International Journal on Advanced Science Engineering Information Technology

Vol.10 (2020) No. 2
ISSN: 2088-5334

DATDroid: Dynamic Analysis Technique in Android Malware Detection

Rajan Thangaveloo[a1], Wong Wan Jing[a2], Chiew Kang Leng[a3], Johari Abdullah[a4]

[a] *Faculty of Computer Science and Information Technology, University Malaysia Sarawak, Kota Samarahan, Sarawak, 94300, Malaysia*
E-mail: [1]trajan@unimas.my; [2]wanjingwng@gmail.com; [3]klchiew@unimas.my; [4]ajohari@unimas.my

Abstract— **Android system has become a target for malware developers due to its huge market globally in recent years. The emergence of 5G in the market and limited protocols post a great challenge to the security in Android. Hence, various techniques have been taken by researchers to ensure high security in Android devices. There are three types of analysis namely static, dynamic and hybrid analysis used to detect and analyze the malicious application in Android. Due to evolving nature of the malware, it is very challenging for the existing techniques to detect and analyze it efficiently and accurately. This paper proposed a Dynamic Analysis Technique in Android Malware detection called DATDroid. The proposed technique consists of three phases, which includes feature extraction, feature selection and classification phases. A total of five features namely system call, errors and time of system call process, CPU usage, memory and network packets are extracted. During the classification 70% of the dataset was allocated for training phase and 30% for testing phase using machine learning algorithm. Our experimental results achieved an overall accuracy of 91.7% with lower false positive rates as compared to benchmarked method. DATDroid also achieved higher precision and recall rate of 93.1% and 90.0%, respectively. Hence our proposed technique has proven to be able to classify malware more accurately and reduce misclassification of malware application as benign significantly.**

Keywords— **android malware; dynamic analysis; static analysis; hybrid analysis; malware detection.**

I. INTRODUCTION

Worldwide smartphones market is dominated by Android operating system (OS) with a staggering figure of 86.3% in 2018 as reported by IDC statistic data [1]. Android gains its popularity due to its open source concept which enables users to use it freely in Google Play as well as other third-party apps stores. This fact has encouraged millions of mobile applications developments, which have assisted in our day to day living and businesses. Owing to this huge market, attackers are interested in targeting Android platform where people spend most of their time. According to Novinson [2], Android-based malware samples has increased exponentially in 2018 compared to 2017 with a record of 5 million malwares in the first eight months alone. Goodin [3] stated in his report that hundreds of thousands of poorly secured devices with Google's Android OS had been attacked by a powerful denial-of-service attack. Besides, it is reported that there are around three hundred applications of botnet found in the official Google Play market [3]. The malwares will silently enlist the devices into the vicious network that sent junk traffic to website once the user installed the applications. The malware causes their device to become unresponsive or go offline. Moreover, providing a secure communication for 5G mobile network remain a challenge due to limited protocols to address the security issues.

It is imperative that a serious work begins intensively in Android Malware detection to defend and safeguard against these attacks. According to Skovoroda and Gamayunov [4], there are many methods based on three main techniques namely static analysis, dynamic analysis and hybrid analysis (combination of Static and Dynamic) to detect and analyze the behavior of the malicious application. The limitation of detecting Android malware with static analysis is that it does not find vulnerabilities present in the runtime environment. This is because the technique uses static signatures from the application's manifest file. As such, it is unable to accurately detect malware which does not have obvious malicious signature. In addition, most of the apps are obfuscated, or bytecode encrypted.

On the other hand, dynamic analysis is used to overcome the limitation faced by the static analysis where it performs the analysis during its runtime. Certain application will reveal their original behaviors during its run time, hence dynamic analysis helps to uncover some features that cannot be determined by static analysis. The common behaviors that concerned in the analysis is system calls, API calls, network traffic, or even file access. Among them the most popular in dynamic behaviors used is the network