International Journal of LNCT
ISSN: (Online):2456-9895 Volume-7 Issue-31 August -2023

A Review on IOT Botnet Detection Techniques

Harshita Patel
Btech Scholar
TIT & Science, Bhopal.

Laxmi
Btech Scholar
TIT & Science, Bhopal.

Mayank Raj
Btech Scholar
TIT & Science, Bhopal.

Ravi Ranjan
Btech Scholar
TIT & Science, Bhopal.

Abstract: IoT devices are vulnerable to a wide range of security risks and attacks, including assaults from botnets, due to basic security weaknesses. Because of this, developers of botnets continue to exploit the security flaws present in IoT devices to take control of several host devices on networks and execute cyberattacks against their intended target systems. Finding IoT bot vulnerabilities is challenging since methods to get around detection and security measures are constantly being developed. In this paper, various machine-learning-based botnet detection strategies will be examined together with the conceptual frameworks of IoT botnet assaults. The Bot-IoT Dataset, a current realistic IoT dataset that includes state-of-the-art IoT botnet attack scenarios, is used in this study to assess and compare several botnet detection approaches.

I. INTRODUCTION

The Internet of Things (IoT) has recently gained prominence in both academics and business. The Internet of Things (IoT) has become a crucial technology that will serve as the foundation for a variety of advancements in smart environments, including smart homes, smart healthcare, and smart everything. IoT is being adopted in a number of applications to improve services as a result of the exponential rise of IoT devices and technological advancements. Electronics, software, sensors, actuators, and connection between IoT devices enable them to connect, communicate, and share data. The affordability of IoT devices is boosting their growth and popularity[1].

With the Internet of Things' enormous potential comes enormous concern, particularly in terms of cybersecurity. The connected devices are clearly distinct from computers, which contributes to the completely distinct security landscape of the Internet of Things. These gadgets often have a limited range of specific capabilities and are quite simple. Accurately identifying and detecting botnets, specifically unidentified botnets in the initial infection, are the most demanding challenges in both academic and industrial studies given the security issues caused by the ongoing development of botnets. First off, the C&C mechanism of botnets exhibits a variety of cognitive traits. Botnets propagate by making use of zero-day weaknesses, peer-to-peer connections, phishing, bitcoin networks, and lightning networks. Additionally, botnets propagate very quickly, have much more infection pathways, are more covert, have higher technical substance, and have more destructive capability than typical network security concerns. Finally, as botnets are typically in a passive mode, they frequently lack traditional attack features and merely sustain the connection status via C&C channels[3].

In this paper, we will describe the operation of the IoT botnet and the key detection techniques that have been applied to identify IoT botnet attacks. And we'll emphasise the difficulties for the upcoming projects.

IoT Botnet Life Cycle:

IoT botnets operate in at least three key stages[4,5], which are detailed below:

Phase 1: Scanning Phase: A bot employs scanning and reconnaissance to find a susceptible device. The botmaster searches for IoT devices that are weak. Once it does, it begins to attack it by brute force or by taking advantage of a weakness. Once the compromised gadget has been taken advantage of, it transforms into a bot and begins interacting with the botmaster. For instance, the Mirai virus transmit fingerprint packets to search for pseudorandom IPv4 addresses in order to find Internet of Things (IoT) devices that may be accessed via Telnet service on port 23 or port 2323 [6]. The bot hacks new victims by abusing weak credentials with brute force attacks or by taking advantage of widely known IoT device vulnerabilities.

Phase 2: Propagation Phase: Based on the architecture of the vulnerable device, an appropriate variation of the bot is installed and run. Often, the bot terminates the process linked to the relevant service in order to destroy any other previous malware and lock ports to itself in order to avoid targeting devices affected by any other prospective malware and take full control. To swiftly grow the IoT botnet, the malicious code propagates and recruits new bots [6]. The bots are still awaiting instructions from the botmaster at this time.

Phase 3: Attack Phase: Harmful actions including spam, cryptocurrency mining, and DDoS are carried out. By delivering instructions to all of the distributed bots via the command and control server, the attacker starts the attack. As a result, the bots launch the assault after obtaining the same instructions.

IoT Botnet Architecture:

Centralized botnets: Reduced latency is achieved by the botmaster managing and monitoring all bots from a single central server; in other words, all bots are instructed by and report back to one server. In this design, the botmaster may have access to one or more central servers. The server makes use of the HTTP and IRC protocols. One drawback of the botmaster server might be that it is a single point of potential total failure[7]. The Mirai family of centralised IoT botnets is one of the most well-known.

