International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 06 June 2024, pp: 18-21 www.ijaem.net ISSN: 2395-5252

Behavior-Based Malware Detection

J. Asvica, R. S. Dhanusree, S. Dharshana, S. Lavanya, P. N. Sowbarnika, S.Yaswanthraj

Department of computer science and engineering(cyber security), Sri Shakthi institute of engineering and technology, Coimbatore-India
Department of computer science and engineering(cyber security), Sri Shakthi institute of engineering and technology, Coimbatore-India
Department of computer science and engineering(cyber security), Sri Shakthi institute of engineering and technology, Coimbatore-India
Department of computer science and engineering(cyber security), Sri Shakthi institute of engineering and technology, Coimbatore-India
Assistant Professor, Department of computer science and engineering(cyber security), Sri Shakthi institute of engineering and technology, Coimbatore-India
Assistant Professor, Department of computer science and engineering(cyber security), Sri Shakthi institute of engineering and technology, Coimbatore-India

Date of Submission: 28-05-2024 Date of Acceptance: 06-06-2024

ABSTRACT — Malware is software code that has malicious intent. In recent years, there have been huge changes in the threat landscape. As our dependency on the Internet for social related information sharing and work increases, the number of the possible threats is huge and we are indeed susceptible to them. Attacks may from the individual or organisational level, to nation-states resorting to cyber warfare to infiltrate and sabotage enemies operation. Hence, the need for a secure and dependable cyber defense is relevant at all levels. Malware can only do harm if it is allowed to propagate and execute without being detected. Detection based on signature alone is not the answer, because new malware with new signatures cannot be detected. Thus, behavior-based detection is needed to detect novel malware attacks. Moreover, malware detection is a challenging task when most of the latest malware employs some protection and evasion techniques. In this study, we present a malware detection system that addresses both propagation and execution.

I. INTRODUCTION

In the early stages of the computer age, malware was created with limited objectives. However, recent paradigms have also been driven by motives of espionage, and gaining profit and information. This thesis is concerned with detecting malware before it can cause significant damage.

Malware, short for malicious software, poses a significant threat to computer systems, networks, and data worldwide. Traditional signature-based antivirus programs are effective against known malware strains but fall short when dealing with novel or rapidly evolving threats. To address this limitation, behavior-based malware detection has emerged as a vital approach in cybersecurity.

Behavior-based malware detection focuses on identifying malicious activities based on the behavior exhibited by software rather than relying solely on known signatures. This proactive approach allows for the detection of previously unseen malware variants and zero-day attacks, providing a more robust defense against evolving cyber threats.

II. LITERATURE REVIEW

2.1 Devesa, Jaime, et al. "Automatic behaviour-based analysis and classification system for malware detection." International Conference on Enterprise Information Systems. Vol. 2. SCITEPRESS, 2010.

Malware is any kind of code explicitly designed with harmful intentions, such as viruses, trojan horses or worms. Malware represents a high-priority issue to security researchers and poses a major threat to the privacy of computer users and their informationIn.Still, the traditional approach to analyse malware requires that a human analyst manually performs the tests and extracts the information in order to classify the sample (Moser et al., 2007).As future lines of work, we plan to

expand the features identified by the system until now. This is, defining more regular expression rules to perceive both malicious and legitimate behaviour since, in this way, the
classification will give better results. Moreover, combining our approach with static analysis techniques
may improve the obtained results.

2.2 Ahmadi, Mansour, Ashkan Sami, Hossein Rahimi, and Babak Yadegari. "Malware detection by behavioural sequential patterns." Computer Fraud & Security 2013, no. 8 (2013): 11-19.
For many years, malware has been the subject of intensive study by researchers in industry and academia. Malware production, while not being an organised business, has reached a level where automatic malicious code generators/engines are easily found. These tools are able to exploit multiple techniques for countering anti-virus (AV) protections, from aggressive AV killing to passive evasive behaviours in any arbitrary malicious code or executable. Development of such techniques has lead to easier creation of malicious executables. Consequently, an unprecedented prevalence of new and unseen malware is being observed. Reports suggested a global, annual economic loss due to malware exceeding $13bn in 2007.

