RESEARCH ARTICLE OPEN ACCESS

Finding Malware in Internet Traffic by Bot and Providing Recommendations

Azhar Ushmani

ABSTRACT

The increasing security threats on the organizations' network require sound strategies to handle and leave the organizations stable when delivering services to their customers. While companies have deployed security strategies, gaps must be addressed to ensure they deliver sustainable services in their competitive environment. This paper performs a systematic literature review and recommends a hybrid solution encompassing the current promising bot approaches leveraging Artificial intelligence. The combination of the security features of the approach will lead to the development of an effective solution that helps organizations address the security challenges affecting them. They will detect and deter attacks as they build on their network, leaving a stable operational zone to help deliver their strategies.

Keywords: Deep Learning, Artificial Intelligence, Bot, Machine Learning.

I. INTRODUCTION

Malware remains challenging to most organizations despite increased efforts to curb it and maintain delivery strategies in the competitive business environment. Organizations face various challenges when delivering to their markets due to the effect of malware. These challenges arise since malware is programmed to collect various data or destructive activities when it attaches to the organization's network. When dealing with the current attackers, the challenge is that they are more sophisticated and use techniques that compromise the organizations' networks. Most organizations have not managed to keep up with the pace at the attackers are evolving, leading to continued compromises and threats in their networks. With technological advances, companies must move to Artificial Intelligence (AI) powered measures to drive their security strategies across their network. This need drives the development of this paper to check solutions and recommend developing a solution that helps organizations maintain stability in their competitive business environment. The paper considers the recent literature to identify the procedures and progress identified and serves as the basis for recommending the solution to apply to detect malware in the organization. Given the fast evolution of malware and attackers and the inability of conventional strategies to handle the threats facing organizations, deploying bots (robots) will support the detection based on certain operational patterns learned through machine learning.

II. THEORY INTERNET TRAFFIC

Internet traffic refers to the amount of data transmitted between computers or devices over the internet. This data can take many forms, including text, images, videos, and other types of digital content. Internet traffic can be measured in various ways, including the number of bytes or packets of data transmitted, the number of connections between devices, and the time it takes to transmit data from one device to another (Ghaffar et al., 2021). Internet traffic is generated by online activities, including browsing the web, downloading and uploading files, streaming video and audio content, sending and receiving emails, using social media platforms, and playing online games. As more and more people connect to the internet and use it for various activities, internet traffic continues to grow and expand.

III. MALWARE

Malware is a collective term for malicious software, which refers to programs installed or transferred to cause destructive actions where they land (Pachhala et al., 2021). The primary effects are compromising the operations by stealing or interfering with the data.

Bots

Nguyen and La (2019) define robots as programs that can learn or be programmed to behave in a specific way or perform a specific action when a trigger event or behavior occurs. Artificial intelligence has led to the rise of bots that allow organizations to perform automated functions and to achieve certain goals when organizations are delivering to the competitive business environment.

Contribution to the Current Literature

This paper will support the current organizations by providing additional insights based on the current literature to help the organizations deliver effectively to the clients who expect service availability at all times. The insights and recommendations from this paper will help organizations be more prepared to handle threats in the competitive business environment. The current world contains many technological developments that companies should consider when deploying solutions they can rely on to support the stability of their businesses. As a result, future malware detection and elimination strategies will be effective since they will leverage the capabilities of robots to support the automatic detection of malware based on machine learning and command initiation strategies.

IV. EMPIRICAL STUDIES

Various authors attempted to address the topic in several ways. For instance, Mijwil et al. (2022) highlight the impact of COVID-19 on the norms of operations among companies. In their paper, Mijwil et al. (2022) note a shift towards the virtual environment to operate when delivering the organizations' mission. In virtual or online environments, attackers and attacks increase with the sophistication of attackers who leverage any available means to attack organizations. These attackers also keep learning the strategies companies deploy to protect themselves and determine how to breach and compromise them. In their paper, Mijwil et al. (2022) surveyed the existing cybersecurity measures given the increased attack surfaces in organizations. The key attacks were hacking and data theft that leveraged presence on computer systems. It took time before the organizations realized the threats affected their operations in the competitive business environment. This study concludes by identifying machine learning ad deep learning as effective strategies to deter unauthorized entry into the organizations' systems (Mijwil et al., 2022).

