International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Android Ransomware and Its Detection Methods

Manish Kaushik, Leena Bhatia, Vipin Kumar Jain

Abstract: Ransom ware is the most dangerous malware which locks the entire system data (files/folders) of user and demands ransom form user in order to decrypt data. Ransomware attacks are increasing day by day. Mobile phones are used not only for communication purpose but users also store their personal data and many other things in their mobile phone. 80% to 87% mobile phones are using Android operating system. Attackers have also targeted android smartphones just like personal computers. Due to rapid increase in ransomware we need to develop effective solution. There are different approaches like static, dynamic and hybrid which are used to detect ransomware.

Keywords: Ransom ware, Static, Dynamic, Hybrid approach.

I. INTRODUCTION

Nowadays user stores each and every type of data whether it is personal or sensitive, in smartphones. There are large numbers of applications available on google play store as well as third party applications like fitness, news utility, books, movies, entertainment music etc. that provide confidentiality and save human‘s time. Android, is one of the largest open source mobile operating system. Android also give permission to install applications from unknown sources and due to globalization and fragmentation of Android, it has become the famous target for attackers. One out of thirty-six mobile had high risk application installed [1].

Table 1. Smartphone’s operating system market share. [2]

Year	2017	2018	2019	2020
Android	85.1%	85.1%	86.6%	86.6%
iOS	14.7%	14.7%	13.4%	13.1%
Other	0.2%	0	0	0

There are different versions of Android available in the market out of which 10.4% of mobile devices use the latest version of Android 9.0-Android Pie [3] so that the user get protected from new security threats, while the other users (15.4% users – Oreo 8.1, 10.9% - Oreo 8.0, 7.9% users-Nougat 7.1, 11.4% users Nougat 7.0 and remaining users uses older android versions) are still using older android versions because they are not getting newer security updates Ransomware can easily target them.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Manish Kaushik*, Principal & Professor, Department of Computer Science, S. S. Jain Subodh P. G. College, Jaipur, India.
Leena Bhatia, Associate Professor, S.S. Jain Subodh P.G. College, Jaipur, India.
Vipin Kumar Jain, Assistant Professor, Department of Computer Science, S. S. Jain Subodh P. G. College, Jaipur, India.

In today’s world large numbers of users are switching from ATMs/Cash transactions to mobile banking with the help of their smartphones. That’s why different type of malware attacks preferably on Android smartphones. In 2013 a malware was found named Ransomware that locks the data and demands money from user at the expense of personal files/folders [4].

Recently DoubleLocker ransomware attacks on victim’s smartphone it changes device pin and encrypt all data store in mobile. And it is impossible for user to access data without paying ransom. According to the Symantec Internet security threat report [1] published in 2019 mobile ransomware infection increased by 33% as compared to 2017. Mobile ransomware nastiest affected U.S., (63%), China (13%) and Germany (10%). Presently managing mobile device security continues to challenge for any organizations. In 2018, one out of thirty-six devices used in organizations were at high risk. Android user install unknown source applications other than Google play store applications. Attackers give temptation when user either download and install unknown source applications then they present themselves as paid applications for free, or show applications to boost your system performance, etc. In 2019 annually damage due to ransomware attacks globally reaches to $ 11.5 billion.

There are two forms of ransomware:

- Locker Ransomware (Lock Screen Ransomware)
- Crypto Ransomware (File Encryptor Ransomware)

WinLocker ransomware also known as lock screen ransomware. It just locks the screen of smartphone without encrypt the personal files and demands ransom to unlock the mobile. But Crypto ransomware encrypts the mobile phone files and folders. After encryption of data user is came to know that his all data is encrypted and attacker demands ransom [5] to decrypt data in smartphone.

In 2014 popular mobile ransomware was CryptoLocker and other similar families. After that there will be a large increase in mobile ransomeware. These ransomwares generally display a message on smartphone screen that system is locked due to illegal activity and phone will unlock only after paying ransom. These ransomwares are delivered via malicious android applications. In order to regain access phone boot in safe mode and then user uninstall the infected application. Booting of phone will not work if mobile ransomware encrypt data and demands money in order to decrypt data.

Many attackers use different phishing methods and other social media trap for user to download the android ransomware application onto their mobile phones. An attacker shows that ransomware application as a useful application to victim. These apps also install on smartphone via adware banner on social networking websites. A phishing email is sent to user showing that this mail is sent from relative, friend,

coworker or boss. This type of email has malicious link which is redirected to the download site of ransomware application and then it automatically installs unwanted application to smartphone. These attackers also lure the user by showing ransomware paid application for free. The users download these malware applications considering it as safe applications.

Ransomware apps required different types of permission to access the mobile phone. The user gives all permission to ransomware application as result of that phone locks down or these types of apps encrypt personal data on smartphone.

