Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 79 (2015) 30702-30704

ISSN: 2229-712X

Review: malware detection systems in android

Sagar Aradwad, Sagar N Tulsani and Bhushan S Chaudhari
Sandip Institute of Technology and Research Centre.

ARTICLE INFO

Article history:
Received: 17 September 2014;
Received in revised form:
15 February 2015;
Accepted: 25 February 2015;

Keywords
Malwares,
Permissions,
Android.

ABSTRACT
Number of smartphones users is rapidly increasing. With this smartphones usage mobile malware attacks are also growing. Any malicious code or program used to access the information, gain the access or disrupt is known as malware. The developers of the malwares use the third party apps in order to inject the malicious contents into the phones and destroy the security. Various malware detecting tools are used to fight against these malwares. Malware detectors use various techniques for the detection of malwares. The main aim of this paper is to put light on the various malwares, malware detection, limitations and the various features involved.

Introduction

Usage of the Smartphone is increasing day by day. All these functionalities gives opportunities to the attackers to get attracted towards the smartphones. Smartphone use is now not just limited to personal conversation but has expanded to financial transactions, internet banking and for storing personal data. This results in the vulnerability of malware attacks with the target for information and identity theft. In year 2004[1], the researchers from Kaspersky Lab first found the malware for mobile phones. That malware was known as called Cabire. Thus from that time onwards the malwares in the phones increased largely depending on how popular that phone is. This paper mainly focuses on the mobile malwares and their analysis with various detection and prevention techniques.

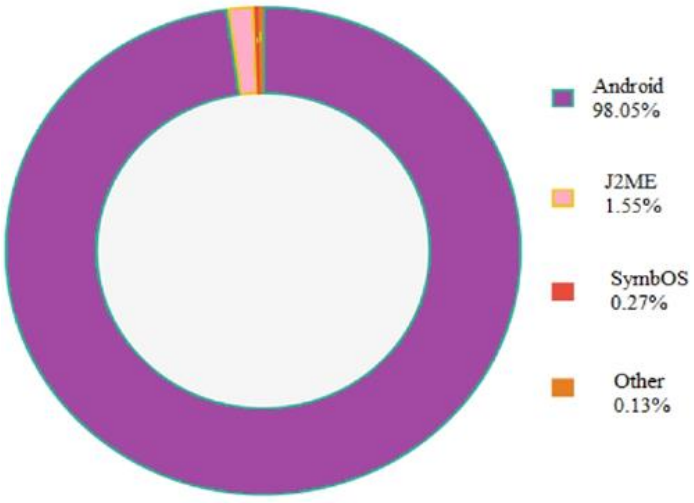

Fig 1: OS wise malware distribution [13]

Basic Terms

Malware

Legitimate services but they steal credentials in order to perform financial frauds. For an instance, recently there was one fake security app developed for Facebook,

It is the worldwide epidemic whose objective is to subvert the intended function. which assured that it would provide the security to the Facebook user's accounts, but rather have stolen the information of users.

Mobile Malware[11]

Malicious software targets the devices in order to Adware and Spywares damage or removes and changes the entire system. These malwares targeted the Symbian OS [1] in year 2004. Such nefarious codes installs themselves or sticks up and comes in with the package we are installing. Further thus they perform functions without the user's knowledge or permission. The goals of these mobile malwares are key logging, phishing, unwanted advertisements, spying, etc. [2].

Spyware is the thing which collects the information that is confidential. It collects all this information from the user secretly and transfers this information to the third party. They also might advertise the information and hence referred to as the' adware'. It mainly accesses the information like location, browsing history, messaging habits, contacts and the downloading preferences. As the hardware's information it accesses the version of the OS, IMEI number, IMSI number, product ID which can be used as weapons for further more haphazard.

Viruses and Trojans

Trojans in mobiles affects the devices by replicating themselves to smooth and unharmed programs. Thus later these Trojans which gets installed with the various apps carries the malicious actions.

Botnets

There is the great similarity between Trojans and the mobile viruses. Various third parties may use the malicious code in order to root the phone and gain the super authentication to access flash memory and various files.

Malwares mainly plays their role by affecting the programs that run in background. These malwares waits for the event to occur so that they can push themselves up into it and can do their intended tasks. They execute without letting the user know about their presence.

Applications that are Phishing

Similar to the PC attacks, the malware attackers creates the phishing apps for the mobile. These apps seem to be comes from the phase called as learning and the other

Tele:
E-mail addresses: sagar.aradwad@gmail.com

Who creates the malware?
input is the program under inspection.
Malware creators are also called as the hackers, crackers, or even the black hats. During the lifecycle of 5 Malware detection techniques the software there are two checkpoints were the malicious code can be inserted. They are pre-release phase and post release phase. The hacker inserts the internal threat into the code before the release of the software. Later, the other people from the organization may inject the malware at the post release phase of the software.

