International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8 Issue-8S3, June 2019

A Malicious Attacks and Defense Techniques on Android-Based Smartphone Platform

MA Rahim Khan, RC Tripathi, Ajit Kumar

Abstract:In this digital era after computer and internet smartphone is the third revolution and making ubiquitous computing possible. Android lead the smartphone market as most used operating system. This popularity of Android also makes it primary targets of cyber attackers and hackers. There are many different types of cyber-attacks targeted towards Andorid environment. In this review paper, we have investigated various attacks reported with respect to Android and have also gathered different type of defenses available to protect users from these attacks. This work is focus on accumulating various literature works available in this domain and provide a comprehensive representation of these works. The various works are grouped into two broad categories i.e. signature and non-signature based, and techniques mentioned in each work is studied and technical observations are made against them which help to understand the usability of these techniques. Such organized and details review work is required to study the problem in depth and works towards solution. The literature works are summarized and organized in proper table which help to visualized and easy comparison the information.

Keywords: Smartphone, Android

I. INTRODUCTION

Smart phones have been an integral part of our daily life. We use them to make calls, send messages, check emails, take photos, and surf the Internet every day. From year 2007 to 2018, a total of 7015 million units of smart phones were purchased by the end users, among which 84.2% of devices were powered by Android operating system [1]. The popularity of Android devices has, however, made them the most attractive targets for cyber- criminals. There are many different type of cyber-attacks which are targeted towards Android such as data theft, hacking etc. and technically malware acts as platform for many or most of these cyber-attacks.

Revised Manuscript Received on May 24, 2019.

MA Rahim Khan,Department of Computer Science, Lingaya's Vidyapeeth, Faridabad, Haryana 121002. India Email ID: khan_rahim@rediffmail.com

RC Tripathi, Department of Computer Science, Lingaya's Vidyapeeth, Faridabad Haryana - 121002. India Email ID: rctripathi@lingayasuniversity.edu.in

Ajit Kumar, Department of Computer Science, Sri Sri University, Cuttack, Odisha 754006. India Email ID: ajitkumar.pu@gmail.com

A report published by "Pulse Secure", it was reported that Android developed malware accounts for 97% of all mobile malware and due the large numbers users of Android operating system (OS) it is the most targeted OS in the among all other mobile and smart devices OS [2,6]. The malware infections are increasing rapidly in this decade. In near future the malware effects from individual to organization, which in turn affect the banking, email, transmitting the sensitive information and many more activity that will be disrupt by the malware.

Although Android is most targeted OS but the Android architecture has multi-layers security such as permission system, Linux kernel, certification etc. In this multi-layers security, permission plays important role and certification is also very crucial [3]. Apart from Android security, Google also provides security services to keep Android platform safe and secure from cyber attackers. Some of key services are explained in further sections.

1.1. Google services for Android Security

Along with Android intrinsic security, Google also try to provide extra security to Android devices and protect users by offering various services. Some of popular services are explained further in this section [4].

Google Play: Google Play is a service offered by Google which help Android users to find, install, and purchase apps for handheld devices running Android device. Google Play acts as a bridge between developers and potential users or buyers. It also help users to decide on a application by providing review, license verification, security scanning, and other security services.

Android updates: As discussed in aforementioned section there have been many known vulnerabilities in Android platform in past and which were patched time to time by developers. The different patches related to security or new features are deliver to end users by the Android update service using the web or over the air (OTA) as transmission medium.

Application services: Android also enhances user's experience by providing various cloud-based services such as back-up and notifications. Application Frameworks provides necessary infrastructure to Android applications to use these cloud services.

Retrieval Number: H10930688S319/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Verify Apps: Earlier we have discussed that Android is the main target of many cyber attacks and suspicious or/and malicious applications act as tool for many of these attacks. The verify apps service of Google help users to detect such malicious apps and provides proper option to take appropriate action such as blocking the installation. The service also continually scan the device for all installed apps and warn or help to remove suspicious or malicious apps.

SafetyNet: This is usually indirect user service and help to improve the safety and privacy of user. SafetyNet is a privacy preserving intrusion detection system (IDS) which assist Google to track and mitigate known security threats and identify new security threats.

SafetyNet Attestation: This is a third-party API which help Google to determine whether the device is Compatibility Test Suite (CTS) compatible or not and also help to identify source and destination of app communication (app to/from app server). For example, a rooted Android system is not consider CTS compatible by Google.

Android Device Manager: Google offer web-based device manager which help to locate lost or stolen Android device. The user have to registered and perform few initial configuration to utilize these services effectively.

Despite Android secure architecture and Google security services cyber attackers and malware writers are successful in past and continuously try to attack. The reason lies in the update and modification in attack method. For example, repacked Android application is one of recent attacks on Android platform which offers ways to launch malware and other cyber-attacks. In recent years several studied have been done which suggest the Android malware insert into the repackaged Android app by the hackers or developers. The popular apps usually infected by the repacking of the apps.

