BOOK CHAPTER | Android Malware Infections

A Review On Android Malware Attacks

Ndatsu, Z. & Almustapha, A.J.
Department of Computer Science
The Federal Polytechnic
Bida, Niger State, Nigeria
E-mails: zainab.Ndatsu@fedpolybida.edu.ng, al-mustapha.A.Jiro@fedpolybida.edu.ng

Abstract

This paper presents a review on Android Malware attacks. Malicious software is also known as malware is one of the most serious problems in the cyber world today. Malicious software that are developed by hackers are mainly polymorphic or metamorphic that can alter its code as it spreads. It is necessary for Android users to have the knowledge of this malware. It provides an introduction and review of the key developments within this field, in addition to making suggestions for future research.

Keywords: Malware, Security, networks, Androids, Infections, Cyberworld.

Introduction

The smartphone arrives with different operating system (OS) which includes windows operating system, iOS, and android operating system. Among these, android OS is the most popular and friendly due to its openness and application availability in different open sources. This android OS is own by Google corporation which has made the android application free in an open market. This openness of application has made android a soft target for malicious software (Adebayo, *et al*., 2013).

In 2017, Nokia released the "Threat Intelligence Report," which examines malware behaviour in communications networks and found that 72 percent of network infections target smartphones, with Android accounting for 68.50 percent, Windows PC accounting for 27.95 percent, and others accounting for 3.54 percent. The majority of infections, 69 percent, target Android devices (Alqahtani *et al*., 2019). New malware which are developed every day are known to be the most altered versions of the previous one by the use of enlightened replication method. A large number of samples have been used. Having a large number of data sets contributes to the prophetic ability and dependability of the built model that gives a presentable outcome (Dewanje & Kumar, 2020). Detecting, analysing, and removing malware is in high demand across computing and mobile platforms. Many researchers have developed many approaches and algorithms including (Christodorescu *et al*., 2005; Siddiqui, 2008; Shabtai *et al*., 2011; Eder *et al*., 2013; Mirjalili & Lewis, 2016).

Citation: Ndatsu, Z. & Almustapha, A.J. (2022): A Review On Android Malware Attacks
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

Malware Types

According to Tahir (2018), malware are in different forms and can be found in more than one class.

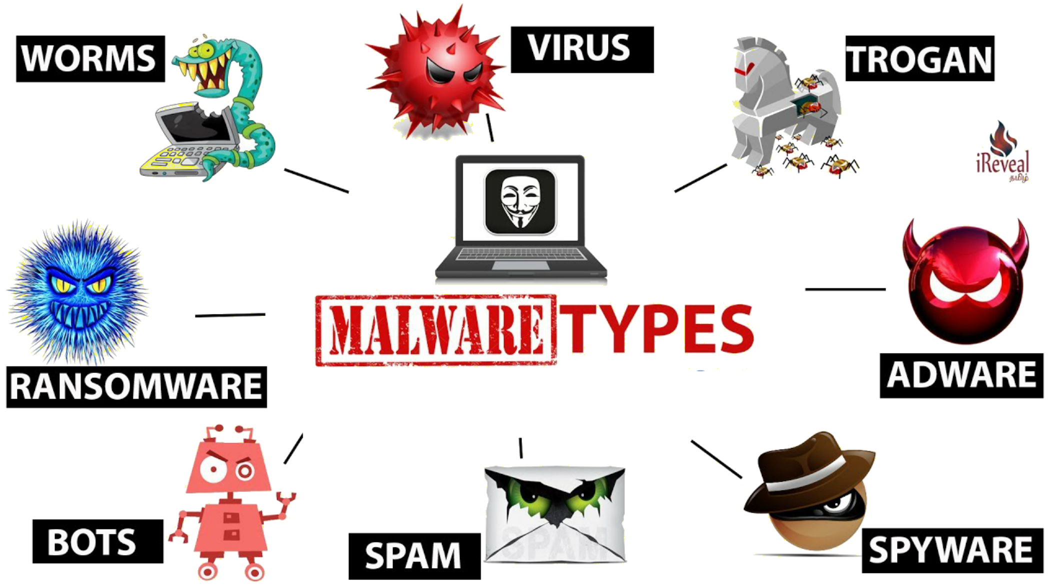

Fig. 1: Types of Malware
Source: https://www.ndimensionz.com.au/2017/09/19/what-are-the-types-of-malware-that-could-be-potential-threat-to-the-computer-system/

The different types of malware are explained below.

Worms are malicious part of program that duplicate, transmit over storage medium, consume internet and system resources which leads to low performance of the system. They can duplicate themselves, antivirus scanners are able to identify these codes because of multiple existence.

Viruses affect system and other files by duplicating itself. It attaches itself to files mostly the executable files, programs and spread over the system and network system which lead to low performance and denial of service.

Rootkit creates an environment for itself and other malware by taking control of the operating system. Avoid to be detected and consider as normal applications by malware antivirus in the system by using the masking techniques.

Trojan Horse serves as useful package but it has negative reasons. They don’t duplicate but it is transmit into a system by network interaction for instance downloading. It takes vital evidence, users' activities can be observed, and data on the system if they exist can be deleted, altered, or damaged.

Spyware takes user’s vital information with their knowledge or spy on activities of the user. It however is connected on the system without their acquaintance and unknowingly collects the material and gives to the designer. Big establishment for instance Google also utilise spyware to get their users information requirement.

Cookies are text files that contain information that is saved on the user's computer by the web browser for future use. Cookies appear to be harmless, but when they are employed by malware, they constitute a menace.

Adware place advertisement on users systems without their authorization and disturb the present action perform by the user. Their purpose is to get monetary again. It has negative effect as other malicious program.

Sniffers are computer program that watch and write the traffic of the network. Users' activity can indeed be monitored, and content on the platform can be erased, edited, or damaged if it exists.

Botnet which gives hacker access to control and harm the system. They are a collection of compromised systems that are managed by hackers/attackers and used to carry out nefarious operations without the owner's knowledge. Denial of service attacks can be form by them, spam messages be send by them and also steal users information.

Spam which is Junk emails which are identical emails send to many users at the same time. It takes many of bandwidth and also causes low performance of the system.

Keyloggers are types of spyware that makes use of record key strokes to access credit card details, passwords, and other vital and important figures. It gets into a system from installation of malware program or visiting any infected site by user.

Ransomware has become a frequent threat for network computer. It encrypts users data, stop some software and denial users the use of operating system unless their requests are met. Their request is mostly in form of finance. It is not guaranteed that the system will be released.

Different Techniques for Malware Detection

Detection techniques of Malware can be divided into three (3) groups heuristic based, signature based and specification based Tahir (2018). The three techniques detect and identify malware and ensure systems safety from those malwares that can cause a potential loss data and resources.

Heuristic Based

In order to detect and address known and undiscovered malware threats, this detection technique identifies or distinguishes between normal and aberrant activity of a computer system. There are two (2) steps to the detection process. The operations of the computer system are examined without being attacked in the first stage, and a record of critical information is preserved that may be tested in the event of an assault. In the second stage, this difference is examined in order to identify a specific type of malware.

The following three (3) key modules are contained in the activity detector utilized in heuristic based techniques. These are Collection of Data, Algorithm Matching and Interpretation.

1. Collection of Data: in this module the collection of data is done either dynamic or static.
2. Algorithm Matching: This module is in charge of matching the activity signature with the information converted from the interpretation module. Activity detector explains the functionality of how the three (3) modules work together.
3. Interpretation: This module interprets and transforms the collected data from data collection module into intermediate form.

Signature Based

In malicious codes a line of bit defines as signature is encoded in its code to detect malware type in future. The detection technique based on signature is used by recent antivirus software. The antivirus software separates the code of the infected file and searches for patterns that are specific to a malware kind. Malware signatures are stored in a database and then compared throughout the detection process. String or pattern scanning or matching is another name for this type of detection technology. It can also be static, dynamic, or hybrid.

Specification Based

Programs are examined in terms of their specifications in a specification-based detection technique, which looks for normal and anomalous behaviour. The main difference between this technique and heuristic based detection techniques is that Heuristic-based detection techniques used machine learning and AI algorithms to detect valid and invalid program activity, whereas specification-based detection techniques analysed the behaviour defined in the system specification. This approach involves a manual comparison of a system's regular operations. By reducing false positives and raising false negatives, it overcomes the limitations of heuristic-based approaches. The specification-based detection method is derived from the heuristic-based detection technique, and each malware detection technique can be hybrid, dynamic or static (Tahir, 2018).

Detection Techniques for Android Malware

The malware detection technique is divided into classification, analysis, malware detection and eventual containment (Adebayo & AbdulAziz, 2014). Classification techniques which include association mining, machine learning, rule-based decision tree and many others have been used in the classification of computer programs into malicious or benign set. Malware analysis is the process of finding instances of malware utilising various schemes and properties of known malware characteristics.

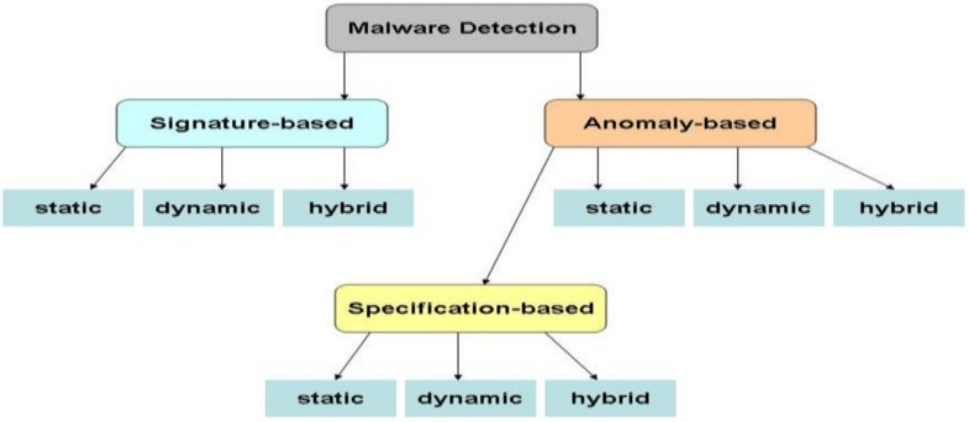

Fig 2: Malware Detection Framework
Source: https://www.researchgate.net/figure/Figure-1-Malware-Detection-Techniques_fig1_321788929

On the other hand, malware detection entails quickly identifying, detecting, and validating any incidence of malware in order to prevent additional system harm. The final task is to contain the infection, which entails attempting to stop the pathogen's aftereffects and preventing future system harm. Several techniques have been used for detecting android malware applications. These techniques are pattern recognition detection, anomaly detection, rule based detection, misuse detection among others.

Android Malware Analysis

Android malware analysis is the analysis of android application to examine malicious contents. Android malware analysis is divided into dynamic and static analysis. Due to numerous obfuscation measures, static analysis has become ineffective. Dynamic analysis fills in the gaps left by static analysis (Adebayo & AbdulAziz, 2014). In the dynamic analysis, strategies such as monitoring changes to the system registry and inserting hooks into the system interface or library were utilised. Dynamic analysis, on the other hand, can be prone to substantial false negative and false positive rates because the heuristics are not based on the core properties of malware.

Static analysis statistically examines the code of program rather than really running it. This static analysis approach has the advantage of being able to analyse all of the code and possibly record the entire programme performance, liberated of any one pathway performed throughout execution time. Furthermore, the ability of statics analysis' to spot fresh malware or malware variants is limited.

Recent researches have to use the Dynamic and Static Analysis. Which involves both static and dynamic techniques in a simultaneous form to examine the malicious programs?

Concluding Remarks

The existing detection techniques used Particle Swarm Optimization inclusive Apriori Algorithm (Adebayo & AbdulAziz, 2014),with Apriori association analysis for its signature extraction (Muazzam *et al*., 2008) which was typified with drawbacks. Particle Swarm Optimization was utilised by the authors to optimise the development of candidate detectors (flag bearers), it will enhance the identification procedure by lowering false positives and enhancing true positives, a large number of Android applications were collected both malicious and benign. After a thorough study of program samples, the features from both samples were retrieved. To choose high-ranked features from the set of created features, three feature selection procedures were applied. The association rules were created using the features that were used to detect malicious Android applications (Adebayo & AbdulAziz, 2019).

References

1. Adebayo, O. S., & Abdul Aziz, N. (2019). Improved Malware Detection Model with Apriori Association Rule and Particle Swarm Optimization. *Security and Communication Networks*, *2019*, 1–13. https://doi.org/10.1155/2019/2850932q
2. Adebayo, O. S., & AbdulAziz, N. (2014). Techniques For Analysing Android Malware. *International Conference on Information and Communication Technology For The Muslims World (ICT4M) 2014*, 1–6.
3. Alqahtani, E. J., Zagrouba, R., & Almuhaideb, A. (2019). A Survey on Android Malware Detection Techniques Using Machine Learning Algorithms. *2019 Sixth International Conference on Software Defined Systems (SDS)*, 110–117. https://doi.org/10.1109/SDS.2019.8768729
4. Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, Yael Weiss "Andromaly": a behavioral malware detection framework for android devices". Journal of Intelligent Information Systems 38(1) (January 2011) 161{190}, 2011.
5. Christodorescu, M., Jha, S., Seshia, S. a., Song, D., & Bryant, R. E. (2005). Semantics-Aware Malware Detection. 2005 IEEE Symposium on Security and Privacy (S&P'05), 32–46. https://doi.org/10.1109/SP.2005.20
6. Department of Computer Science, Virtual University of Pakistan, & Tahir, R. (2018). A Study on Malware and Malware Detection Techniques. *International Journal of Education and Management Engineering*, *8*(2), 20–30. https://doi.org/10.5815/ijeme.2018.02.03

7. Dewanje, A., & Kumar, K. A. (2020). *A New Malware Detection Model using Emerging Machine Learning Algorithms*. I.J. of Electronics and Information Engineering, Vol.13, No.1, PP.24-32, Mar. 2020. http://.org/ 10.6636/ijeie.2021.03 13(1).04
8. Siddiqui, M. A. “Data Mining Methods for Malware Detection,” A dissertation submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Modeling and Simulation in the College of Sciences at the University of Central Florida, Orlando, Florida, 2008.
9. Thomas Eder, Michael Rodler, Dieter Vymazal, Markus Zeilinger “A Framework For Analyzing Android Applications”. Workshop on Emerging Cyberthreats and Countermeasures ECTCM 2013.