Most common feature of android ransomware is Screen locking. This ransomware is known as Loker ransomware. This type of ransomware gains administrative rights and lock smartphone screen. There is some ransomware which will change the inbuilt android screen PIN lock mechanism. They change the default PIN of smartphone to new PIN because victim grants administrative rights to malicious app. Some ransomware encrypts personal data on smartphone and demand ransom from user. These types of ransomware know as crypto ransomware. Attackers may use default cryptosystem or customized cryptosystem to encrypt personal data. Few ransomware display ransom messages and encrypt files in the background in a particular program. They scan SD card having files with different extensions such as pdf, txt, doc, docx, gif, bmp, mp4, mp3 and avi then encrypt them using customized cryptosystem.

Modern ransomware use command & control server to get encryption keys. If a permanent C&C communication is established than ransomware operator can execute any command on victim's smartphone. Few examples of command that are using by android ransomware are: lock or unlock phone, send SMS to any or all contacts on phone, activate or deactivate mobile data or Wi-Fi, track user location etc. Modern ransomware attacker's demands ransom through crypto currencies like Bitcoin because these currencies are untraceable.

II. TECHNIQUES TO DETECT RANSOMWARE

Ransomware is detected by using static approach, dynamic approach and hybrid approach

Static Approach:

This approach is based on the non-executable code which is created at compile time. In this type of approach software is analyzing before executing to check whether it is malicious or not [6]. In Android all source codes, certificates, assets etc. are compose in an apk file. This apk file is analyzed in static approach. H. Kang et al. [7] use static analysis technique and consider applications developer certificate serial number and suggested that for successful malware detection application certificate serial number is then compared with pre-defined suspicious malicious certificate serial numbers.

A service to analyze applications statically by using third party libraries and for security warning a pattern match is used this method is proposed by L. Batyuk et al. [8]. They were providing mitigation measures on the basis of user requirement by changing binary application packages. L. Apvrille et al. [9] gives classification module. This module consists of different classification algorithms like SVM (Support Vector Machine), Linear regression etc. By using this approach, we get best results. Saxe Joshua & Berlin Konstantin [10] detects malware on neural networks using two-dimension binary program features and they achieve 95% detection rate. Kanwal et al. [11] proposed a method based on permission, code and text analysis. Application install from google play store marked as safe. Extraction process is done before doing the permission analysis, code analysis and text analysis. Dex file is extracted from apk file during extracting process. Jar files extracted class files and then class files extracted java files. In text analysis ransom, locked, money, etc. keywords are searched. To open java files a custom file reader is used. Application can be declared safe or not on the basis of keywords. In code analysis they check if the app is trying to encrypt data. OnBackPressed() and OnPause method are used. If vulnerability is found user is notified to uninstall the application.

To detect android ransomware an approach is given by Karimi and Moattar [12]. For feature like selection and classification LDA algorithm is used. By using Androguard tool apk file is disassembled and then opcode sequence is extracted. Using opcode sequence an image is created and LDA is used for feature selection. Opcode sequences selected in feature selection are used to make new image. For classification LDA algorithm is used. In approach given by Andronio et al. [13] independent Threatening Text detector, Encryption detector and Locking detector) are executed parallel to identify ransomware. Text classification is used by threatening text editor to detect coercion attempts. If the detection results are positive that means the sample containing ransomware. In threatening text detector analysis localization, text classification, text extraction and other source of text are analyzed. Natural language processing is used by text classification to check whether a string contains frightening sentences. Encryption detector analysis uses getExternalStorageDirectory() and CipherOutputStream, delete() functions to check whether the disassembled code contains unwanted file encryption processes. Locking detector analysis that if the application under analysis is capable to lock the device.

Ezhilchelvan, P. D., & Mitrani, I. [14] gives a model to detect ransomware in IOT environment by analysis different types of ransomware families over the period of two years. They give model to detect crypto locker ransomware. Yalew et al. [15] gives android backup system for android mobile. In this backup of all system files is store in the backup of full system.

Dynamic Approach:

This approach is used during application runtime and it contains the features that represent the behavior of application. Taint analysis [16] is a real time analysis which is used to determine whether the important data is safe or not. Droid Ranger developed a tool based on heuristic & filtering detection method that uses permission to identify suspicious apps in android market. In this method manifest file declared permissions to filter app. After filtering apps are matched with malware footprint.

