International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 03 - Issue 03 || March 2017 || PP. 102-105

Malware Detection Techiniques and Tools for Android Mobile – A Brief Review

Dr. Bhaskar V. Patil[#1]
[#1]*Bharati Vidyapeeth University Yashwantrao Mohite institute of Management, Karad [M.S.], INDIA*

Dr. Rahul J. Jadhav[#2]
[21]*Bharati Vidyapeeth University Yashwantrao Mohite institute of Management, Karad [M.S.], INDIA*

Abstract: Android has the biggest market share among all Smartphone operating system. The number of devices running with the Android operating system has been on the rise. By the end of 2012, it will account for nearly half of the world's Smartphone market. Along with its growth, the importance of security has also risen. Security is one of the main concerns for Smartphone users today. As the power and features of Smartphone's increase, so has their vulnerability for attacks by viruses etc. Perhaps android is more secured operating system than any other Smartphone operating system today. Android has very few restrictions for developer, increases the security risk for end users. Antivirus Android apps remain one of the most popular types of applications on Android. Some people either like having that extra security or just want to be extra cautious just in case and there is nothing wrong with that. In this list, we'll check out the best antivirus Android apps and anti-malware apps on Android!
The efficacies of these applications have not been empirically established. This paper analyzes some of the security tools written for the Android platform to gauge their effectiveness at mitigating spyware and malware.
Keywords: Virus, Security threats, Android smartphone security, Internet, Malware

I. INTRODUCTION

Now a day's android smartphone are very essential part of our life. The uses of android smartphone are increased day by day. Android is a modern mobile platform that is designed to be truly open source. Android applications can use advanced level of hardware and software, as well as local and server data, exposed through the platform to bring innovation and value to consumers. Android platform must have security mechanism to ensure security of user data, information, and application and network. [1]

A people can share information from one mobile to another mobile or another computer. In the current days there are various ways or method for sharing information because people can carry several gigabytes or terabyte of data from one destination to another destination. We also know history and which devices are used to exchange information in the world**.** In the process of exchanging the information using communication media there will be a problem of attack of malware or worms. A mobile virus is malicious software that targets mobile phones or wireless-enabled Personal digital assistants (PDA), by causing the collapse of the system and loss or leakage of confidential information. Viruses are capable of displaying different messages, denying all kinds of access, data thefts, changes in valuable data or files, deleting systems or any files, or it disable hardware. Therefore, an early detection and prevention mechanism is very important for the security of the mobile smart phones. Using Anti-virus software is a good way to detect viruses Anti-virus software is specifically written to defend a system against the threats that malware presents. Anti-virus software may work differently and ranges from large security packages to small programs designed to handle a specific virus.

The large number of Anti-virus software available in the market and some are being launched, each one of them offers new features for detecting and eradicating viruses and malware. Therefore people have a choice of different types of Anti-virus i.e. both in the form of freeware software or licensed software. People frequently change their Anti-virus software according to their liking and needs without evaluating the performance and capabilities of the various Anti-virus software available. Hence there is a need to find parameter for measuring performance of Anti-virus software for finding good and also suitable for the specific needs of the users.

II. ANDROID FUNDAMENTALS

Applications are programmed primarily in Java though the programmers are allowed to do native programming via JNI (Java native interface). Instead of running Java byte code, Android runs Dalvik byte code, which is produced by the application build tool chain from Java byte code. Dalvik is a virtual machine designed to run in low-memory environments and is similar to the Java Virtual Machine (JVM) with the most notable difference being that it is register based (JVM is stack based). Most of the JVM concepts

such as classes, class loaders, reflection, and so on are adopted as specified by the Java Language Specification in the Dalvik virtual machine. There are separate sections for keeping strings, class definitions, code items, and so on. Android applications are made of four types of components, namely activities, services, broadcast receivers, and content providers. These application components are implemented as classes in application code and are declared in the Android Manifest. The Android middleware interacts with the application through these components. Android application packages are jar files1 containing the application byte code as a classes.dex file, any native code libraries, application resources such as images, config files and so on, and a manifest, called Android Manifest. It is a binary XML file, which declares the application package name, a string that is supposed to be unique to an application, and the different components in the application. It also declares other things (such as application permissions) which are not so relevant to the present work. The Android Manifest is written in human readable XML and is transformed to binary XML during application build. Only digitally signed applications may be installed on an Android device. Application packages are signed similar to the signing of a jar file. Signing is only for the purpose of enabling better sharing among applications from the same developer and recognizing packages that come from the device vendor (such packages may have more privileges) and not verifying trust in the application.

