ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Malware Detection: "Analysis & Classification of Malwares on Android"

Admane Ganesh Ulhas

ME Student, Department of Computer Engineering, MCOERC, Nasik, Savitribai Phule, Pune University Maharashtra, India

ABSTRACT: Due to the quantum jump in functionality, the rate of upgrading traditional mobile phones to smart phones is tremendous. One of the most attractive and eye-catching features of smart phones is the availability of a huge number of apps for users to download and install. However, it also means hackers can easily or simply distribute malware to smart phones, launching a choice of attacks. Research in these areas, it focuses on efforts from app designer, app store central control, and users, who are also required to defend against such malware. In recent times, a new generation of Android malware families has emerged with advanced avoidance capabilities which make them much more difficult to detect using conventional methods. Thus proposed work is investigates using a parallel classification approach for early detection of Android malware. Proposed work is provide high detection accuracy and Increase performance. Analysis of malwares is nothing but the possibility of malwares and classification is classifying the malwares.

KEYWORDS: Android, Malwares, parallel classifier, Analysis, Classification.

I. INTRODUCTION

Now a days, researchers founds very huge and speedy enlargement of the Mobile Malwares on Mobile Computing devices such like Smartphone's and tablets and so on. These computing devices are more and more popular presently. In realism, Mobile Malwares has already become to serious concern. The reason behind this uncontrolled growth of Android or mobile malware is the being there of user friendly feature-rich apps which are offered to users via online application stores. These Stores become the gateway through which malware can be easily distributed on android application. Even though official app markets such as Google Play store take up some anti malware system to screen out malware, but those apps are loosely checked exclusively based upon what permissions they use. More critically, presence of third-party app markets allows simple and straightforward distribution of android app with no any security inspection or test. Both official and third-party app markets have been enticing or attracting targets for the attackers to distribute their malware.

In view of the fact that February 2011, Google introduced Bouncer to its app store in order to screen submitted apps for malicious behaviour. in spite of this measure, there were still some report outbreaks of Android malware distributed by he use of the official market. For example of DroidDream was distributed through the official Android Market and according to Symantec affected 50,000 to 200,000 users. In actuality, the analysis process of Bouncer, which is based on run-time dynamic analysis, has been before verified by Oberheide and Miller to be vulnerable to detection avoidance by well-crafted malicious apps [5][6]. The third party Android app stores that have emerge in recent years have also become a extremely strong source of malicious app distribution like these stores have weak to missing measures to prevent malicious apps from being uploaded and distributed to user's devices.

In Studies [5][7] such as have exposed that current families of Android malware are difficult to punctually spot in the wild. This is because of the avoidance techniques being used harmless apps that provide functionalities that users want. By employing polymorphic techniques and encrypting malicious payload and signature-based scanning is with no trouble bypassed. With greater than before code obfuscation, malware analysts take longer to uncover the malicious behavior, classify samples, and generate signatures for detecting the new threats. In addition, some Android malware families similar to AnserverBot are well-known to have the capability to fetch and execute malicious payloads at run time hence rendering the zero-day detection of such malware by past signatures quite unproductive.

These challenges call for new and more successful detection approaches to ease the impact of evolving Android malware. Hence, in this paper we propose a scheme for early detection of Android malware by means of parallel

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

classification. Main objectives of system are Malware detection system will detect all types of malware and malware families. Malware detection accuracy is high because use of parallel classifier.1) to design system to Detect all types of Malwares and their categories or families on android. 2) To improve detection accuracy by using parallel classifier. 3) To detect the system level malwares. 4) Complete white box analysis [5].

II. RELATED WORK

Literature survey is study of existing system of malware detection techniques and existing methods. Different types of malwares detection and Classification methods are disused below.

1. Simple Analysis of Malwares Based on permission and intent

In [2] this method is based on analysis of sure combination of permissions and intents used by the applications. These combinations build a distinctive characteristics to classify the apps into benign and malware classes.