A system named as RansomProber proposed by Chen et al. [17] detects ransomware based on encryption, foreground and layout analysis. Encryption analysis is used to check whether any file is encrypted. Using foreground analysis RansomProber check that if the encryption process is belongs to any application that is using by user. In encryption analysis predefined directories must be protected. RansomProber measures data transformation degree. Three user interfaces named FileList, Button and Hint Text is present in the activities during file encryption. If click behavior of user exists then UI widgets are further analyzed.
A technique designed with configuration, monitoring and processing modules is proposed by Song et al. [18]. This technique detects ransomware then configuration module is applied. This module specifies the path of the files which are needed to be protected. These locations are called priority protection area (PPA). In real time the information of PPA is registered in monitoring module and it protects the corresponding file. If user determines the process as ransomware then using feedback of user the process is automatically detected and deleted. In process monitoring module processor share memory usage, process, storage input output count, I/O count are continuously monitor and detect ransomware. Suspicious processes are stopped forcibly by monitoring module in the processing module. The permission module in android analysis warns user about the risk of ransomware. By applying machine learning to dynamic analysis can achieve ransomware detection rates accuracy over 96% [19].

Hybrid Approach:
Hybrid approach is consisting of both static and dynamic methods. Hybrid method was proposed by Ferrante et al. [20]. Static method depends on frequency of opcodes. Dynamic method is based on the network and statistic on system call, CPU, monitoring of memory. First static method is used when application is installed on mobile. If application identified as malware than there is no permission to run on device and using dynamic detection all other applications are allowed to run. In static method the apps are pre-processed in order to find value of frequencies of opcode order that are appropriate to be process by the classifier. Then classifier undergoes into the learning phase. After learning phase classifier classified these applications as trusted or ransomware. In dynamic detection observations of system behavior is used. Similar to static detection, dynamic detection is also consisting of two phases i.e. pre-processing phase and learning phase.
MARVIN [21] is used to analyze malware and for solving problems like obfuscation and dynamic code loading. This method is based on hybrid approach. The system gives scores for unknown applications using machine learning. It consists of 135,000 android apps dataset out of which around 15,000 were malware. This tool has 98.24% accuracy score. Gharib and Ghorbani [22] give a real time hybrid framework known as DNA-Droid. Using static analysis this framework quickly analysis a sample and if anything is found suspicious, it will continuously check and check the runtime activities of the sample. In this framework static analysis, dynamic analysis and detection modules are used. Static module consists of three components to evaluate the apk file and then decides whether it is ransomware, or benign. These three components modules are Text Classification Module, Image Classification Module and API calls and permissions Module. Disassembled APK is resolving to extract the strings in Text Classification Module. It deletes meaningless words or stop words to clean the strings and remaining words are then lemmatized. Image Classification Module compares applications images with this collection of logos using the Structural Similarity Index Measure algorithm which reports the number of detected images as a feature. API calls and permissions Module uses AndroidManifest.xml file to extract the list of permissions and we can obtain a record of API methods by decompiling an APK. In Dynamic module malware behavior is detected and its properties are check by executing the sample in a virtual environment.

III. RESULTS AND DISCUSSION

This part presents the summary of comparison results for Static, Dynamic and Hybrid analysis in terms of techniques, activation mode and accuracy.

Table 2.: Summary of comparison results for Static, Dynamic and Hybrid Analysis.

Analysis	Techniques	Activation	Accuracy
Static Approach	Use Linear Regression, SVM, Code Analysis, Text detector, Encryption detector, Locking detector,	Static mode	95%
Dynamic Approach	Taint Analysis, encryption, foreground, layout analysis, PPA	Run Time mode	96%
Hybrid Approach	It uses opcode, obfuscation approach, text classification, Image classification, API calls	Static and Run Time mode	98%

Using summarized results from Table2. we can say that Hybrid Analysis gives better result as compare to Static and Dynamic analysis. But static and dynamic analysis becomes ineffective in case of obfuscated code or with run-time infections. Hybrid method is use for obfuscated code and run-time infections with high accuracy rate of 98%.

IV. CONCLUSION

In this paper static approach, dynamic approach and hybrid approach are shown to detect ransomware. Static methods are having high accuracy as compared to dynamic methods for the detection of ransomware. But they are ineffective with run-time infections. Hybrid approach overcomes the deficiency of static and dynamic approach. Little research work is already done to detect and prevent mobile from ransomware attacks. But there is need to develop method to detect mobile ransomware by using static and dynamic methods with high accuracy.