There are lot of techniques to detect the malware and also by the use of the commercial antivirus products, but the challenges take place while the android app initially downloaded from non-official app market. In further section, Android security updates and various Android based attacks are discussed and explained.

II. ANDROID SECURITY ENHANCEMENT AND ATTACKS

In the aforementioned section, we have listed that Android architecture and Google security services continuously offers the services to protect Android platform from cyber attackers but still attackers are successful. To investigate the reason of successful attack on Android platform it is important to understand the security enhancement. Table 1 list out the important security enhancement of various major Android version and total users share. One can observe clearly that Android developers have keep improving the Android version by version. This also indicates that different version of Android has vulnerabilities in past and that leads to cyber and malware attacks. Patching these vulnerabilities prevents attacks but there are always "zero-day" vulnerabilities which attackers discovers and forms attacks around the newly discovered "zero-day" vulnerability.

Table 1. Android version and increasing security features and users [Source: source.android.com/security].

Android Version	**Security Enhancement**	**Users Share (1-7 *May, 2019*)**
Android 1.5	ProPolice, safe_iop, OpenBSD dlmalloc and malloc	None
Android 2.3	No eXecute (NX), Linux mmap_min_addr, Hardware-based No eXecute	0.3%
Android 4.0	Address Space Layout Randomization (ASLR)	0.3%
Android 4.1	PIE (Position Independent Executable), Read-only relocations, dmesg_restrict enabled, kptr_restrict enabled	1.2%
Android 4.2	Verify Apps, control of premium SMS, Always-on VPN, Certificate Pinning, Improved grouped based display of Android permissions, installd, OpenSSL, FORTIFY_SOURCE	1.5%
Android 4.3	SELinux, Removing setuid/setgid, ADB Authentication, Capability bounding, AndroidKeyStore Provider	0.5%
Android 4.4	Per User VPN, AndroidKey store with ECDSA and DSA algorithms, Certificate Pinning,	6.9%
Android 5.0	Encrypted by default,Smart Lock,Multi user, restricted profile, and guest modes,Updated cryptography for HTTPS and TLS/SSL	14.5%
Android 6.0	Run time permissions, Verified Boot., Hardware-Isolated Security,Fingerprints, SD Card Adoption,System Hardening, Restriction on Clear Text Traffic, USB Access Control	16.9%

Retrieval Number: H10930688S319/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Android 7.0	File-based encryption,Direct Boot, Verified Boot,Kernel hardening, APK signature scheme v2,Trusted CA store, Network Security Configuration	19.2%
Android 8.0	Android Verified Boot (AVB), Sandboxing. Userspace hardening, Streaming OS update, Install unknown apps,Privacy	28.3%
Android 9.0	Biometric support,Dynamic analysis,Metadata encryption, StrongBox, 3DES support,Version binding, eSIM	10.4%

2.1 Attacks on Android-based Smartphone Platform

Android suffers most from the malware attacks but there are other cyber attacks which cause lot of harm to users. These attacks can be islotated cyber attacks or based upon use of malware as attack tool. Table 2 list out few of very popular cyber attacks targeted to Android platform. The data is money of today's digital era and so data theft is the top cyber attack targeted to Android.

Table 2. Different type of attacks on Android Environment.

Attack type	Description	Impact	Available Solutions
Data theft	Most of user of smartphone has many personal and financial information.	Direct loss in terms of money and reputation.	1. Verified apps 2. Anti-theft scanning 3. Monitoring
Identity theft	Smartphone is also being used as authentication for many online services using NFC, OTP etc. Attacker get access of mobile device and impersonate the user using their smartphone running Android.	Loss can be very huge and only limited with the attacker thought.	1. Avoid jail-breaking 2. Avoid suspicious apps 3. Monitoring
Remote Access	Attacker get access of smartphone and can proxy user's device to launch attacks or can perform any operation within device.	Innocent user can be convicted as attacker and the real attacker will be out of range.	1. Avoid jail-breaking 2. Avoid suspicious apps 3. Monitoring 4. Anti-malware
Blotware	Pre-installed application can be benign or malicious.	Resource consumption or depends upon the type of blotware.	1. Avoid suspicious apps 2. Monitoring

Every attacks on Android platform is dangerous for user but Malware is the top threats for Android. In further sections, a detail discussion on different type of Android malware and various defense techniques are discussed.

III. ANDROID MALWARE AND TYPES

Malware is a harmful software, which is used to bypass control to distract the functionality of any apps, find or gathering sensitive information without the knowledge of users. Moreover, harmful software is known as the badware. The categories of malware or virus, worm, trojan horse, rootkit, botnet, ransomware [5,6] etc. In the evolution of malware, first malware F-Secure [8] is a trojan horse for palm devices. First android devices malware was Fake player [10,11], which was launched in early august 2010, main aim of this trojan horse to immediately occupy the space in memory. As per application wise, first Russian android malware was ANDROIDS_DROIDSMS, it is a fraud application to send SMS by the premium rate. To track the GPS location, a game Tap Snake [12] trojan horse application was introduced, which is used hypertext transfer protocol queried by Global Position System (GPS) application.