Decentralized botnets: Peer-to-peer (P2P) botnets are another name for them. Each bot is connected to at least one other bot, and each bot functions as both a client and a server. The orders won't reach every bot until every bot is connected to every other bot. Because of the varied peer communication in this architecture, it is challenging for bots to coordinate, but at the same time, it is more complex and harder to detect. Peer-to-peer networking is the communication protocol used by this kind of IoT botnet. Hajime is one of the most well-known decentralised (P2P) IoT botnets[8,9].

Hybrid botnets: A hybrid botnet combines the previous two types of architecture (centralised and decentralised) since it consists of two different types of bots, some of which may

work as servers and clients as well as clients only. High message delay is present.

II. TECHNIQUES FOR DETECTING BOTNET

To the Bot-IoT subdataset with all 46 characteristics, Koroniotis et al. utilised three machine-learning techniques: Support Vector Machine (SVM), Recurrent Neural Network (RNN), and Long-Short Term Memory Recurrent Neural Network (LSTM-RNN)[11]. The experiment's findings demonstrated that the SVM classifier had the best accuracy and recall rates but required the most time to train when all the characteristics were included. This classifier acquired the best accuracy and the lowest relative fall-out rates using only the 10 highlighted characteristics. In other words, the SVM outperformed the other two approaches in terms of results.

A hybrid intrusion detection system (HIDS) was implemented in the study reported in [12] with the goal of increasing the precision with which IoT threats were discovered. This system combines a behavioural IDS for detecting zero-day attacks with a signature-based IDS for detecting well-known assaults. With only 13 of the original 46 features from the Bot-IoT datasets used when performing binary classification, the classification results from both systems were combined using the boosting method, with the behavioural part consisting of a One-Class SVM and the Signature-based part consisting of a C5 decision tree. The proposed system's detection accuracy was compared to the detection accuracy of various algorithms, including C4.5, Naive Bayes (NB), Random Forest (RF), multi-layer perceptron networks, Support Vector Machine (SVM), Classification And Regression Tree (CART), and K-Nearest Neighbor (KNN) algorithms. Their findings revealed that the suggested system had the best accuracy rate, with the Random Forest algorithm coming in at roughly 92.67% behind it.

Bidirectional long short term memory recurrent neural network (BLSTM-RNN) for botnet detection was introduced by the authors of [13]. A unidirectional LSTM-RNN was put up against the suggested solution in comparison. This was done to determine whether the latter approach could match the increased accuracy and loss metrics obtained on the collected dataset. The two models equally achieved excellent levels of accuracy and minimum loss metrics for the various Mirai attack pathways.

In order to improve the detection of IoT botnet malware, researchers in [16] suggested a method for creating a PSI-graph to reflect the relationships among PSI. This method was extremely helpful for static analysis details. Based on a convolutional neural network (CNN), the visual convolution neural network classifier was also used to detect IoT malware and was successful in doing so without using the pre-selected characteristics. In their paper, they proposed a unique method for Linux IoT botnet detection based on the combination of a PSI graph and a CNN classifier. The test's results showed that the PSI graph CNN classifier has a 94% F-measure and a 92% accuracy.

In [18], artificial neural networks (ANN) were used to recognise DDoS assaults. As previously mentioned, the Bot-IoT dataset is unbalanced, thus the Synthetic Minority Over-sampling Technique (SMOTE) was employed to raise the amount of normal samples until they were the same size as the DDoS records. The suggested system, which was trained using 66% of the dataset and evaluated using the remaining 34%, is for binary classification. Out of the 46 features that were originally included, only 41 were utilised. The testing findings demonstrated that the SMOTE approach enabled 100% detection accuracy for DDoS attacks.

III. SUMMARY

Upon closer inspection of the research included in this evaluation, the following patterns emerge:

The majority of IoT-Botnet detection tools choose a behavioural strategy that is mostly based on machine learning, with some cutting-edge research using deep learning. Modern solutions seldom employ hybrid or signature-based strategies. The majority of cutting-edge solutions use the Bot-IoT dataset, however very few research have addressed its unbalanced nature. Observed research mostly ignored assault types that were underrepresented. Most research choose to develop their models using only one family of classification algorithms, with the accuracy rate being the primary performance metric of their chosen classification models. Few research provided sufficient details on their feature selection methods, or they mainly used one feature selection methodology in their models.