Aljabri et al. (2021) conducted a similar study to identify how corporations can address the increasing cybersecurity threats and maintain stability when driving their operations. The goal was to address the increasing risks of the internet with the increased usage among many people whom attackers target as the channel to attack the corporate network and maintain effective delivery to the customers (Aljabri et al., 2021). According to Aljabri et al. (2021), studying network detection was the solution to address the network challenges. In this attempt, Aljabri et al. (2021) note the essence of Machine Learning (ML) and Deep learning (DL) models to develop network detection solutions to detect network attacks. Aljabri et al.'s (2021) solution leveraged an intelligent system using training datasets. These datasets contained the information to help the intelligent system to detect network attacks. The system also had metrics to define when the intelligent system can successfully detect a threat and classify it as a threat.

The advances to Industry 4.0 have had positive and negative effects on organizations. This development has also led to the evolution of threats as cyberspace contains organizations' data, and many operations happen, making it a source of threats to the operational environment (Abdullahi et al., 2021). DL and ML remain dominant in the prevention of cyberattacks affecting organizations. In this case, organizations have shifted towards smart intrusion detection systems that use intelligent architectural networks supported by AI to deliver security solutions. In this case, Abdullahi et al. (2021) note the integration of support vector machines (SVM) and random forest to increase accuracy in detection and learning and maintain memory efficiency.

Similarly, Wazzan et al. (2021) surveyed botnet detection approaches that will provide sustainable solutions to organizations. In their study, Wazzan et al. (2021) focus on botnet formation, the malicious activities involving botnets, and the existing methods. Wazzan et al. (2021) found that a communication process supports botnet operations in the scanning, propagation, and attack phases.

V. RESULTS AND DISCUSSION

Several research findings will enhance organizations' cybersecurity posture and make them more effective in their delivery to the competitive business environment. Firstly, organizations have integrated most of the methods considered secure. However, there are still attacks on their networks. The rise of AI has served organizations since it has provided a direction to follow toward automating their security strategies. However, corporations are yet to achieve their full potential when choosing the security options to support their delivery. The gap in implementing the strategies implies that companies continue facing attacks besides their attempts to deploy security measures to protect their network from attacks in their operational environment.

VI. LIMITATIONS

There are several limitations to achieving full coverage of the concepts that will help organizations utilize bots in securing their networks. Firstly, there are time constraints to research. Therefore, the findings will still leave room to be enhanced with time.

VII. RECOMMENDATIONS

Organizations can use AI to enhance attack detection using bots in several ways. Firstly, all cybersecurity strategies should be directed at using AI to automate the delivery of reliable solutions to protect organizations (Wazzan et al., 2021). They should focus on automating and integrating AI into their security strategies to make them effective and lead to productivity in their operational environment. Secondly, companies require a hybrid approach to make a botnet detect network issues when delivering to a competitive business environment. This hybrid approach should entail machine learning-based detection, where the bot learns from training data and then recognizes malware based on what it has learned. It should also use heuristic-based detection that leverages a ruleset and identifies patterns that relate to known malware. Behavioral-based detection should also be a feature of the bot to know the normal traffic behavior and tell when there is an abnormality. Besides, the bot should also have a signature-based detection capability that helps it match the malware with known signatures.

CONCLUSION

The challenges in the organizations' networks require automated and effective solutions to address the organizations' needs and leave them competitive in the business environment.. the current attacks are beyond human monitoring since they are automated. Organizations must stick to using bots to drive their attack detection.

Notes

1. Developing the bot with all these capabilities needs a programming investment that many organizations could find a huge investment.
2. Developing a bot with these capabilities will address the organization's security challenges. However, attackers could still compromise these measures through a bug in programs.
3. No organization is immune to insider threats. Attacks could still occur after developing an effective bot.

REFERENCES

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198.

Aljabri, M., Aljameel, S. S., Mohammad, R. M. A., Almotiri, S. H., Mirza, S., Anis, F. M., ... & Altamimi, H. S. (2021). Intelligent techniques for detecting network attacks: review and research directions. Sensors, 21(21), 7070.

Ghaffar, Z., Alshahrani, A., Fayaz, M., Alghamdi, A. M., & Gwak, J. (2021). A topical review on machine learning, software-defined networking, internet of things applications: Research limitations and challenges. Electronics, 10(8), 880.

Mijwil, M., Salem, I. E., & Ismaeel, M. M. (2023). The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review. Iraqi Journal For Computer Science and Mathematics, 4(1), 87-101.

Pachhala, N., Jothilakshmi, S., & Battula, B. P. (2021, October). A comprehensive survey on identification of malware types and malware classification using Machine Learning Techniques. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1207-1214). IEEE.

Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of Things botnet detection approaches: Analysis and recommendations for future research. Applied Sciences, 11(12), 5713.