IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205352|

A Survey on Automatic Framework for Android Malware Detection Using Machine Learning

Om Patil, Viraj Dalvi, Yash Chaudhari, Akshay Narkhede, Prof.Mrs. Suvarna Potdukhe

Department of Information Technology, RMD Sinhgad School of Engineering, Warje, Pune, India

ABSTRACT: Malware is a big problem in the realm of operating systems and software. Specifically, the Android operating system, for reasons related to developer compromise. As a result, numerous malware detection algorithms have been created. However, techniques for detecting newer versions or worse variations of malware continue to be inadequate. Despite the fact that multiple detection and analysis approaches are being researched and developed to their greatest potential, the detection accuracy of emerging viruses remains a critical issue. In this research, we propose and investigate a new technique that will be built into an application for more accurately and informatively identifying malware in an Android operating system. The ability to access datasets from the appropriate operating system is a critical component of the process. In the sky of information technology, the suggested methodology falls under the department of Machine Learning. During training, the model will discriminate harmful files based on unique characters recognised when performing feature selection.

KEYWORDS: Mobile; Android; Malware; Operating system; Machine Learning; Malicious.

I. INTRODUCTION

With the growth of the Android market and the rising reliance on mobile phones, harmful applications are on the rise. Improving the efficacy of malicious application identification has become an urgent requirement in the current environment. As a result, integrating machine learning technology to malicious application detection, which can cut labour costs and enhance detection efficiency, has emerged as a hot research topic. Because present tactics are ineffective, various types of malware attacks can arise. The proposed model will significantly improve detection of various malware types.

II. REVIEW OF LITERATURE

Peng Tian and Xiaojun Huang, This paper proposes a new model for detecting Android malicious applications. The model obtains the API call sequences of APP runtime, and extracts features from them. These features have the highest correlation with malicious attributes detection and have the characteristics of small redundancy between each other. And noticed that API subsequences generated by normal behavior that may exist in a malicious application can interfere with the training of the detector. We use VSM, and K-means combined with the GBDT algorithm to eliminate this interference and improve the detection accuracy. Experiments show that this method can effectively eliminate the influence of interference API sequence and obtain higher detection.[1].

Fei Chen, Yan Fu ,In this paper, we propose a new approach for the dynamic detection of malicious executables on the platform of Windows. Our approach extracts signatures of malicious executable's behaviors by using API (Application Program Interface) interception technique which makes possible the detection of unknown malicious executables. The dynamic detection of unknown malicious executables is achieved in three major steps: getting the sequence of API function calls of the executable, processing the API sequence to generate a vector, calculating the similarity between the vector and the feature library constructed by security policies to verify if the executable is malicious. The experiment confirms that this approach is effective in detection of unknown malicious executables.[2]

Yingbo Li, Jing Fang and Cheng Liu,With the increasing popularization of smartphones in life, malicious software targeting smartphones is emerging in an endless stream. As the phone system possesses the highest current market share, Android is facing a full-scale security challenge. This article focuses on analyzing the application of Dalvik injection technique in the detection of Android malware. Modify the system API (Application Program Interface)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205352|

through Dalvik injection technique to detect the programs on an Android phone directly. Through the list of sensitive APIS called by malicious programs, eventually judge the target program as malicious or not.[3]

Yong Li, Due to the rapid growth of android malicious application samples, traditional detection methods need to spend a lot of time training, a detecting method for malicious mobile application based on incremental SVM was proposed to achieve incremental learning of the detection system. The method used the SVM as the classification and training algorithm and extracted sensitive permissions and APIs as application characteristics. Based on SVM, a dual weight function was designed to filter the historical training samples to avoid redundant samples, and the incremental learning method of SVM was implemented in combination with KKT conditions. Therefore, the training time could be reduced, and the learning efficiency of the malicious application detection system could be improved without reducing the training accuracy.[4]

Xie Bailin, Yu Shenzhen, Wang Tao,Today more and more network-based attacks occur at application layer. Observed from the network layer and transport layer, these attacks may not contain significant malicious activities, and generate abnormal network traffic. However, traditional security techniques usually detect attacks from those two layers. Although some security techniques can detect some application layer attacks, these techniques can only detect some known attacks and these techniques can't detect the unknown or novel attacks that happened on the application layer. In theory, application layer anomaly detection can detect unknown and novel attacks that happened on application layer, so the research of application layer anomaly detection is very important. This paper presents a new application layer anomaly detection method which is based on HSMM. The experimental results show that this method has high detection accuracy and low false positive ratio[5]

Yang Gao,With more and more online services developed into web applications, security problems based on web applications are becoming more serious now. Most intrusion detection systems are based on every single request to find the cyber-attack instead of users' behaviors, and these systems can only protect web application from known vulnerability rather than some zero-day attacks. To detect newly developed attacks, we analyze web logs from web servers and define users' behaviors to divide them into normal and malicious ones. The result shows that by using the feature of web resources to define users' behaviors, a higher accuracy rate and lower false alarm rate of intrusion detection can be obtained[6]