Recommendation: Lack of a systematic method for dealing with the imbalance in the Bot-IoT dataset suggests an erroneous perception of accuracy detection. Combining several machine learning classification techniques may result in more accurate detection models that are also more sensitive. The Bot-IoT dataset needs more research on feature selection because the initial collection of features is huge and various feature selection strategies might offer various views to the classification process.

IV. CONCLUSION

This review provides information on cutting-edge approaches to IoT botnet detection that make use of the Bot-IoT dataset, with a focus on botnet assaults. A deeper analysis of the illustrated solutions was conducted, highlighting the key tendencies as well as the variety of problems that these solutions displayed. Finally, this study makes a series of recommendations for future IoT botnet detection technologies that would assist address the problems with the present ones.

REFERENCES

1. Singh, M.; Singh, M.; Kaur, S. Issues and challenges in DNS based botnet detection: A survey. Comput. Secur. **2019**, 86, 28–52.
2. M. Al-Kasassbeh, M. Almseidin, K. Alrfou and S. Kovacs, "Detection of IoT-botnet attacks using fuzzy rule interpolation," Journal of Intelligent & Fuzzy Systems, pp. 1-11.
3. A. Karim, R. B. Salleh, M. Shiraz et al., "Botnet detection techniques: review, future trends, and issues," *Journal of Zhejiang University Science*, vol. 15, no. 11, pp. 943–983, 2014.
4. Beltrán-García, P.; Aguirre-Anaya, E.; Escamilla-Ambrosio, P.J.; Acosta-Bermejo, R. IoT botnets. In Communications in Computer and Information Science; Springer Science and Business Media LLC.: Berlin, Germany, 2019; pp. 247–257.
5. Alzahrani, H.; Abulkhair, M.; Alkayal, E. A multi-class neural network model for rapid detection of IoT botnet attacks. Int. J. Adv. Comput. Sci. Appl. **2020**, 11.
6. Manos, A.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z. Un-derstanding the mirai botnet. In Proceedings of the 26th {USENIX} security symposium ({USENIX}

Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp.1093–1110.
7. Dange, S.; Chatterjee, M. IoT Botnet: The Largest Threat to the IoT Network. In Advances in Intelligent Systems and Computing; Springer: Singapore, 2019; pp. 137–157.
8. Beltrán-García, P.; Aguirre-Anaya, E.; Escamilla-Ambrosio, P.J.; Acosta-Bermejo, R. IoT botnets. In Communications in Computer and Information Science; Springer Science and Business Media LLC.: Berlin, Germany, 2019; pp. 247–257.
9. Bertino, E.; Islam, N. Botnets and internet of things security. Computer **2017**, 50, 76–79.
10. Edwards, S.; Profetis, I. Hajime: Analysis of a decentralized internet worm for IoT devices. Rapidity Netw. **2016**, 16, 1–18.
11. N. Koroniotis, N. Moustafa, E. Sitnikova and B. Turnbull, "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset," *Future*
12. K. Ansam, G. Iqbal, V. Peter, K. Joarder and A. Ammar, "A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks," Electronics, vol. 8, no. 11, p. 1210, 2019.
13. McDermott, C.D.; Majdani, F.; Petrovski, A.V. Botnet detection in the internet of things using deep learning approaches. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8.
14. Vishwakarma, R.; Jain, A.K. A Honeypot with machine learning based detection framework for defending iot based botnet DDoS attacks. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1019–1024.
15. Tzagkarakis, C.; Petroulakis, N.; Ioannidis, S. Botnet attack detection at the IoT edge based on sparse representation. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019; pp. 1–6.
16. Nguyen, H.-T.; Ngo, Q.-D.; Le, V.-H. IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier. In Proceedings of the 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 28–30 September 2018; pp. 118–122.
17. Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-baiot—network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Comput. **2018**, 17, 12–22
18. D. A. D. B. o. S. A. w. S. f. I. Environment, "Soe, Yan Naung; Santosa, Paulus Insap; Hartanto, Rudy;," 2019 Fourth International Conference on Informatics and Computing (ICIC), pp. 1-5, 2019.
19. N. Koroniotis, N. Moustafa and E. Sitnikova, "A New Network Forensic Framework based on Deep Learning for Internet of Things Networks: A Particle Deep Framework," Future Generation Computer Systems, 2020.
20. N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," 2015 military communications and information systems conference (MilCIS), pp. 1-6, 2015.