

Multi Agent Anti-Malware Model, a Paradigm Shift from Mere Detection to Prevention of Cyber Threats

IBENEME-SABINUS, IFEOMA LIVINA¹, AGBAKWURU ONYEKACHI ALPHONSUS²,
ELEBERI LETICIA EBELE³

¹*Department of Cybersecurity, Federal University of Technology Owerri, Imo State Nigeria.*

²*Department of Computer Science, Imo State University Owerri, Imo State Nigeria.*

³*Department of Computer Science, Imo State University Owerri, Imo State Nigeria*

Abstract- *The security of information and data over the internet is one of the top challenges facing most business organization's today as all businesses rely on internet services for their day-to-day operations. malware is one of the topmost challenging threats as systems are being locked up, business disrupted and even closed down as a result of this deadly threat. This research work deployed the activities of Mobile Agents. The agents were trained using Random Forest, Support Vector Machine and Decision Tree Machine Learning Algorithms to develop an Anti-Malware Model. In this research paper authentication scheme, the agents monitor all downloads including users' behaviour, scan all entries into the system, check for attachments in all external files and emails, eject external device, block all advertisements and flag up links and websites that are not registered into the Threat Intelligent Database (TID) as suspicious activities. With this the probability of success for all attempts to sneak into the system reaches near to zero. This practice will also solve the problem of False Positive Detection Rate (FPDR) during data training process as this model will serve as a mitigation apparatus to all kinds of malware activities as information are stored in the systems' Threats Intelligent Database (TID) for references and thereby cushion the effects and ugly activities of malware to our promising organizations.*

Keywords: *Mobile Agents, Anti-Malware, Machine Learning Algorithms, Threats Intelligent Database.*

I. INTRODUCTION

Malware posing an extraordinary and growing threat across various cyber domains, has challenged the effectiveness of traditional cybersecurity methods. As a set of malicious programming codes or scripts designed to compromise targeted computer systems, programs, mobile and web applications, using various forms including computer viruses, worms, ransomware, rootkits, trojans, dialers, adware, spyware, and keyloggers [1]. Its growing armed-race between attackers and defenders makes the threat ecosystems highly volatile, dynamic, stochastic, and unpredictable [2]. The threats have led to substantial

financial losses, reputational damage, and operational disruptions [3]. This is to say, the landscape of cybersecurity should as a matter of urgency be undergoing dramatic transformation with the integration of advanced techniques. Based on the intention to cushion the effect of malware threats, a real-time detecting mechanism is preferable [4]. As its prevention and mitigation in businesses have become so worrisome as most researcher have delved into its detection to attest and confirm its entrance into computer systems. This research paper tends to develop a new Anti- Malware preventive model by stopping its entrance starting from the first principle. This model will go a long way in isolating and neutralizing all suspected attachments, files, mails, popup advertisement and reject external devices by the installation of Mobile Agents. Due to the capacity of these mobile agents to operate independently and autonomously, it will be deployed and trained using some Machine Learning algorithms such as Decision Tree (DT), Support Vector Machine (SVM) and Random Forest (RF), instead of training using some dataset which may result to a False Positive Detection Rate (FPDR) due to compromised and incomplete dataset [5]. Adoption of these mobile agents will redirect data training operations and prove FPDR abortive as the model shows that mobile agents will operate as required.

II. ALGORITHMS

The system is implemented in Python 3x using Streamlit for the web interface. Different machine learning algorithms will be deployed and used for the training of the mobile agents for this practice; the algorithms include Decision Tree (DT), Random Forest (RF) and Support Vector Machine (SVM). DT assists in the classification and regression of task, RF maintains high accuracy and robustness in handling complex data, dimensional data, large number of data, missing values in the data and provide feature

importance scores which helps to interpret results. SVM classifies task such as images, text and bioinformatics classification; it can be used to predict continuous outcomes and detect anomaly in the training process.

III. ANALYSIS OF THE EXISTING SYSTEM

Malware is a kind of attack that is designed to harm or exploit, encrypts a victim's system or data, they enter into organization's systems through different means such as when user visits compromised website

to download files with attachments, open a compromised mail, clicking on untrusted links and by exploiting vulnerabilities in organization system. The perpetrators sneak into organization system to cause harm and exploit the system or in most cases demand for a ransom payment before decrypting the system, and payments are usually made in cryptocurrencies to avoid traceability [6]. Majority of small and medium scale businesses are being hit by this type of attack and huge sum paid as well as disrupting business activities and financial losses.