Malware detection using this method: The initial stage is the Extractor which extracts the permissions and intents used by the target app from the manifest file. Manifest file is the heart of applications which contains the every minute detail of the functionalities and capabilities of parent app. The after that stage is the pre-processor which prepares the gathered information for the classifier stage and sifts the redundant data. Third stage is Classifier which evaluates the processed information against the distinguishing matrix and classifies the apps as benign, malware or benware [2].

2. Malwares Detection by using Bayesian Classsification Approach

In [3] the Bayesian-based classifier consists of learning and detection stages. The learning stage uses a training set of identified malicious samples in the wild and another set of benign Android applications, jointly called the app corpus. The Java-based package analyzer uses more than a few 'detectors' to extract the most wanted features from each app in the corpus. The feature set is after reduced by a feature ranking and selection function, while the training function computes the massive and restricted possibilities used within formulating or modeling the algorithm employed for the final classification decisions.

In this technique implemented a Java-based Android package analyzer and profiling tool for automated reverse engineering of the APK files. In this method initial, the .apk files are decompressed into divide folders containing the Manifest file, .dex file along with additional resource subfolders. Afterwards, the manifest file is transformed into readable format using AXML2jar. The .dex file is followed by disassembled by means of a tool called Baksmali [3][13]. Baksmali be a disassembler used for the .dex format secondhand by Dalvik. Baksmali disassembles .dex files into many files with .smali extension. Every .smali file contains only one class information which is corresponding to a Java .class file. The files in the decompressed folders are mined to extract related properties afterward used to construct the Bayesian classification-based models [3][13].

3. Malwares Detection and classification by using Linear SVM

In [4] this method author uses SVM (Support Vector Machine) in this method to watch the preferred resource features, an agent is required that can constantly examine the corresponding features within a device. This research on the other hand executes a normal application and an irregular application on the Android stage to check malware detection. SVM structure of the Android malware detection system, which principally consists of a mobile agents and an analysis or investigation server

4. Comparsion of Methods

In [2] simple Malware detection system is suitable for only static analysis so it poor performance. In [3] Malware Detection using Bayesian classification it use reverse engineering approach is faster than simple malware detection and dynamic method but it reverse engineering is very complicated process. In Malware detection using SVM it support vector machine but it is very old approach of detection [4].

III. PROPOSED SYSTEM AND IMPLEMENTATION DETAILS

New detection system that is malware detection: analysis and classification of malwares on android is uses two main phases analysis phase and classification phase. If the possibilities of Malwares are present in android applications then it can only classify. This new detection system support for classification purpose it uses parallel classifiers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Fig.1 shows analysis phase of malware detection and classification system. In analysis phase task are performed first upon system take input android application (normal or malicious) then this android .apk is convert into the .jar file by use of convertor and after decompile process of jar file is converted into .dex file it is also called decompile file. Exactor is extracting all files and folders in dex files and template or pattern are generated. If generated template or patterns are fit into suitable classification form then it can go to classification.

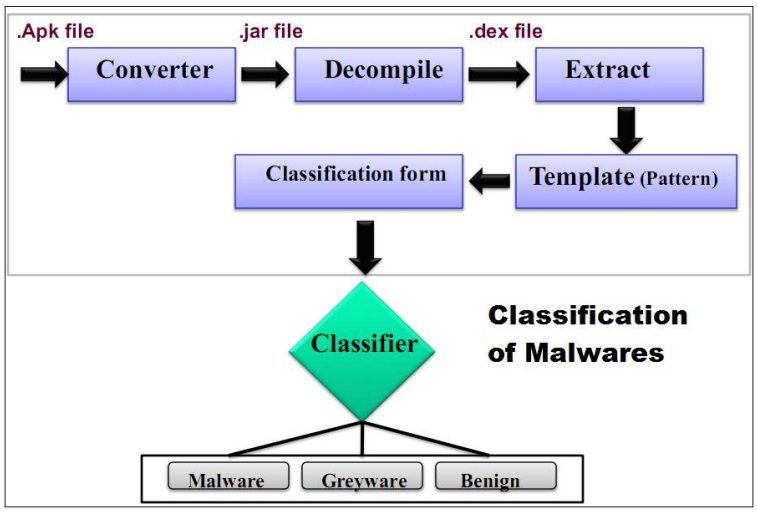

Fig 1. Analysis phase of the system

Fig. 2 shows the classification phase of the system. After the analysis phase second phase classification phase. In classification phase we use different classifiers for the classification of malwares. All classifier work parallel.