First, IOS based malware was launched in august 2010, it takes the advantage of Secure Shell (SSH) password to replica other jailbroken iPhone devices [13]. Moreover, a report by Trend micro [14], mobile banking site effected Zeus malware to pass the two-way authentication technique. After that, day by day rapidly growth in android functionality, hacker taking the advantage of a vulnerability to hack the devices.

One of malware is DroidDream [15] , it can access the root of android devices, this types of malware not only gain International Mobile Station Equipment identity (IMEI) and International mobile Subscriber identity (IMSI) ,also install more obscure malware to get other information from devices. Google's release the google security tools to clean the devices, which is done by the malware writer, take the advantage and release different tools, by which cybercriminals gain information and find the backdoor activities. At present scenario, lot of malicious android apps are available, which is

Retrieval Number: H10930688S319/19©BEIESP
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

used send premium SMS, GPS location spyware and Google+ application to monitoring telephone conversation etc. Kaspersky [16] release a report, 1,319,148 malicious packages has been detected in mid-2017. Moreover, in year Q4 2016, Mobile ransomware was 200,054, ransomware rapidly growing in every past year to reached up to 3.5 million in 2017.Currently, RedDrop[18] is android based malware ,it have fifty three Androids application packages (APKS) , automatically download 7 more malicious application.

3.1. Types of malware

Virus: virus is a piece of code, which is replicate itself and dispersing across the application. Viruses spread through by attaching the executable file, propagate in the system by script code, document and week point into web application. The activity of viruses to create the command and control [26], the viruses do the attack to snip information, steal money, destroy the target host. Most popular example of viruses in android are Universal Cross-Site Scripting (UXSS) Attack, Malware Hidden in Downloaded Apps, Lasco, Command and Control (C & C) [26], CardBlock, CardTrap Android Installer Hijacking and crossover[27] are example of viruses .

Worm: worm is a piece of code, ability of replication and disperse across the network from devices to device without human intervention [26]. Inside the worm, contain the "payload" that destroy the network host, the target of worm to trouble the networks bandwidth by creating congestion on the web server. Moreover, worm take the advantage of "payload" to theft information, delete files from target system. The main techniques of spreading worm across the network through opening infected email attachment. The most popular example of the worm in anroid is ADB.Miner Android [Gdata link].

Trojan: It is the type of Malware, show itself in opening of web application to download and install. Attacker steal information, modify file, keep monitoring the activities of user and logs by using the remote the access the target host. The most popular example of trojan are MasterKey, FakePlayer, GantSpy[25], DownAPK[15] etc.

Spyware: It is the type of malware, which is used to monitor the user activities without user acceptance. Attacker collection key logs, steal account information etc. Exploit vulnerabilities is the most import goal of Spyware. Most important example of spyware in Android is RedDrop[17]

Ransomware: It is the type of malware, which is used to lock the computer resources until the victim must pay crypto currency. After payment ransom malware will get rid of from system. In Year 2017 of semantic report [18, 32], declared 36% increase in Ransomware attack and introduce the hundreds of new malware variants. Most popular Android malwares are Xbot, Simpllocker FakeDefender and adultPlayer [33].

Botnet: It is a piece of code that is used to compromise the device to create the bot, so that remote server to control the device without user's consent, called Bot-Master. Bot-Master control the number of devices. Botnet is the Distributed denial of services attacks, hack the server data by web spider, gather information by spam bots. Most popular example of Botnet in Androids are Geinimi, Beanboot and DoubleDoor[29].

Rootkit: It is the type of malware to gain remote access and controls on the device. Rootkit gain administrative access to run various malicious apps to steal the information, do the harmful action and edit the system configuration. Rootkit hide itself into the system, it remains into the system for long period of time with help of obfuscation. Most popular example of Rootkit in Androids are Godless, HummingBad and Checkpoint [28].

Backdoor: Most dangerous malware is the Backdoor malware, which is used to open the backdoor for other malware, it can open the any port for other application. In the simplest way, backdoor open the vulnerability for another malicious program. Most popular example of Backdoor malware is Brador[34] .

Key-loggers: Basically Key-Loggers is program, which is install on victim system. This type of malware maintains the records of Key-Stork, whatever the user does any activities by keyboard, records in Key-Loggers program. Most common Key-Logger Malware in Android are FlexiSpy[35], mSpy.

3.2. Popular Android Malware

In the aforementioned section Android malware and different class/type of malware are discussed. There were many popular cases of Android malware in past which either causes huge losses to user or get attention from cyber world. In the Table 3, some of popular Android malware (2010-2018) are listed with its type and brief description. From the table it can be observe that Android malware are active since 2010 and are evolving over time with advance threats such as ransomware etc.. It also demands that security solutions must be evolve along with attackers and should be ahead of attackers.