REFERENCES

1. Symantec internet security and threat report (ISTR) volume 24, 2019. http://www.symantec.com/content /dam/symantec/docs/reports/istr-24-2019-en.pdf
2. https://www.idc.com/promo/smartphone-market-share/os
3. https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/
4. https://www.welivesecurity.com/wpcontent/uploads/2016/02/Rise_of _Android_Ransomware.pdf.
5. Meet Kanwal, Sanjeev Thakur, Balwinder Singh Saggu, Survey of Detection tools for Android Ransomware, http://www.serialsjournals.com/articles. php?volumesno_id=1095&journals_i=268&volumes_id=848.
6. P Ravi Kiran Varma, Kotari Prudvi Raj, K. V. Subba Raju (2017), "Android mobile security by detecting and classification of malware based on permissions using machine learning algorithms", International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I- SMAC), IEEE.
7. H. Kang, J.-w. Jang, A. Mohaisen, and H. K. Kim, "Detecting and classifying android malware using static analysis along with creator information," I.J.D.S.N, vol. 2015, p. 7, 2015.
8. L. Batyuk, M. Herpich, S. A. Camtepe, K. Raddatz, A.-D. Schmidt, and S. Albayrak, "Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within android applications," in MALWARE'11. IEEE, 2011.
9. L. Apvrille and A. Apvrille, "Identifying unknown android malware with feature extractions and classification techniques," in Trustcom/BigDataSE/ISPA, 2015 IEEE, vol. 1. IEEE, 2015, pp. 182–189.
10. Saxe, Joshua & Berlin, Konstantin (2015). Deep neural network-based malware detection using two-dimensional binary program features. 11-20. 10.1109/MALWARE.2015.7413680.
11. Meet Kanwal ; Sanjeev Thakur (2017), "An app based on static analysis for android ransomware", International Conference on Computing, Communication and Automation (ICCCA), IEEE
12. Alireza Karimi, Mohammad Hosein Moattar (2017), "Android Ransomware Detection Using Reduced Opcode Sequence And Image Similarity", 7th International Conference on Computer and Knowledge Engineering, IEEE.
13. Andronio N., Zanero S., Maggi F. (2015) HelDroid: Dissecting and Detecting Mobile Ransomware. In: Bos H., Monrose F., Blanc G. (eds) Research in Attacks, Intrusions, and Defenses. RAID 2015. Lecture Notes in Computer Science, vol 9404. Springer, Cham.
14. Ezhilchelvan, P. D., & Mitrani, I. (2015). Evaluating the probability of Malicious co-residency in public clouds. IEEE Transactions on Cloud Computing, 5(3), 420–427.
15. Yalew, S. D., Maguire, G. Q., Haridi, S., & Correia, M. (2017, October). Hail to the Thief: Protecting data from mobile ransomware with ransomsafedroid. Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA) (pp. 1-8). IEEE.
16. William Klieber, Lori Flynn,Amar Bhosale, Limin Jia, Lujo Baner. Android Taint Flow Analysis for App Sets. In IEEE, pages 1- 6, 2014.
17. Jing Chen, Chiheng Wang, Ziming Zhao, Kai Chen, Ruiying Du, and Gail-Joon Ahn (2017), "Uncovering the Face of Android Ransomware Characterization and Real- time Detection", IEEE Transactions on Information Forensics and Security.
18. Sanggeun Song, Bongjoon Kim, and Sangjun Lee, "The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform," Mobile Information Systems, vol. 2016, Article ID 2946735, 9 pages, 2016.
19. Sowmya Gaitond, Rekha S Patil, "Leveraging Machine Learning Algorithms For Zero-Day Ransomware Attack", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019.
20. Ferrante A., Malek M., Martinelli F., Mercaldo F., Milosevic J. (2018) "Extinguishing Ransomware - A Hybrid Approach to Android Ransomware Detection". In: Imine A., Fernandez J., Marion JY., Logrippo L., Garcia- Alfaro J. (eds) Foundations and Practice of Security. FPS 2017. Lecture Notes in Computer Science, vol 10723. Springer, Cham.
21. M. Lindorfer, M. Neugschwandtner, and C. Platzer, "Marvin: Efficient and comprehensive mobile app classification through static and dynamic analysis," in Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual, vol. 2. IEEE, 2015, pp. 422–433.
22. Gharib A., Ghorbani A. (2017) DNA-Droid: A Real-Time Android Ransomware Detection Framework. In: Yan Z., Molva R., Mazurczyk W., Kantola R. (eds) Network and System Security. NSS 2017. Lecture Notes in Computer Science, vol 10394. Springer, Cham.

AUTHORS PROFILE

Manish Kaushik received the Ph.D. in Feb. 2007 from University of Rajasthan, Jaipur. He is currently working as Principal & Professor in the Department of Computer Science, S. S. Jain Subodh P. G. College, Jaipur. He has published over 60 research papers in many International & National Journals and Conferences and having 19 years of teaching & research experience.

Dr. Leena Bhatia MCA, M.Tech.(CS), Ph.D. (CS), UGC-NET(CS), Associate Professor at S.S. Jain Subodh P.G. College, Jaipur. Having total teaching experience more than 20 years.

Dr. Vipin Kumar Jain received the MCA and Ph.D from Banasthali Vidhyapith University, Niwai, Tonk(Rajasthan). He is currently working as an Assistant Professor, Department of Computer Science, S. S. Jain Subodh P. G. College, Jaipur and having more than 20 years experience. His research interests include Image Processing and Artificial Intelligence.