Parallel approach identify and detecting malwares on android as well as system level. The parallel classifier algorithm included: j4.8 Decision tree (tree based), k-mean (function based), Naïve Bayes (probabilistic based) and Bloom filter (rule based) and call graph for system level.

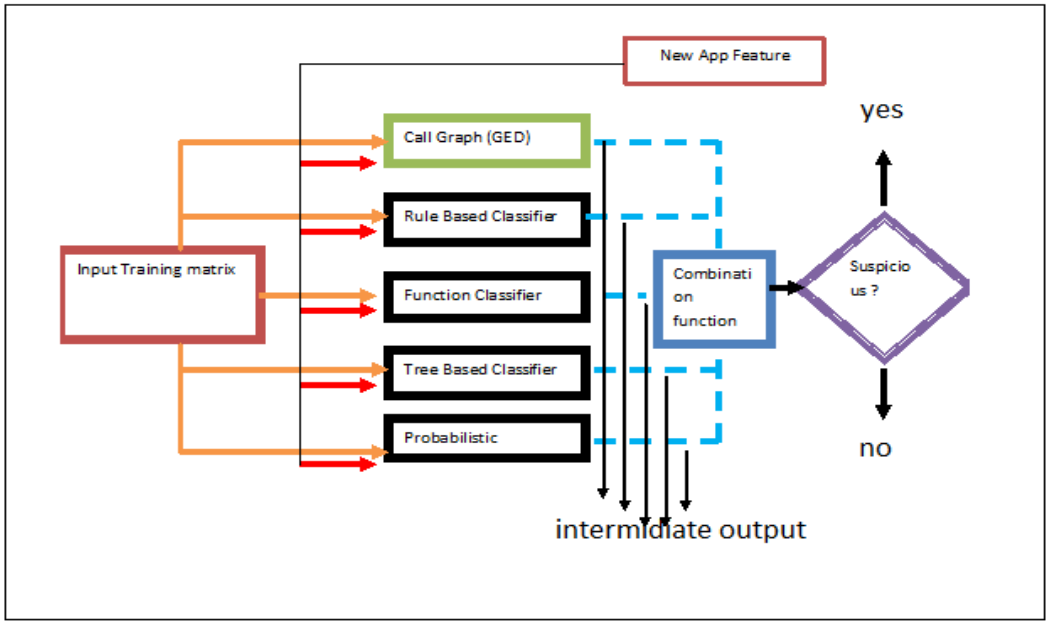

Fig 2. Classification phase of Malwares detection system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