Retrieval Number: H10930688S319/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

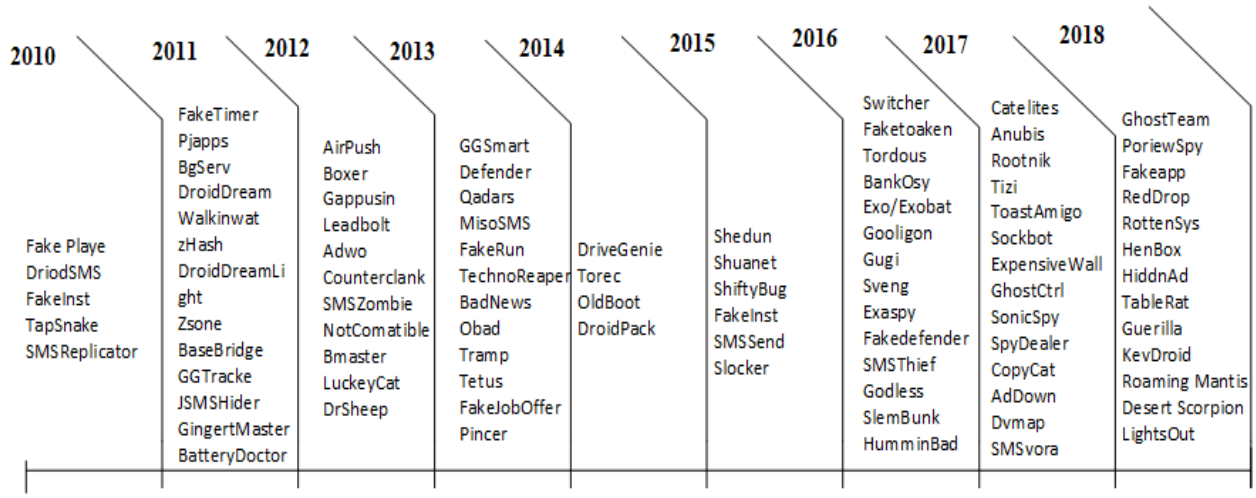

Figure 1. Android Malware timeline.

Table 3. Evolution of Malware 2010-2018.

Year	Name Malware	Type	Description
2010	FakePlayer[10]	Trojan	First Trojan malware, which is used to send the premium rate of SMS messages.
2010	DroidSMS[36]	Trojan	Identified in august 2010, this is the first fraud malware apps that send SMS with premium rate with user consent.
2011	GoldDream[37]	Botnet	This have the capability of bot malware; it has ability to command and control (C &C) server to exploit the root.
2011	DroidDream[19]	RootKit	This is RootCager malware, ability to exploit the root privileges, first market android malware.
2012	Bmaster	Botnet	This is third party app, once installed, theft the sensitive data from devices, such ID,IMEI , GPS DATA etc.
2012	Defender	Ransomware	Defender is first ransomware in Android, once install this malware, user paid $99.99 to access the device.
2013	FakeRun	Adware	This malware did not steal any personal information, used to ads and share on Facebook account.
2013	BadNews	Adware	This is repacked malware, masqueraded as an ads on networks,
2014	OldBoot	Backdoor	This is malware have the ability to reinstall itself , installed malware ,open the backdoor in device.
2014	DrioidPack	Trojan	This is first malware that transfer from windows to android devices. Once installed, attempted to uninstall legitimate bank app and asked to user for authentication to steal info.
2015	FakeInst[39]	Trojan	This malware used the repackaged clone technique
2015	Gazon[15]	Virus	This malware is spread itself via text message, send a hyperlink to win prize of $200
2016	HumminBad[28]	Virus	The main aim of this malware to generate the ads-based revenue, gain access the root, control over device to steal personal and private info.
2016	Godless[21]	Rootkit	This malware is open source framework to access root privileges. Once Install app, cause ads annoying app.

2016	FakeDefender[33]	Trojan	Fake defender is trojan's malware, use to display the fake security alert message to influence user to purchase an app to remove the security risk.
2017	BadRabbit[23]	Ransomware	Basically, this malware is ransomware family, dropper spreads this malware through Drive by Attacks. Dropper program on victim computer are install secretly to help known malicious programs to evade detection
2017	Judy[24]	Adware	"Judy" is an auto-clicking adware which was found on 41 apps developed. Infected devices to generate large amounts of fraudulent clicks on advertisements, generating revenues.
2018	RedRop[18]	Spyware	This malware is known as the Zero-day threat. Fifty-three malware- ridden apps are exfiltrating sensitive data – including audio recordings, Dropbox accounts to prepare for further attacks and extortion purposes
2018	GhostTeam[38]	Adware	The GhostTeam loads malicious JavaScript code that harvests the user's Facebook login credentials. This data is later sent to a remote server under the attackers' control. GhostTeam publish ads on social web site to earn the money.