2.3 The Multimedia Information Design field at Cincinnati State Technical Wagener, Gérard, Radu State, and Alexandre Dulaunoy. "Malware behaviouranalysis." Journal in computer virology 4 (2008): 279-287.
Several malware analysis techniques suppose that the disassembled code of a piece of malware is available, which is however not always possible. This paper proposes a flexible and automated approach to extract malware behaviour by observing all the system function calls performed in a virtualized execution environment. Similarities and distances between malware behaviours are computed which allows to classify malware behaviours. The main features of our approach reside in coupling a sequence alignment method to compute similarities and leverage the Hellinger distance to compute associated distances. We also show how the accuracy of the classification process can be improved using a phylogenetic tree. Such a tree shows common functionalities and evolution of malware. This is relevant when dealing with obfuscated malware variants that have often similar behaviour. The phylogenetic trees were assessed using known antivirus results and only a few malware behaviours were wrongly classified.

2.4 Devesa, J., Santos, I., Cantero, X., Penya, Y. K., & Bringas, P. G. (2010, June). Automatic behaviour-based analysis and classification system for malware detection. In International Conference on Enterprise Information Systems(Vol.2,pp.395-399)SCITEPRESS.

Several malware analysis techniques suppose that the disassembled code of a piece of malware is available, which is however not always possible. This paper proposes a flexible and automated approach to extract malware behaviour by observing all the system function calls performed in a virtualized execution environment. Similarities and distances between malware behaviours are computed which allows to classify malware behaviours. The main features of our approach reside in coupling a sequence alignment method to compute similarities and leverage the Hellinger distance to compute associated distances. We also show how the accuracy of the classification process can be improved using a phylogenetic tree. Such a tree shows common functionalities and evolution of malware. This is relevant when dealing with obfuscated malware variants that have often similar behaviour. The phylogenetic trees were assessed using known antivirus results and only a few malware behaviours were wrongly classified.

2.5Aslan, Ömer Aslan, and Refik Samet. "A comprehensive review on malware detection approaches." IEEE access 8 (2020): 6249-6271.
According to the recent studies, malicious software (malware) is increasing at an alarming rate, and some malware can hide in the system by using different obfuscation techniques. In order to protect computer systems and the Internet from the malware, the malware needs to be detected before it affects a large number of systems. Recently, there have been made several studies on malware detection approaches. However, the detection of malware still remains problematic. Signature-based and heuristic-based detection approaches are fast and efficient to detect known malware, but especially signature-based detection approach has failed to detect unknown malware. On the other hand, behavior-based, model checking-based, and cloud-based approaches perform well for unknown and complicated malware; and deep learning-based, mobile devices-based, and IoT-based approaches also emerge to detect some portion of known and unknown malware. However, no approach can detect all malware in the wild. This shows that to build an effective method to detect malware is a very challenging task, and there is a huge gap for new studies and methods. This paper presents a

detailed review on malware detection approaches and recent detection methods which use these approaches. Paper goal is to help researchers to have a general idea of the malware detection approaches, pros and cons of each detection approach, and methods that are used in these approaches

III. EXSISTING SYSTEM

Develop a behavioral analysis engine that monitors the activities of running processes in real-time. This engine should be capable of analyzing various behaviors such as file system interactions, network communications, system calls, and process behavior.Establish a baseline of normal behavior for different types of software and system processes. This baseline can be created by observing the behavior of legitimate software under normal conditions. Any deviation from this baseline could indicate potentially malicious activity.Implement anomaly detection algorithms to identify deviations from the established baseline. Techniques such as machine learning, clustering, or statistical analysis can be employed to detect anomalous behaviorDevelop heuristic rules to identify suspicious behavior patterns. These rules can be based on known patterns of malware behavior, such as attempts to modify system files, inject code into other processes, or establish unauthorized network connections.Monitor network traffic to detect suspicious communication patterns indicative of malware activity. Analyze network packets for known malware signatures, command and control communication, or unusual data transfer patterns.Integrate the behavior-based malware detection system with existing security infrastructure, such as antivirus software, firewalls, and intrusion detection systems, to provide comprehensive protection against malware threats.