IV. RESULT

1. Help page

Fig. 3. Help page of malware detection system

2. Analysis process

Fig. 4. Analysis process of malware detection system

3. Classification process

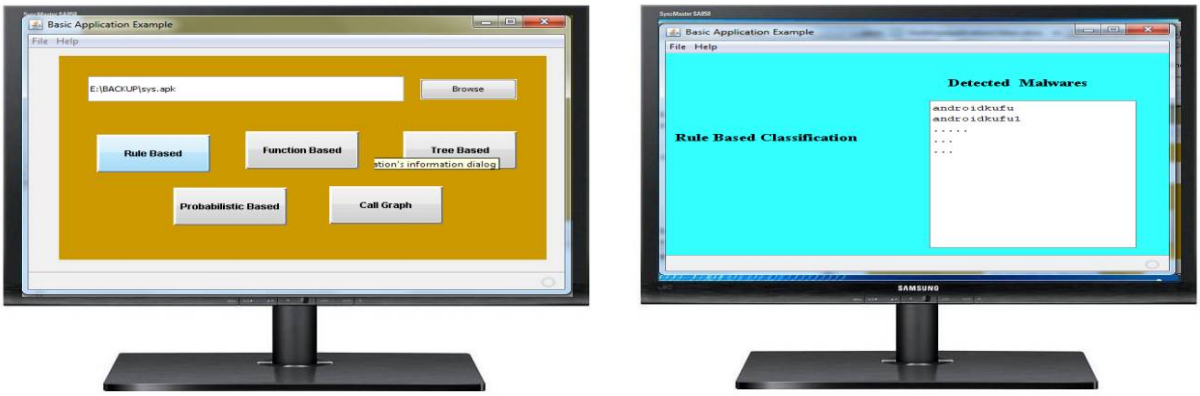

Fig. 5. Classification process of malware detection system

V. CONCLUSION AND FUTURE WORK

This project reveals the unseen or hidden solution to the major challenge in previous detection system. The project consists of two phases, first is analysis phase and second is classification phase. In analysis phase is used for checking the possibility of malware and classifier phase is used for to classify the detected malware. For the classification of malware we use the parallel classifier techniques so it provide and improve the detection accuracy and increase performance due parallel work.

ACKNOWLEDGMENT

I am thankful to Dr. Varsha H. Patil, Head of Department Computer Engineering and vice Principal, MCOERC, Nasik for giving her precious time and guideline during this paper also for her expert guidance and continuous encouragement throughout this paper. I would like to express deepest appreciation towards, Nasik and Prof. Dr. G. K. Kharate, Principal MCOERC, Nasik,. I am also thankful to Dr. N.A. Deshpande (ME Coordinator) and Prof. Swati Bhavsar, whose invaluable guidance supported me in completing this paper.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

REFERENCES

1. Vaibhav rastogi,yan chen and xuxian jiang "catch me if you can:Evaluating android anti-malware against transformation attacks", International IEEE Trancation on information forensics and security,2013.
2. Fauzia idrees and muttukrishanan, “Investigating the android Intens and permissions for malware detetection,” seventh internationa workshop on selected topics in mobile and wireless computing,2014.
3. S. Y. Yerima, S. Sezer and G. McWilliams. "Analysis of Bayesian Classifcation Aprroaches for Android Malware Detection," IET Information Security, Vol 8, Issue 1, January 2014.
4. Hyo-sik ham, Hwan-hee kim, myung-sup kim nd mi-jung choi,”Linear SVM-Based android malware detection for Realiable IoT services”,Hindawi pulishing corporaition jornal of applied mathematices, volume 2014
5. Suleiman Y. Yerima, Sakir Sezer, Igor Muttik "Android Malware Detection Using Parallel Machine Learning Classifiers" 2014 Eighth International Conference on Next Generation Mobile Applications, Services and Technologies
6. J. Oberheide and C. Miller, “Dissecting the Android Bouncer” SummerCon 2012.
7. Apvrille and T. Strazzere, “Reducing the window of opportunity for Android malware Gotta catch ’em all,” Journal in Computer Virology vol. 8, No. 1-2, pp. 61-71, 2012. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
8. Zhiyong shan and xin wang,”Growing grapes in your computer todefend angainst malware”, IEEE Transaction on Information forensics and security,vol.9,no2,feb 2014
9. Yan qiao, Tao li and shigang chen,”one memory access bloom filers and their generatization”,unviversity of florida,Gainesville,FL 32611,USA
10. Justin sahs and Latifur khan.”A Machine Learning approach to android malware detection”,European Intelligence and Security Informatics Conference,2014.
11. Tomas Eder,Michael Rodler,Dieter vymazal and zeilinger,”ANANAS- A framework for analyzing android applications”,International conference on availbility,reliability and security,2013
12. Dolly uppal,Rakhi sinha, Vishakha Mehra and vinesh Jain,”Malware detection and classification Based on Extraction of API sequences”,internation conference on advances in computing, communications and informatics,2014.
13. Baksmali: http://code.google.com/p/smali,Accessed June 2013.

BIOGRAPHY

ADMAENE GANESH ULHAS, Department of Computer Engineering, MCOERC, Nasik, Savitribai Phule, Pune University, Maharashtra, India