After discussing about Android malware, its type and few of popular Android apps, it is important to understand the current state of anti-malware techniques. In further section, different anti-malware techniques from literature are listed and explain in detail.

IV. ANDROID MALWARE DETECTION TECHNIQUES

In the literature there are many Android malware detection techniques which can be broadly classify in two main groups , 1) Signature-based detection and 2) Non-Signature-based detection. These detection techniques can also be group on the based-on type of analysis i.e. static or dynamic analysis. In further section, these techniques are explained in details with the support of available literature works.

4.1. Signature based detection

Signature-based detection uses the signature to detect malicious programs. Signature is a sequence of bytes extracted from previously known malware. Static signature-based detection does not run the program whereas dynamic signature-based detection executes the program in a safe environment and checks for the signature [9] .

Signature-based detection gives higher accuracy for known malware but totally fails when encountered with the "zero-day" and "unknown" malwares. The Signature-based detection is also limited to the signature database which demands a regular update of newly created signatures and storing the signature database at end-host requires space proportional to the number of signatures.

DroidEagle, is a methodology which uses the layout resources within an app to detect apps which are visually similar [40]. DroidEagle has two subsystems RepoEagle and HostEagle which is use to scan and detect visually similar applications in apps repositories and host machine respectively.

Authors of a recent work have proposed OpSeq that calculate similarity scores based on normalized opcode sequences and app permission requests [42]. According to authors combination of structural and behavioral features creates a distinctive fingerprint for a given Android application and improve overall recall rate of OpSeq. It is a signature-based method works against obfuscation techniques but can only detect known malware.

DroidMOSS, is a system to measure similarity by using fuzzy hashing technique to effectively localize and detect repacked applications [40, 48]. In this work, authors performed a systematic study of six popular third party Android app market and found out that 5% to 13% of apps hosted on these third party marketplaces are repackaged to achieved various purposes such as stealing or re-routing ad revenues and injecting different kind of malware.

Context triggered piece-wise hash (CTPH) is used twice (T-CTPH) to generate two fingerprint of each application to detect repacked application [45]. Authors also optimize the hash similarity calculation algorithm which optimize the efficiency of process.

Recently, Vidal et all (2018) proposed a dynamic detection of malware in Android apps[51]. In this dynamic technique have the advantage to reduce the computation cost, because it is based on comparison of sequences in a large amount of information. The result obtains by applying the boot sequence to reduce the search space at pattern recognition eventually denied the malicious application install. this pattern recognition system working based on monitoring, analysis and decision making.

Gurulian et al (2016) proposed a fast and application store agnostic approach in which the adversary cannot the significantly plagiarized the elements without the substantially minimizing the attack potential[42]. In this approach the detection process can be initiated from the client side, prior to an installation. The approach is effective when the attacker only copy the name and icon of the android application.

Gadyatskaya et al (2016) attempt to fill the gap between the resource based repackaging detection and the implementation of the technique and observe that the resource-based approach detection

Retrieval Number: H10930688S319/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

approach is very useful to detect the plagiarized applications [52]. The experiment results show that the technique is effective if the separately different types of files. Generally, in repackaging the multimedia files, libraries, raw resources and images are least frequently changed in repackaging, while the main dex code _file, the manifest _file and the compiled resources (e.g., strings) are the most frequently changed resource file types.

Prevalent usage of obfuscation in Android malware has also cast doubt on the reliability of most Android malware analysis tools [42,43], and, in particular, static ones. The majority of these tools rely upon some static features which are obtained from the source code and are severely impacted by little transformations in the source code [43]. Consequently, they are not resilient to transformation attacks. Also, obfuscation has turned out to be a new barrier to protect Android users [44], and, therefore, detecting obfuscation is critical in understanding the underlying semantics of malware specimens.

4.2. Non-Signature based detection

Non-Signature-based detection, is capable of overcoming the limitations of signature-based detection. The non-Signature-based detection does not use malware specific signature. In this detection method a normal profile is developed and any diversion from normal profile is treated as malicious.

Now a day's Artificial intelligence [AI] which includes the term machine leaning and deep learning played an important role in cybersecurity. The attackers try to use the AI in the cybercriminals activity to exploit the user and the developer of the android application. The AI is played a significant role in the detecting the android malware. The permissions and intents information are declared and stored in manifest file of each Android application. Many of earlier works have used permissions and Intents as feature to build malware classifiers or any other ML based classifiers (Di Cerbo et al.[54], 2010; Geneiatakis et al.[53], 2015; Sanz et al.[55], 2012).

In CLANdroid, authors have uses Information Retrieval techniques and five semantic anchors: identifiers, Android APIs, intents, permissions, and sensors to detect similar apps [46,50]. CLANdroid is mainly focused on detection of similar app which need not to be a repacked app,for example similarity is, searching similar apps for car booking service and repacking is distributing same game apps by changing developers details or replacing advertisement channel code etc.