IV. PROPOSED SYSTEM

Develop a real-time monitoring system that analyzes the behavior of running processes Monitor activities such as file system interactions, registry modifications, network communications, and process behavior Establish a baseline of normal behavior for different types of software and system processes Use machine learning algorithms to dynamically update the baseline as the system evolves Define heuristic rules based on known malware behavior patterns Look for indicators such as code injection, privilege escalation attempts, and suspicious process chains Integrate with existing security tools such as antivirus software, firewalls, and endpoint detection and response (EDR) systems Provide interoperability to facilitate seamless sharing of threat intelligence and response actions.

V. METHODOLOGY

-

VI. EXPERIMENTAL RESULT

Malware detection graph.

VII. RESULT AND DISCUSSION:

Malware detection and quarantining.

VIII. CONCLUSION:

In conclusion, The use of behavior-based malware analysis, often combined with machine learning techniques, has proven to be an efficient and effective approach for identifying and detecting malware. This method focuses on the activities of malware when it infects a system, either by extracting behavioral traits from the malware code statically or by dynamically monitoring its behavior in a sandbox environment. The approach has shown promise in improving the detection of unknown malware, although it can be slow and resource-intensive. Overall, behavior-based malware analysis has been widely employed and is essential for designing real-time monitoring and mitigation of malware, offering a more resilient alternative to traditional syntactic specifications in the face of evolving malicious code.

REFERENCES

[1] Pinchas Tamir; "High School Preparation and College Biology" BIOSCIENCE, 1969.
[2] Mieke Van Houtte; "Tracking Effects on School Achievement: A Quantitative Explanation in Terms of The Academic Culture of School Staff", AMERICAN JOURNAL OF EDUCATION, 2003.
[3] Pamela S. Ecker; Jason Caudill; David Hoctor; Colleen Meyer; "Implementing An Interdisciplinary Capstone Course for Associate Degree Information Technology Programs", 2004.
[4] Corinne Alfeld; David M. Hansen; Steven R. Aragon; James R. Stone; "InsideThe Black Box: Exploring The Value Added By Career and Technical Student Organizations to Students' High School Experience", CAREER AND TECHNICAL EDUCATION RESEARCH, 2006
[5] Leandro S. Almeida; M. Adelina Guisande; Ana Paula Soares; Luísa Saavedra; "Acesso E Sucesso No Ensino Superior Em Portugal: Questões De Género, OrigemSócio-educational E PercursoAcadémico Dos Alunos", PSICOLOGIA-REFLEXAO E

CRITICA, 2006.

[6] Jose Maria Cela-Ranilla; Mercè Gisbert; Janaina Minelli de Oliveira; "Exploring The Relationship Among Learning Patterns, Personality Traits, and Academic Performance in Freshmen", EDUCATIONAL RESEARCH AND EVALUATION, 2011.

[7] M. D'Amico; Grant B. Morgan; Thashundray C. Robertson; "Student Achievement in Identified Workforce Clusters: Understanding Factors That Influence Student Success", COMMUNITY COLLEGE JOURNAL OF RESEARCH AND PRACTICE, 2011.

[8] Lama M. Al-Qaisy; "The Relation of Depression and Anxiety in Academic Achievement Among Group of University Students", INTERNATIONAL JOURNAL OF PSYCHOLOGY AND BEHAVIORAL SCIENCES,2016.