III. ANDROID ANTI-MALWARE SOLUTIONS

With the proliferation of malware, there are now scores of both free and paid anti-malware products available in the official Android market. Many are from obscure developers while well established, mainstream antivirus vendors offer others. In order to get an insight on the workings of the antimalware products, we briefly describe the necessary parts of the Android security model. Android achieves application sandboxing by means of Linux UIDs. Every application (with a few exceptions relating to how applications are signed) is given a separate UID and most of the application resources remain hidden from other UIDs. Android anti-malware products are treated as ordinary third party applications and have no additional privileges over other applications. This is in contrast with the situation on traditional platforms such as Windows and Linux where antivirus applications run with administrator privileges. An important implication of this is that these anti-malware tools are mostly incapable of behavioral monitoring and do not have access to the private files of the application. The original application packages however remain intact and are readable by all applications. These application packages may thus be used for static, signature based malware detection. Moreover, Android provides a broad- cast when a new application is installed. All the anti-malware applications we study have the ability to scan applications automatically immediately following their installation, most likely by listening to this broadcast. Android also provides a Package Manager API, which allows applications to retrieve all the installed packages. The API also allows getting the signing keys of these packages and the information stored in their Android Manifest such as the package name, names of the components declared, the permissions declared and requested, and so on. Anti-malware applications have the opportunity to use information from this API as well for malware detection.

IV. MALWARE INFECTION METHODS

There are several methods that the Android devices could be infected with malware. The following are four different methods which malware can be installed on the phone:

1) Repackaging legitimate application - This is one of the most common methods used by the attackers. They may locate and download legitimate popular application from the market, disassemble it, add malicious code and then reassemble and submit the new apps to the official or alternative Android market. Users could be vulnerable by being enticed to download and install these infected applications. It was found that 86.0% repackaged legitimate application including malicious payloads after analyzing more than 1,200 Android malware samples.
2) Exploiting Android's - Application bug there could be a bug in the application itself. The attacker may use this vulnerability to compromise the phone and install the malware on the device.
3) Fake applications - It was also discovered that there are fake applications created to include malware which allows attacker to access your mobile device. Attackers upload on the market fake applications that seems are legitimate to users but they are malware by themselves. For example, Spyeye's fake security tool was found in the market which is a malware.
4) Remote Install - The malware could be installed in the user phone remotely. If the attacker could compromise users' credentials and pass them in the market, then in this case, the malware will be installed into the device without the user knowledge. This application will contain malicious codes that allow attacker to access personal data such as contacts list.

V. POPULAR DIFFERENT ANTIVRUS

"Precaution is better Than Cure", I'm firm believer of this quote; hope you understood my point of view. It is better to install one **best android antivirus** app before your smartphone running out of your hands. So to help you out guys we have listed some of the popular best antiviruses for Android. There are many viruses programmed for their harness, which replicates themselves and once it established, all data will be ruined. If you are smart and backup your Android phone, you'll regain the files, if doesn't it will shooting in the dark to get it back There are some best antivirus for android mobile to fight against these issues which are listed below.

1. **360 Security – Antivirus Boost** - This is one of the most popular and highly rated antivirus Android apps available right now with over 100 million downloads and 10 million ratings resulting in a 4.6 overall rating. This antivirus and anti-malware app comes with a ton of features, including the ability to scan your device files for malware, scan your apps and games, enable real-time protection, and even come with an anti-theft feature. You can also use the app's built in cleaner and booster service if you want, but the validity of those types of features aren't particularly substantiated. Perhaps the most useful feature for this one is an app lock that lets you password protects any app on your device which is great for keeping nosy people away

2. **AVG Antivirus FREE for Android** - As we all used the AVG antivirus in Windows/Mac, but AVG proved that it doesn't only work well on the desktop. You can scan and destroy the virus/malware and protect your smartphone from security threats. With AVG Antivirus app, you can scan all your Media files, Apps, APK files and other and kill without fail. Like CM security, you can find your stolen/lost smartphone that make it attract others. AVG packed with other essential features like App booster that exit the background app/service that consumes your memory as well as CPU. You can also use the AVG antivirus app to lock your phone from the anonymous attacks.