Wataru Matsuda,The targeted attacks cause severe damage worldwide. Detecting targeted attacks is challenging because the attack methods are very sophisticated. Network-based solutions such as Firewall, Proxy Server, and Intrusion Detection System (IDS) have been widely used. In addition to this, recently, detection methods for malicious programs by monitoring behavior on the endpoints called Endpoint Detection and Response (EDR) have been proposed. Also, some researchers introduce detection methods using DLLs by analyzing suspicious files on the sandbox, such as Cuckoo. Using Cuckoo is one of the solutions for analyzing files that are already identified as malicious. In this research, we propose a real-time detection method of malicious tools using DLL information collected by System Monitor (Sysmon): a free logging tool provided by Microsoft. The purpose of our method is detecting new malicious processes in the production environment. We focus on DLLs commonly loaded by malicious tools regardless of the environments, then propose "the common DLL lists" for detection. Moreover, we introduce a practical detection method that utilizes Elastic Stack as Security Information and Event Management (SIEM). By using Elastic Stack, DLL information loaded on computers can be uniformly monitored and enables real-time detection by comparing logs with the common DLL lists. We evaluate the effectivity of the proposed method using four free malicious tools introduced by US-CERT: China Chopper, Mimi Katz, PowerShell Empire, and HUC Packet Transmitter. As a result, our method detected China Chopper, Mimi Katz, PowerShell Empire with 100 false positive occurred for HUC Packet Transmitter, and false positive rate was 0.55lists are useful for detecting malicious tools in real-time using Elastic Stack.[7]

Parnika Bhat, Kamlesh Dutta,Android is currently the most popular operating system for mobile devices in the market. Android devices are being used by every other person for everyday life activities and it has become a center for storing personal information. Because of these reasons it attracts many hackers, who develop malicious software for attacking the platform; thus, a technique that can effectively prevent the system from malware attacks is required. In this paper, and malware detection technique, Mildrid has been proposed for detecting malware applications on Android platform. The proposed technique statically analyses the application files using features which are extracted from the manifest file. A supervised learning model based on Naive Bayes is used to classify the application as benign or malicious. Mildrid achieved Recall score 99.12[8]

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205352|

Dr. V. Lakshman Narayana1,Mobile Ad Hoc Networks (MANETs) are infrastructure-less networks that are mainly used for establishing communication during the situation where a wired network fails. Security related information collection is a fundamental part of the identification of attacks in Mobile Ad Hoc Networks (MANETs). A node should find accessible routes to remaining nodes for information assortment and gather security related information during route discovery for choosing secured routes. During data communication, malicious nodes enter the network and cause disturbances during data transmission and reduce the performance of the system. In this manuscript, a Time Interval Based Blockchain Model (TIBBM) for security related information assortment that identifies malicious nodes in the MANET is proposed. The proposed model builds the Blockchain information structure which is utilized to distinguish malicious nodes at specified time intervals. To perform a malicious node identification process, a Network Block Monitoring Node (NBMN) is selected after route selection and this node will monitor the blocks created by the nodes in the routing table. At long last, NBMN nodes understand the location of malicious nodes by utilizing the Blocks created. The proposed model is compared with the traditional malicious node identification model and the results show that the proposed model exhibits better performance in malicious node detection[9].

III. OPEN ISSUE

Android has over one billion active users across all of their mobile devices, causing a surge in the amount of information received from different users, factors that have driven cybercriminals to build malware to tackle the problems presented by malware. Android has a unique design and security restrictions, such as a unique user ID for each application, system permissions, and its distribution mechanism, Google Play. The primary goals are to improve malware detection accuracy while also reducing money and effort. The proposed model will also handle the challenge of determining if a file is malware or not.

IV. CONCLUSION

The principle of application monitoring is studied deeply, and the dynamic detection of application based on Hook technology is used to obtain the system API callsequence. On the basis of the existing research, thefeature selection algorithm is extended and the most helpful features of detection are extracted. Aiming at the problem of interference in the application API sequence, a detection model is designed and implemented. A scheme of using the vector space model to remove the interference API sequence is proposed.

REFERENCES

1 Stephen Feldman ,Dillon Stadther ,Bing Wang, “Manilyzer: Automated Android Malware Detectionthrough Manifest Analysis ,” in 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems.

2 WILLIAM ENCK,PETER GILBERT,SEUNGYEOP HAN,VASANT TENDULKAR,BYUNGON CHUN,LANDON P. COX,JAEYEON JUNG,PATRICK MCDANIEL,ANMOL N. SHETH,”TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones,” ACM Transactions on Computer Systems (TOCS) TOCS Homepage archive Volume 32 Issue 2, June 2014

3 Corrado Aaron Visaggio,Eric Medvet,Gerardo Canfora,Francesco Mercaldo “Detecting Android Malware using Sequences ofSystem Calls,” in Third International Workshop on Software Development lifecycle for Mobile ESEC/FSE 2015

4 Alberto Ferrante,Eric Medvet,Francesco Mercaldo,Jelena Milosevic,Corrado Aaron Visaggio, “Spotting the Malicious Moment: CharacterizingMalware Behavior Using Dynamic Features,” 2016 11th International Conference on Availability, Reliability and Security

5 Zhenyu Ni, Ming Yang, Zhen Ling, Jia-nan Wu, Junzhou Luo , ”Real-time Detection of Malicious Behavior in Android Apps,” 2016 International Conference on Advanced Cloud and Big Data 6 Quan Hu, Xiuliang Mo, Chundong Wang ,”Based on the Markov Chain Model of Android Platform Malicious APP Detection Research,” 2016.4 Journal of Tianjin University of Technology Vol. 32, No. 2

7 (2017) The Xposed webpage .[Online]. Available: http://repo.xposed.info

8 Li Wang Yuanchun Wan , Weidong Hao ,”Based on Honeypot Android Malicious Code Dynamic Analysis,” 2016 Microcomputer Application Volume 32, No. ll

9 (2017) The malicious application set webpage . 10 (2017) The virustotal webpage .[Online]. Available: https://www.virustotal.com

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details