V. RESULTS AND DISCUSSIONS

In one of the work, authors have proposed technique to measure app similarity based on claimed behavior [47]. Raw features were extracted using information retrieval method and then augmented with ontological analysis and used as attributes to characterize apps. Agglomerative hierarchical clustering method were used to cluster the apps. Experiments were carried out on 17,877 apps mined from BlackBerry and Google app stores. Proposed method improves the existing categorization quality from 0.02 to 0.41 and from 0.03 to 0.21 for Blackberry and Google stores respectively.

Table 4. Different Techniques and methods for Detecting Android Malware.

Works	Techniques	Observations
DroidEagle [41]	layout resources tree	Static method, Tree comparisons is costly
OpSeq [42]	sequence of opcode and permissions requests	Static method, work only for known malware
DroidMOSS [40]	Fuzzy hashing	Can not handle Obfuscation
TaintDroid [56]	Realtime dynamic taint	Dynamic, It uses some basic data ow rules to track the movement of tainted variables, method files and IPC messages from sources until they reach a specified Java library sink.Depends on Dalvik virtual machine
RiskRanker [57]	systematic approach	application based on native code, dynamic class loading, and callback handlers, discover if dangerous behavior is present,
SCanDroid [58]	security certification tool	application manifest match what is requested within the app's components, discover if dangerous behavior is present
DroidRanger[59]	permission-based behavioral fingerprinting	benign apps tend to request combinations of permissions, discover if dangerous behavior is present

Retrieval Number: H10930688S319/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

CrowDroid [60]	application based on logs collected	limited to extracting only Linux-speci_c information like open files, IPC and Android specific data.
DroidScope [61]	virtual machine introspection	API tracing, native instruction and Dalvik tracing, and taint tracking.

Aforementioned section presented a detailed discussion about different techniques and methods for detecting Android malware. There have been so many techniques to defend Android from malicious attacks but due to inherit limitations of some of techniques and advancement of attacker's attack there is a need for innovative techniques to defend Android platform. In further section we have presented our conclusion and listed the future scope.

V1. CONCLUSION

In this review work, we have discussed a very crucial cyber threats of Android security and Android malware. We have discussed the Android security and Google services for securing Android platform. A detailed discussion about Android malware types and popular Android is presented. Based upon available literature various defenses i.e. signature and non-signature based detection against Android malware is also discussed in-depth. Many of these techniques are successful to defend against Android malware but most of them are either specific to Android malware type or solve a specific problem. Some of techniques have inherit limitations such as signature-based detection can not detect "zero-day" based malware, some are limited with the resource consumption which is very important for smartphone. In this work we have listed few selected works so in future review work a high number works can be discussed on various parameters. A sample test result of various techniques based on a standard malware dataset can be also published after setting various experiment which will present a clear status of those techniques and will help to compare and select right techniques.