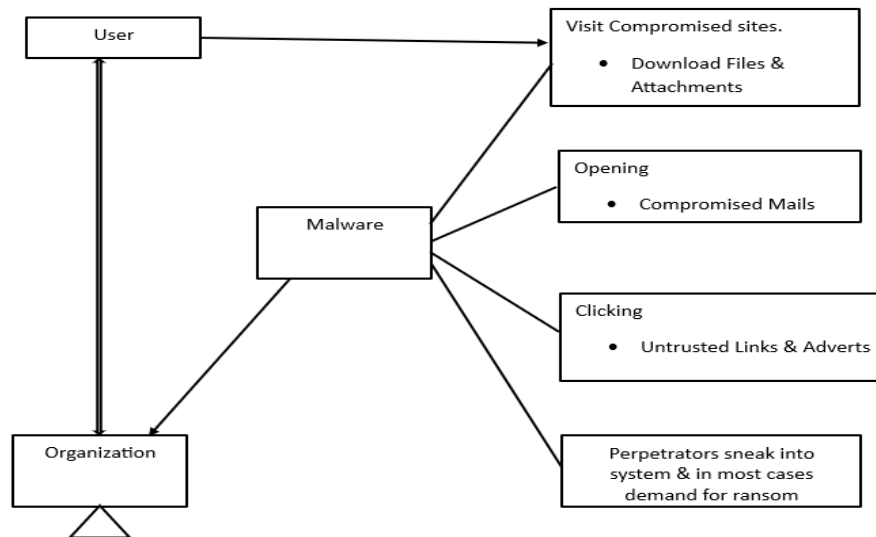


Figure 1: Data Flow Diagram (DFD) of the Existing System

Figure 1 above illustrates how the malware penetrates and affects organizational system. Here, the user opens email, download files, that carries attachments without knowing that its content might be malicious; clicks on pop-up menu with adverts, and equally clicks on malicious links which can easily redirect the user to a compromised website. These processes and activities in an organization can affect system.

IV. WEAKNESS OF THE EXISTING SYSTEM

Traditionally, organizations use firewalls, other preventive measures which the perpetrators work tirelessly to bypass detection and at the same time achieve their ugly intention. Affected systems are immediately isolated, securing backups, investigating the source of the attack, and reporting

the attack to law enforcement and paying the ransom (if feasible) are also considered, along with measures to prevent future attacks.

V. ANALYSIS OF A STRATEGIC ANTI-MALWARE MODEL

The proposed system will deploy the activities of mobile agents to create an anti-malware application that identifies attachments from emails, downloads, block advertisements raise alarm of links and website that are not classified as trusted link in the Threat Intelligent Database (TID). The mobile agents transport its state from one environment to another while keeping the data intact. It can then "pick up where it left off" and performs perfectly and appropriately in the new environment (Figure 2).