3. **AndroHelm Mobile Security -** AndroHelm's Mobile Security app is a lesser known option that can still provide a bunch of benefits. The main functionality focuses solely on security with features that include real-time protection from malware and spyware, scanning apps upon installation, frequent updates of the antivirus database, quarantine mode, app backups, virus protection, and a lot more. One of the more useful features include a set of functions that let you remotely block your device, delete stuff from it, and let you find your device in the cast of theft.

4. **Avira Antivirus Security** - Avira Antivirus Security is a relatively newer and lesser known antivirus app but it's quickly growing into one that people really seem to like. It comes with the basic stuff like device scanning, real-time protection, and even the ability to scan the external SD. It also includes modern features, like a Stagefright Advisor to help you work around that particular vulnerability. There is also some anti-theft feature, privacy features, blacklisting features, and device admin features.

5. **CM Security** - CM Security had some viral success back when it was one of only a few free antivirus Android apps and was, at the time, the best free option available. It has some competition now, but CM Security is still pretty decent when it comes to antivirus and anti-malware protection as it has been ranked very high on AV-TEST repeatedly for several years now. On top of its antivirus and anti-malware features, CM Security also includes one of the better app locks that we've used (it even has fingerprint scanner support now) that not only locks your apps, but takes selfish of people trying to nose around in your business.

6. **Lookout**- Lookout is a natural option for many users because this antivirus Android app comes installed on many Android devices (particularly those on T-Mobile in the United States). The free version is a bit more comprehensive than most and includes antivirus, anti-malware, and anti-theft protection although the paid version gives more of all of those things. Paid subscribers also get anti-theft alerts, real-time web browsing protection, a privacy adviser, and some data backup features. It's not a bad option and it's even lighter than many other security suites.

7. **McAfee Security and Power Booster** - McAfee is arguably one of the most recognizable names in the entire antivirus space and their Android app is finally high profile as well. There is virtually no difference between the free and paid version sans a few features so this is a great way to get a lot of protection for free although the paid version can get some pretty decent features like phone support and backup services. McAfee added a "power booster" into the app which has been the chic thing to do over the last year or so. McAfee too provides a lot of features for free just like other apps in this list. This app is actually locking your phone if any thieves try to uninstall it. Along with this, the app brings with it other features like anti-theft, web surfing protection, app locking and call blocking.

VI. CONCLUSIONS

In the past few years Smartphone users have increased quickly. There are attackers who are now targeting smart phones. The main reason for this because the lack of user awareness regarding how their devices can be compromised. Today, smart phones like Android are not just used as a portable telephone. Android devices can access the internet, make online bank transmissions, manage social networks, etc. All these functionalities of a mobile phone seem very attractive for an attacker to gain information of the user and use it to his/her benefit. Therefore, users need to be aware enough and have full responsibilities to read and understand the permissions requested by the application before agreeing to grant access.

VII. ACKNOWLEDGMENTS

The researchers are grateful to the authors, writers, and editors of the books and articles, which have been referred for preparing the presented research paper. It is the duty of researcher to remember their parents whose blessings are always with them.

VIII. REFERENCES

[1] Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh, Review on Android and Smartphone Security, Research Journal of Computer and Information Technology Sciences, Vol. 1(6), 12-19, November (2013), Page No- 12-19

[2] Yajin Zhou, Xuxian Jiang, "Dissecting Android Malware: Characterization and Evolution," Proceedings of the 33rd IEEE Symposium on Security and Privacy (Oakland 2012), San Francisco, CA, May2012

[3] Technology, "Architecture of Android OS" techneology.com, Nov 2011. [Online]. Available: http://www.techneology.com/2011/11/architecture-of-android-os.html.

[4] Android developer, Android-SDK. [Online]. Available: http://developer.android.com/sdk/index.html

[5] A Survey of Malware Detection Techniques, Nwokedi Idika, Aditya P. Mathur, Department of Computer Science, Purdue University, West Lafayette, IN 47907, Page 1 - 48

[6] A Survey of Malware Detection Techniques, Nwokedi Idika, Aditya P. Mathur A Survey on Android Malware and Malware Detection Techniques, Dhaval Baraiya Prof. Hiteishi Diwanji, *International Journal for Scientific Research & Development| Vol. 3, Issue 01, 2015, Page no 143-147*