT devices, and utilize blockchain technology to create decentralized networks. They may also specialize in specific attacks or target multiple platforms. To mitigate these threats, organizations and individuals must adopt robust security practices and stay informed about the latest developments.

The increasing popularity and portability of mobile devices have expanded the threat landscape for botnets. This has opened up new avenues of research as botnets infiltrate mobile and cloud environments. In the future, [23] botnets may leverage machine learning to autonomously learn user behavior patterns and exploit vulnerabilities, enabling them to launch sophisticated attacks against individuals and systems.

Botnet attacks are on the rise. In the fourth quarter of 2021 alone, Spamhaus [24] identified a 23% increase in botnet command-and-control (C&C) servers. This translates to a monthly average jump from 885 to 1,090 C&C servers. A report from Sektorcert [25] published in June 2024 on Analysis of botnet attacks shows that a large number of attack attempts, around 563,000 per day, have been observed. These attacks include brute force attacks, phishing, email-borne malware, DDoS attacks, and cryptojacking.

The future of botnet research and mitigation involves a multifaceted approach. Advanced techniques like data mining and hidden Markov models can help identify and analyze botnet behavior. By understanding their internal workings, we can develop more effective countermeasures. Additionally, innovative approaches like graph theory can be applied to analyze botnet structures and vulnerabilities. However, challenges remain, particularly in addressing the trust issue when

 doi:10.20944/preprints202412.0660.v1

attempting to clean infected devices. Overcoming these challenges will be crucial in the ongoing battle against botnets [26].

Conclusion

In conclusion, botnets pose a significant threat to cybersecurity, capable of causing widespread disruption and financial loss. As technology continues to evolve, cybercriminals continually refine their tactics to exploit vulnerabilities and launch sophisticated attacks. This ongoing evolution necessitates a proactive approach to cybersecurity, requiring constant adaptation to the ever-changing threat landscape. The power and capabilities of mobile devices, tablets, and smartphones are raising new security concerns, as the amount of personal data stored on these devices and the increasing number of daily transactions performed with them make them attractive targets for attackers. To combat these threats, it is imperative to implement robust security measures, stay informed about emerging threats, and collaborate with cybersecurity experts to develop effective defense strategies. By understanding the various botnet topologies and their evolution, organizations and individuals can better protect themselves from these malicious attacks.

Conflicts of interest: The authors declare no conflict of interest.

References

1. Mims, N. A. (2025). The Botnet Problem. In Computer and Information Security Handbook (pp. 261-272). Morgan Kaufmann.
2. Iftikhar, U., Asrar, K., Waqas, M., & Ali, S. A. (2020). BOTNETs: A Network Security Issue. International Journal of Advanced Computer Science and Applications, 11(11).
3. Tushir, B., Sehgal, H., Nair, R., Dezfouli, B., & Liu, Y. (2021). The impact of dos attacks onresource-constrained iot devices: A study on the mirai attack. arXiv preprint arXiv:2104.09041.
4. Tyagi, A. K., & Aghila, G. (2011). A wide scale survey on botnet. International Journal of Computer Applications, 34(9), 9-22.
5. Dange, S., & Chatterjee, M. (2019). IoT botnet: The largest threat to the IoT network. In Data Communication and Networks: Proceedings of GUCON 2019 (pp. 137-157). Singapore: Springer Singapore.
6. Gaonkar, S., Dessai, N. F., Costa, J., Borkar, A., Aswale, S., & Shetgaonkar, P. (2020, February). A survey on botnet detection techniques. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)* (pp. 1-6). IEEE.
7. Abbas, S. G., Hashmat, F., Shah, G. A., & Zafar, K. (2021). Generic signature development for IoT Botnet families. *Forensic Science International: Digital Investigation*, *38*, 301224.
8. Yamaguchi, S. (2020). Botnet defense system: Concept, design, and basic strategy. *Information*, *11*(11), 516.
9. Gutiérrez, J. A. (1998). A connectionless approach to integrated network management. International Journal of Network Management, 8(4), 219-226.
10. Yamaguchi, S. (2021, January). A basic command and control strategy in botnet defense system. In *2021 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1-5). IEEE.
11. "Start a conversation with DataDome," Drift.click, 2024. https://datadome.drift.click/a430172e-2941-4683-bf0f-f0c3dfc2800e (accessed Oct. 29, 2024).
12. R. F. M. Dollah, M. A. Faizal, F. Arif, M. Z. Mas'ud, and L. K. Xin, "Machine learning for HTTP botnet detection using classifier algorithms". J. Telecommun. Electron. Comput. Eng., Vol. 10, No. 1–7, pp. 27–30, 2018.
13. Putra, M. A. R., Ahmad, T., & Hostiadi, D. P. (2022). Analysis of Botnet Attack Communication Pattern Behavior on Computer Networks. *International Journal of Intelligent Engineering & Systems*, *15*(4).
14. F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer and A. Ali, "Towards a universal features set for IoT botnet attacks detection", Proc. IEEE 23rd Int. Multitopic Conf. (INMIC), pp. 1-6, Nov. 2020.
15. Ade Kurniawan, Ahmad Fitriansyah, "A Literature Review of Historical and Detection Analysis of Botnets Forensics," International Journal of Computer and Communication Engineering vol. 7, no. 4, pp. 128-135, 2018.
16. The New Era of Botnets By Zheng Bu, Pedro Bueno, Rahul Kashyap, and Adam Wosotowsky McAfee Labs™
17. Zeng, J., Tang, W., Liu, C., Hu, J., & Peng, L. (2012). Efficient detect scheme of botnet command and control communication. In Information Computing and Applications: Third International Conference, ICICA 2012, Chengde, China, September 14-16, 2012. Proceedings, Part I 3 (pp. 576-581). Springer Berlin Heidelberg.
18. "Botnet Trends 2023 Review and 2024 Predictions - NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks.," NSFOCUS, Inc., a global network

 doi:10.20944/preprints202412.0660.v1

and cyber security leader, protects enterprises and carriers from advanced cyber attacks., Apr. 29, 2024. https://nsfocusglobal.com/company-overview/resources/botnet-trends-2023-review-and-2024-predictions

19. Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., & Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. Sensors, 24(11), 3571.
20. Malik, R., & Alankar, B. (2019). Botnet and botnet detection techniques. International Journal of Computer Applications, 178(17), 8-11.
21. Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B. B., & Dagon, D. (2007). Peer-to-Peer Botnets: Overview and Case Study. *HotBots*, *7*(2007).
22. Karim, A., Salleh, R. B., Shiraz, M., Shah, S. A. A., Awan, I., & Anuar, N. B. (2014). Botnet detection techniques: review, future trends, and issues. Journal of Zhejiang University SCIENCE C, 15, 943-983.
23. Ogu, E. C., Ojesanmi, O. A., Awodele, O., & Kuyoro, 'S. (2019). A Botnets Circumspection: The Current Threat Landscape, and What We Know So Far. Information, 10(11), 337.
24. Botnet C&C | Botnet Threat Update Q4 2021 | Quarterly Report. (2021). The Spamhaus Project. https://www.spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-q4-2021/
25. https://sektorcert.dk/wp-content/uploads/2024/06/Botnet-EN-TLP_CLEAR-202406.pdf
26. Zhang, L., Yu, S., Wu, D., & Watters, P. (2011, November). A survey on latest botnet attack and defense. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 53-60). IEEE.