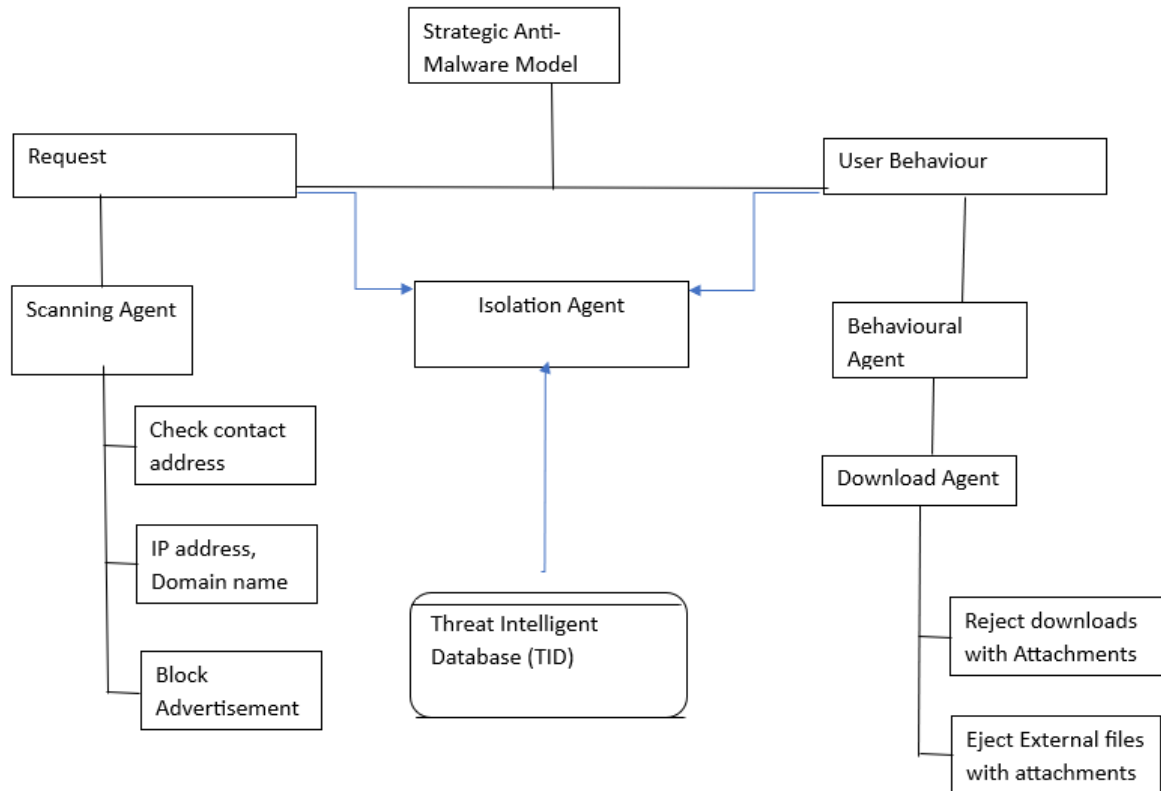


Figure 2: Anti-Malware Model

Multi-Agent Malware Detection Simulation

Safe, simulated multi-agent system to demonstrate detection, isolation, threat intel flows, and a simple dashboard.

Run a Simulation (Single Event)

Input / Event

Sender email

badguy@phishy.com

Agent settings

Blocked file extensions (File Agent)

exe x bat x vbs x

Figure 3: Anti-Malware Simulation Environment

Figure 3 illustrates simulation environment of multi-agent detection activities. The simulation clearly demonstrated how scanning was carried out as different requests were made into the system and practically showed how advertisements were blocked, system ejecting external devices and downloads from third party websites with attachments were rejected.

Run a Simulation (Single Event)

Input / Event

Sender email

badguy@phishy.com

Email contains advertisement keywords?

Downloaded filename

invoice.pdf

USB device inserted recently?

Download URL

https://downloads.thirdparty.net/tool.exe

User behaviour score (1 = normal, 0 = suspicious)

0.50

Figure 4: Suspicious Flags

Figure 4 typifies the operation whereby the model rates activities of all downloaded files, flags and notifies the system of any attachments from compromised websites. The rating is shown to read 1 = Normal and 0 = Suspicious. The Normal indicates that downloaded file is free from attachments and Suspicious reads that user might have visited a compromised websites and downloads full of attachments as clearly shown in figure 4 above.

VI. CONCLUSION

Most organizations sensitive information are facing a lot of cyber threats in our dear global world today, some are even scared of storing them in their organization's server for proper record keeping, documentation and easy accessibility. Most security concern centers on privacy, integrity and validity of information, therefore has call for more secured techniques for anti-malware software in combination with other researched work to completely put a stop to the activities of malware threat in our generation as it hinders and cripples most business infrastructures and activities and at the same time drive investors and collaborative efforts in the world

at large. In this research paper authentication scheme, the agents monitor all downloads including users' behaviour, scan all entries into the system, check for attachments in all external files and emails, eject external device, block all advertisements and flag up Links and websites that are not registered into the Threat Intelligent Database (TID) as suspicious activities. With this the probability of success for all attempts to sneak into the system reaches near to zero. Hence, looking at the security model used to detect, prevent and mitigate malware threats in this paper, one can easily say that there is a very less probability of bypassing the multi-agent's system. With the above security measures put in place, organization's sensitive information can be guaranteed and will go a long way to encourage business enterprise and investment into our business world.

REFERENCES

- [1] Zahra J, Khushboo M, Mohit K, and Binay K (2024) Malware Detection Using Artificial Intelligence: Techniques, Research Issues and Future Directions. International Journal of

Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-14 Issue-1,
DOI:10.35940/ijeat.A4531.14011024 Journal
Website: www.ijeat.org. October 2024. Retrieval
Number: 100.1/ijeat.A453114011024.

- [2] Azaabi C, Alex, and Benjamin A (2024) An Evaluation of Current Malware Trends and Defense Techniques: A Scoping Review with Empirical Case Studies. *Journal of Advances in Information Technology*, Vol. 15, No. 5, 2024.doi: 10.12720/jait.15.5.649-671.
- [3] Ayodeji S, Gupta, G. P., and Kumar, S. (2024). Android malware detection and identification frameworks by leveraging machine and deep learning techniques: A comprehensive review. *Telematics and Informatics Reports*, 12, 100130.
- [4] Elvis N, Ololade R and Chukwujekwu D (2025) Machine learning techniques for real-time malware classification and threat detection in distributed systems. *World Journal of Advanced Research and Reviews*,26(03), 2378-2398.<https://doi.org/10.30574/wjarr.2025.26.3.2433>.
- [5] Sarah B, Shancang L and Lida X (2023) Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security. *Electronics* 2023, 12, 3927. <https://doi.org/10.3390/electronics12183927>.
<https://www.mdpi.com/journal/electronics>.
- [6] Olivia O (2022) Ransomware Attacks in Nigeria: Case Studies and Mitigation Strategies, all content following this page was uploaded on 03 February 2025. The user has requested enhancement of the downloaded file. <https://www.researchgate.net/publication/388634112>.