REFERENCES

1. https://www.gartner.com/en/newsroom/press-releases/2018-02-22-gartner-says-worldwide-sales-of-smartphones-recorded-first-ever-decline-during-the-fourth-quarter-of-2017 [Last Accessed: 20-05-2019]
2. https://www.pulsesecure.net/download/pages/2819/ [Last Accessed: 20-05-2019]
3. [3] Kumar, A., Kuppusamy, K. S., & Aghila, G. (2018). FAMOUS: Forensic Analysis of Mobile devices Using Scoring of application permissions. Future Generation Computer Systems, 83, 158-172.
4. https://source.android.com/security/index.html [Last Accessed: 20-05-2019]
5. Attia Qamar, Ahmad Karim, Victor Chang. (2019) "Mobile malware attacks: Review, taxonomy & future directions" , Future Generation Computer Systems, pp 887-909 .
6. Li Zhang, Vrizlynn L. L. Thing, Yao Cheng:A scalable and extensible framework for android malware detection and family attribution. Computers & Security 80: 120-133 (2019).
7. P. Yan, Z. Yan, A survey on dynamic mobile malware detection, Softw.Qual. J. (2017) 1–29.
8. K. Ohlson, First palm virus found, 2000, 25 September, 2000 12:01;Available from: https://www.computerworld.com.au/article/78795/first_palm_virus_found/.
9. Ajit Kumar, K.S. Kuppusamy, G. Aghila. "A learning model to detect maliciousness of portable executable using integrated feature set", Journal of King Saud University -Computer and Information Sciences, 2019
10. Symantec, AndroidOS.FakePlayer, 2018, 3/21/2018; Available from: https://www.symantec.com/security_response/writeup.jsp?docid=2010-081100-1646-99.
11. B. Irinco, First android trojan in the wild. August 10, 2010, Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/first-android-trojan- in-the-wild/
12. S. Perez, Tap snake game in android market is actually spy app (update).August 17, 2010, Available from: https://readwrite.com/2010/08/17/tap_snake_game_in_android_market_is_ actually_spy_app/.
13. G. Cluley, First iphone worm discovered – ikee changes wallpaper to rick astley photo. 08 NOV, 2009, Available from: https://nakedsecurity.sophos.com/2009/11/08/iphone-worm-discovered-wallpaper-rick-astley-photo/.
14. J. Leopando, Zeus now bypasses two-factor authentication, 2010, Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/zeus-now-bypasses-two-factor-authentication/.
15. J. Zorabedian, Check out this infographic showing the history of mobile threats, 2004–2015, 2015, 19/05/2015 3/21/2018; Available from: https://news.sophos.com/en-us/2015/05/19/check-out-thisinfographic-showing-the-history-of-mobile-threats-2004-2015/.
16. R. Unuchek, IT Threat evolution Q2 2017, Statistics (2017).
17. N. Campbell, Reddrop: the blackmailing mobile malware family lurking in app stores, 2018, Available from: www.wandera.com/blog/reddropmalware/.
18. B. Brenner, 2018 malware forecast: ransomware hits hard, continues to evolve, 2017, 3/21/2018; Available from: https://news.sophos.com/enus/2017/11/02/2018-malware-forecast-ransomware-hits-hard-crossesplatforms/.
19. G. Certifications, Global information assurance certification paper, 2018, 3/21/2018, Available from: https://www.giac.org/paper/gsec/329/libertycrack-first-palm-os-trojan-horse/100917.
20. K. Dunham, Mobile malware attacks and defense, in: Syngress, 2008.
21. M.T.i. Power, Virus profile: Wince/infojack, 2018, 3/21/2018; Available from: https://home.mcafee.com/virusinfo/virusprofile.aspx?key=144191.
22. V. Zhang, 'Godless' mobile malware uses multiple exploits to root devices, 2016, June 21, 2016 3/21/2018; Available from:https://blog.trendmicro.com/trendlabs-security-intelligence/godlessmobile-malware-uses-multiple-exploits-root-devices/.
23. M. Kumar, Bad rabbit: New ransomware attack rapidly spreading across Europe, 2017, Tuesday, October 24, 2017 3/21/2018; Available from: https://thehackernews.com/2017/10/bad-rabbit-ransomware-attack.html.
24. C.P.M.R. Team, The judy malware: Possibly the largest malware campaign found on google play, 2017, Available from: https://blog.checkpoint.com/2017/05/25/judy-malware-possibly-largestmalware-campaign-found-google-play/.
25. E. Xu, New gnatspy mobile malware family discovered, 2017, Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/new-gnatspy-mobile-malware-family-discovered/.
26. N. DuPaul, Common malware types: Cybersecurity 101, 2012, OCTOBER,12, 2012 3/21/2018; Available from: https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101.
27. M. La Polla, F. Martinelli, D. Sgandurra, A survey on security for mobile devices, IEEE Commun. Surv. Tutor. 15 (1) (2013) 446–471.
28. Koriat A.P.a.O., Hummingbad: A persistent