Malwares detection techniques can be broadly differentiated into two main types signature based and the anomaly based. Signature detection focuses on the characterization of the maliciousness of the code which is to be inspected. Whereas the detection technique based on the anomaly refers to the knowledge information of the code under inspection. Anomaly detection is also called as detection based on the specification. It deals with the specific specification or

Detectors of Malware

The malware detector shields the system by detecting malicious behavior. The malware detector performs its functions through various techniques. They accept two the particular set of rules to detect what is the valid behavior so as to decide the program's malware nature. Programs which violate the mentioned specifications inputs namely information of malicious behavior, which are treated as malicious.

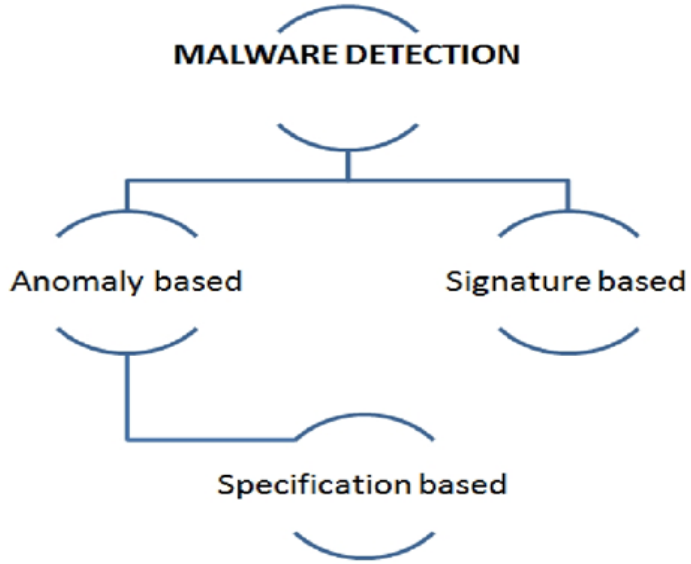

Fig 2: Types of malware detections techniques

Various markets

Smartphone users can download or buy the applications from various markets. Various Smartphones companies like Apple, Google, and Nokia focuses on the various markets for downloading various applications. Apple iOS phones permits the users using these phones to attacker gives the permissions while installation itself.

The permission system of Android is very extensive. Users often approve the permissions like access to contacts, Bluetooth, camera, messages, gallery, etc. install applications only from the Apple App Store [4], also applications in the App Store are rated by Apple

Dataset for Mobile malware

This is the review on various well known iOS, for security. In case the users wish to install the apps from the other markets then they have to do jail breaking of their devices. But there exists ample risk in this process as it violates the phone's warranty. In the same way Android provides their users with an official responsible to inject the spyware as the malware

Symbian, and Android malware, based on data which is gathered from public anti-malware databases. This section mainly focuses on the methodology and the literature survey.

Methodology Study

Allows its users for installing apps from unofficial stores, although they are warned that this may cause malware. For Nokia phones they have appstore called as Ovi. Ovi is the authorized and official markets from installing applications from other sources presently.

To find information about known mobile malware, the public databases of anti-virus companies is merged. The existence of each piece of malware is confirmed by at least two anti-virus vendors, and compared malware reports to identify cases where researchers had used different names for the same piece of malware. Main focus of this review is to collect statistics about

Related permissions

Smartphone prevents the users by alerting them before malware and the related work performed in past for the installing any sensitive information. Permissions are not same.

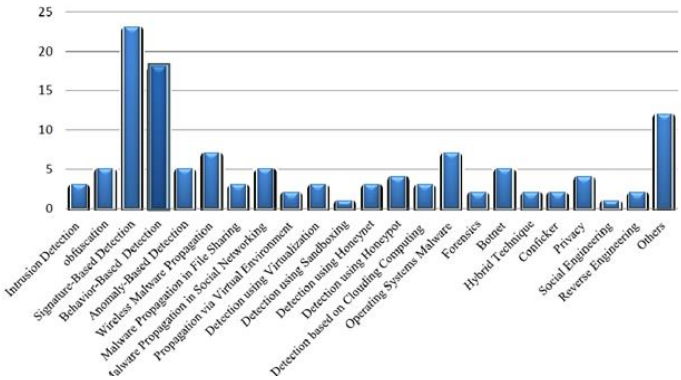

Fig 3: Statistical Survey Of Malware Detection Techniques [14]

Related work

Four malicious applications were developed to evaluate system calls. Crowdroid builds a vector of m features (the Android system calls). Another IDS that relies on machine learning techniques is Andromaly [3] which the ability to detect anomalies. MADAM: a Multi-Level Anomaly Detector for Android Malware [5] uses 13 features to detect android malware for both kernel level and user level. MADAM has been tested on real malware found in the wild and uses a global-monitoring approach that is able to detect malware contained in unknown applications, i.e. not previously classified. [6]MADAM is the framework which attempts malicious actions performed by real malware on Android platform. The framework exploits a multi-level approach i.e. that combines features at the kernel-level and at the application level, and is based upon machine learning techniques. The first prototype of MADAM for Android Smartphone has managed to detect all the 10 monitored real malware, with an impact on the user experience due to the few false positives issued per day. Crowdroid [2] is a machine learning-based framework that recognizes Trojan-like malware on Android smartphones, by analyzing the number of times each system call has been issued by an application during the execution of an action that requires user interaction. A genuine application differs from its trojanized version, since it issues different types and a different number of monitors both the smartphone and user's behaviors by observing several parameters, spanning from sensors activities to CPU usage. 88 features are used to describe these behaviors; the features are then pre-processed by feature selection algorithms. T Monitors smartphones to extract features that can be used in a machine

learning algorithm to detect anomalies. The framework includes a monitoring client, a Remote Anomaly Detection System (RADS) and a visualization component. RADS is a web service that receives, from the monitoring client, the monitored features and exploits this information, stored in a database, to implement a machine learning algorithm.[7] proposes a behavior- based malware detection system (pBMDS) that correlates user's inputs with system calls to detect anomalous activities related to SMS/MMS sending. [8][9] Propose Kirin security service for Android, which performs lightweight certification of applications to mitigate malware at install time. Kirin certification uses security rules that match undesirable properties in security configuration bundled with applications.[10] Performs static analysis on the executables to extract functions calls usage using various techniques.

Conclusion and Further Researches

Rapid increase is seen in phones these days. Android OS is the leading market. There are various testing methods available but it requires large scale of testing required. Users running our application will be able to see their own Smartphone behavior. They could even alert the users when one of their applications shows an abnormal trace. The system can also act as an early warning system, capable of detecting malicious or abnormally behaving applications in the early stages of propagation. There is a survey done on the behaviour of current mobile malware payloads. Presently, mobile malware is motivated primarily by a desire to send premium-rate SMS messages and sell information. There is also survey made on the permissions of Android malware. Android malware commonly requests the ability to directly send SMS messages, which is uncommon among non-malicious applications. Information more importantly user should be careful enough rather than blindly downloading an application.

Reference

[1] Trend Micro. "A Brief History of Mobile Malware".
[2] Dupaul, N. "Common Mobile Malware Types: Cyber security 101", Oct 2013.
[3] I. Burguera, U.Z., Nadijm-Tehrani, S.: Crowdroid: Behavior-Based Malware Detection System for Android. In: SPSM'11, ACM (October 2011)
[4] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, Y. Weiss: Andromaly: a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems 38(1) (January 2011) 161-190
[5] G. Dini, F.Martinelli, A. Saracino, D. Sgandurra: MADAM: a Multi-Level Anomaly Detector for Android Malware
[6] Schmidt, A.D., Peters, F., Lamour, F., Scheel, C., Camtepe, s.A., Albayrak, S.: Monitoring smartphones for anomaly detection. Mob. Netw. Appl. 14(1)(2009) 92-106
[7] Xie,L.,Zhang,X.,Seifert, J.P.,Zhu, S.: pBMDS: a behavior-based malware detection system for cellphone devices. In: Proceedings of the Third ACM Conference on Wireless Network Security, WISEC 2010, Hoboken, New Jersey, USA, March 22-24 2010, ACM(2010) 37-48
[8] Enck, W., Ongtang, M., McDaniel, P.: On lightweight mobile phone application certification. In: CCS '09: Proceedings of the 16th ACM conference on Computer and Communication Security, New York, NY, USA, ACM (2009) 235- 245
[9] Ongtang, M., McLaughlin, S., Enck, W., McDaniel, P.: Semantically Rich Application- Centric Security in Android. In: Computer Security Applications Conference, 2009. ACSAC '09. Annual.(Dec 2009) 340-349.
[10] Schmidt, A.D., Bye, R., Schmidt, H.G., Clausen, J.H., Kiraz, O., Yuksel, K.A., Camtepe, S.A., Albayrak, S.: Static Analysis of Executables for Collaborative Malware Detection on Android. In: Proceedings of IEEE International Conference on Communications, ICC 2009, Dresden, Germany, 14-18 June 2009, IEEE (2009) 1-5
[11] International Journal of Electronic and Electrical Engineering.
[12] ISSN 0974-2174 Volume 7, Number 7 (2014), pp. 717-722 International Research Publication House
[13] Literature Analysis on Malware Detection
[14] A Survey on Techniques in Detection and Analyzing Malware
[15] Executables International Journal of Advanced Research in
[16] Computer Science and Software Engineering
[17] Survey on mobile malware : A war without end International Journal of Computer Science and Business Informatics ISSN: 1694-2108 |vol. 9, No. 1. JANUARY 2014
[18] A SURVEY ON MALWARE PROPAGATION, ANALYSIS, AND DETECTION International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(4): 10-29. The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)