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

mobile chain attack, 2016, Available from: https://blog.checkpoint.com/2016/02/04/hummingbad-apersistent-mobile-chain-attack/.
29. NJCCIC, Botnets, 2018, Available from: https://www.cyber.nj.gov/threatprofiles/botnets/ #LIST-OF-KNOWN-BOTNETS.
30. RISKIQ, The Q4 2017 Mobile Threat Landscape Report, 2017.
31. NJCCIC, 2018, Available from: https://www.cyber.nj.gov/search?q=adware&f_collectionId =577f9817f7e0abcffe31befe.
32. Symantec, ISTR Internet Security Threat Report, 2017.
33. J. Buntinx, Top 4 types of android ransomware, 2017, January 20,2017; Available from: https://themerkle.com/top-4-types-of-androidransomware/.
34. F-Secure, Brador. Available from: https://www.f-secure.com/v-descs/brador.shtml.
35. Symantec, Spyware.flexispy, 2018, cited 2018; Available from: https://www.symantec.com /en/sg/ security-center/writeup/2006-033012-3337-99.
36. "DROIDSMS". Trend Micro Threat Encyclopedia. Available: http://about-threats. trendmicro.com/us/malware/androidos_droidsms.a.
37. Symantec, Android.Golddream Available from: https://www.symantec.com/security-center/writeup/2011-070608-4139-99
38. Kevin Sun, Security Intelligence , Available from: https://blog.trendmicro.com/trendlabs-security-intelligence/ghostteam-adware-can-steal-facebook-credentials/
39. F-Secure Lab , Available from: https://www.f-secure.com/v-descs/trojan_android_fakeinst_ hb.shtml.
40. M. Sun, M. Li, and J. Lui. Droideagle: seamless detection of visually similar android apps. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, page 9. ACM, 2015.
41. Li, Li, Tegawendé Bissyandé, and Jacques Klein. "Rebooting Research on Detecting Repackaged Android Apps: Literature Review and Benchmark." arXiv preprint arXiv:1811.08520 (2018).
42. Gurulian, I., Markantonakis, K., Cavallaro, L., & Mayes, K. (2018). Reprint of "You can't touch this: Consumer-centric android application repackaging detection". Future Generation Computer Systems, 80, 537-545.
43. Kohli, Ayush. "ESEC/FSE: U: DecisionDroid: A Supervised Learning-Based System to Identiy Cloned Android Applications." (2018).
44. Martín, Ignacio, and José Alberto Hernández. "CloneSpot: Fast detection of Android repackages." Future Generation Computer Systems 94 (2019): 740-748
A. Ali-Gombe, I. Ahmed, G. G. Richard III, and V. Roussev. Opseq: Android malware fingerprinting. In Proceedings of the 5th Program Protection and Reverse Engineering Workshop, page 7. ACM, 2015.
45. M. Linares-V´asquez, A. Holtzhauer, and D. Poshyvanyk. On automatically detecting similar android apps. In 2016 IEEE 24th International Conference on Program Comprehension (ICPC),pages 1{10. IEEE, 2016.
A. Al-Subaihin, F. Sarro, S. Black, L. Capra, M. Harman, Y. Jia, and Y. Zhang. Clustering Mobile Apps Based on Mined Textual Features. In Proc. of the 10th International Symposium on Empirical Software Engineering and Measurement, ESEM'16, Sept. 2016.
46. W. Zhou, Y. Zhou, X. Jiang, and P. Ning. Detecting repackaged smartphone applications in third-party android marketplaces. In Proceedings of the second ACM conference on Data and Application Security and Privacy, pages 317-326. ACM, 2012.
47. Qin, Zhongyuan, Xinshuai Zhang, Qunfang Zhang, and Zhongyun Yang. "An efficient method of detecting repackaged android applications." (2014): 056-4 IET.
48. Mario Linares-Vasquez, Andrew Holtzhauer,Denys Poshyvanyk. "On automatically detecting similar Android apps", 2016 IEEE 24th International Conference on Program Comprehension (ICPC), 2016.
49. Vidal, Jorge Maestre, Marco Antonio Sotelo Monge, and Luis Javier García Villalba. "A novel pattern recognition system for detecting Android malware by analyzing suspicious boot sequences." Knowledge-Based Systems 150 (2018): 198-217.
50. Gadyatskaya, Olga, Andra-Lidia Lezza, and Yury Zhauniarovich. "Evaluation of resource-based app repackaging detection in android." In Nordic Conference on Secure IT Systems, pp. 135-151. Springer, Cham, 2016.
51. Geneiatakis, Dimitris, Gianmarco Baldini, Igor Nai Fovino, and Ioannis Vakalis. "Towards a mobile malware detection framework with the support of machine learning." In International ISCIS Security Workshop, pp. 119-129. Springer, Cham, 2018
52. Di Cerbo, Francesco, Andrea Girardello, Florian Michahelles, and Svetlana Voronkova. "Detection of malicious applications on android os." In International Workshop on Computational Forensics, pp. 138-149. Springer, Berlin, Heidelberg, 2010.
53. Sanz, B., Santos, I., Laorden, C., Ugarte-Pedrero, X., Bringas, P.G. and Álvarez, G., 2013. Puma: Permission usage to detect malware in android. In International Joint Conference CISIS'12-ICEUTE 12-SOCO 12 Special Sessions (pp. 289-298). Springer, Berlin, Heidelberg.
54. DroidBox. Droidbox - Android Application Sandbox, 2011. [Online; accessed 01-July-2015].
55. Fuchs, A. P., Chaudhuri, A., and Foster, J. S. Scandroid: Automated security certi_cation of android applications. Tech. rep., University of Maryland,2009.
56. Grace, M., Zhou, Y., Zhang, Q., Zou, S., and Jiang, X. Riskranker:Scalable and accurate zero-day android malware detection. In Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services (New York, NY, USA, 2012), MobiSys '12, pp. 281-294.
57. Zhou, Y., Wang, Z., Zhou, W., and Jiang, X. Hey, you, get off of my market: Detecting malicious apps in official and alternative android markets.In Proceedings of the 19th Network and Distributed System Security Symposium (2012), NDSS '12.
58. Burguera, I., Zurutuza, U., and Nadjm-Tehrani, S. Crowdroid:Behavior-based malware detection system for android. In Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (2011), SPSM '11, pp. 15-26.
59. Yan, L.-K., and Yin, H. Droidscope: Seamlessly reconstructing the os and dalvik semantic views for dynamic android malware analysis. In USENIX Security Symposium (2012), pp. 569-584.

Weblinks:

1. https://source.android.com/security/enhancements/enhancements41
2. https://developer.android.com/about/dashboards
3. https://www.gdatasoftware.com/news/2018/06/30855-critical-vulnerability-first-android-worm-discovered
5.https://nakedsecurity.sophos.com/2019/05/13/study-finds-android-smartphones-riddled-with-suspect-bloatwar

Retrieval Number: H10930688S319/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication