IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ANALYSIS OF FAKE APPS IN ANDROID ENVIRONMENT

Rajender Nyakapu, Naresh Sandela, Vennela Ram, Pavithra Nuthikattu, Preethi Madala

Researcher, Researcher, Researcher, Researcher, Researcher,
Computer Forensics and Information Security,
JNTUH College Of Engineering, Kukatpally, Hyderabad, Telangana, India.

Abstract: The vast usage of smartphones all over the world has given a platform for many developers to develop different apps which can provide user friendly interfaces for the users. The openness of the android operating system made the developers to easily which lead to the rapid development the apps. This rapid development of the apps also gave platform for the hackers to introduce malicious activities by developing fake apps. Fake apps are the apps which appear same as an original app and extract the user sensitive information once the user has installed the fake app into the device. This detection of fake apps has become a need of the day. In this paper we carefully analysed the fake apps and presented few defences and possible measures to detect the fake apps by which user sensitive information can be protected.

Keywords : Android, apps, original apps, fake apps, sensitive information, android developers, hackers.

I. INTRODUCTION

Today common man all over the world has much dependency on smartphones to perform 80% of daily routine activities. The smartphones became very popular in the last decade 2010-2020 because of its user-friendly interface via applications. The applications which are popularly called as apps provide many facilities for the users in their daily lives. The emergence of smartphones has come into existence based on the combination of computation and communication done on the portable smaller devices. By the end of 2020 almost more than 3 billion users are using the apps of the smartphones of which 85% of android users and 15% of iphone users all over the world.

The drastical usage of apps in android smartphones due to its open nature and cheaper cost made most of the attackers to target the android smartphones. The attackers target the smartphones mostly by three ways one of them is by (i) target to extract user sensitive data by sending message and fooling the user to click the message (ii) target to extract the user sensitive information using social engineering attacks (iii) target to extract the user sensitive information by using the applications or apps. There are many existing techniques [1] [2][3] which can detect the first two ways used by the attacker to extract user sensitive information from smartphones. The existing studies also have detection methods [4] [5] for detecting the applications in smartphones but still many solutions need to be enhanced and addresses in this area of detecting the apps.

The smartphone applications which are also popularly called as apps. The apps in android environment do not have proper solutions for detection in the existing studies. The attackers target the apps using two different ways. First way is by using the developer faults or by using the android OS loopholes. Second way is by creating the fake apps and extracting the user sensitive information using these fake apps. In this paper we completely analysed the different types of fake apps used by the attackers to extract the user sensitive information.

Fake apps are the smartphone applications which look like a original app and make the user to install the fake app into the smartphone device. Once the fake app is installed in the place of original app the attackers extract the sensitive or private information of the user by using these fake apps. In this paper we worked on analysis of fake apps and summarize how the fake apps extract the user private information from the users device.

Our paper is organized in five sections, in the first section we described the usage and smartphones and the reasons for existence of the fake apps. In the second section we presented the related studies on the fake apps. In the third section we presented the fake apps and its types. In the fourth section we presented defences for protecting the android smartphones from the fake apps. In the final fifth section we concluded the paper with future scope extension.

II. RELATED WORK

Chongbin Tang et al [6] worked on detection of fake characteristics on industrial fake apps. In this work they clearly demonstrated the strategies used by the attackers who develop fake apps by using the case studies.

M.Kireet, Pavithra rachala et al [7] worked on contemporary attacks in android smartphones. In this paper authors clearly mentioned the attacks done using the fake apps and different recent attacks in android smartphones.

Kireet Muppavaram, Meda Sreenivasa Rao et al [8] worked on the attacks, vulnerabilities in android environment. This paper completely presents complete detail investigation on attacks done to the apps and concludes whether the each app is safe or not should be verified with possible measures and defences.

Martens, D., Maalej [9] worked on detecting the fake apps by using the reviews. Based on the ratings and reviews given by the users the authors presented a model which detects the fake reviews given to the app.

Peng Wu et al [10] worked on detecting the fake apps using multi dimensional model which only detects the IoT related fake apps. This model presents the various algorithms which deals with the fake patterns in detecting the IoT fake apps.

III. FAKE APPS AND ITS TYPES

Fake apps are the smartphone apps which look like the original app. Fake apps are developed by the attackers or hackers. The attackers pick the popularly used apps by the general public and develop the similar kind of popular apps. The users unknowingly install the fake apps by the tricks played by the attackers by which attackers extract the user sensitive information.

Fake apps are of three types as per the study [7], they are (i) fake apps with same original app name but with different icon (ii) fake apps with slight change in app name with same icon (iii) fake app with completely null data.

(i). Fake apps with same original app name but with different icon:

These types of apps were usually developed by the attackers to fool the user and make the user to install the app into the users device. In Figure 1.1 clearly shows the WhatsApp fake app , the orginal app icon is on the left side of the figure and on the right side the fake WhatsApp can be observed in different colour icon. The attackers fool the user by sending the apk of fake WhatsApp by saying it as advanced and latest WhatsApp. The users by thinking it as original app installs the fake app.

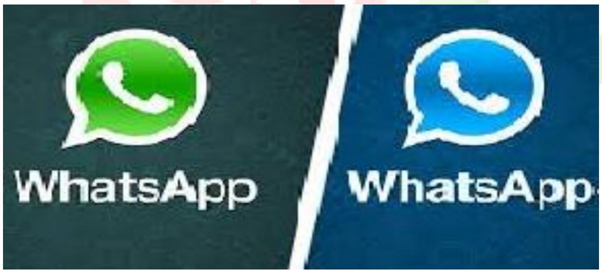

Figure 1. Sample whatsApp fake app

(ii). Fake apps with slight change in app name with same icon :

These types of fake apps have minor or slight change in the app name and attackers fool the user and make the user to install the app into the users device . In Figure 2 it clearly shows the fake app of masquerade technology , the users installs the fake app which is on the right side of the figure.

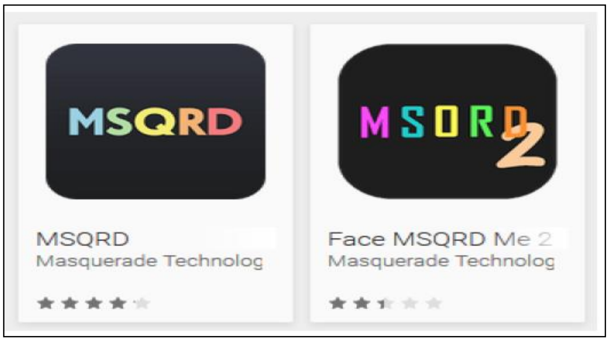

Figure 2. Sample Fake app

(iii). Fake apps with no data :

These types of fake apps are developed by the attackers. The attackers develop the apps with interesting features and makes the user to install the apps. The fact is that these apps wont work properly and as a result the information needed will be extracted by the hacker or attacker.

IV. DEFENCES AND POSSIBLE MEASURES TO PROTECT THE USER DEVICES FROM FAKE APPS

Some of the possible defences required to check whether the app is a fake app or safer app are as follows

(i). To verify the authenticity of the app :

The authenticity of the app is the first phase of checking or verifying the app. As per different existing studies and proper Google recommendations there are few possible ways to examine the authenticity of the apps they are

a) Devloper's identity : To search or the developer□s or company□ s official website in the AppMarket. This proves that the application is a legitimate one. If there is no link but a contact , then the user can try to contact the company or the developer to ask about download information and location. It helps the user to confidently install other apps which have been developed by the same developer or company.

b) Availability of apps created by a specific Developer: Some developer□s applications may not be available in certain countries but there can be fake apps which take this as advantage and try to use the developer□s good reputation. These apps draw users to install them and give all the permissions based on the legitimacy of the developer which in turn makes the user to lose their trust on that specific developer. So users must check if the developer has their apps working in that specific country or domain.

c) Updates: An application with a long history of updates is more likely to be authentic. We can even check if the updates/fixtures made to the application reflect the feedback given by the users, bugs proposed, developments requested by users during the Beta Testing of the application. However, a little caution is needed when installing new apps.

d) Reviews: Reviews can be positive or negative. A fake application usually has a lot of positive reviews. An app is unlikely to have numerous detailed, enthusiastic positive reviews throughout the history of the app�s development. So we need to check if there are detailed customer experience reviews from the app history (i.e. updates). Negative reviews are also useful. They help to identify issues previously faced by the users. With the help of these negative issues we can even pay attention to suspicious permissions, unauthorized changes to settings or net wallet, abnormal reactions of the app seen by the users. Therefore, checking reviews before installing gives the user outlook of the app.

(ii). Behavioural detection : This type of detection is needed for the fake app detection. Though the process of behaviour detection is little bit tough as number of fake app datasets available in the markets are less. The behaviour of the devices after installation of the app should be verfified. If the device performance is degraded in terms of the speed then the app data should be clearly verified in terms of extraneous irrelevant permissions are used by the app or not.

(iii). Permission based verification : Android Operating system consists of more than 135 permissions as per the android developer source[11]. If the app contains more than 50% of permissions proper permissions checking should be done by using the methods[ ] [ ]. If more number of extra permissions are required for the app then that could be treated as Fake app.

V. Conlcusion

The immense usage of smartphones lead to the development of smartphone applications by the developers to provide easy interfacing for the user by user friendly apps. The openness of android environment has made the attackers or hackers to choose the android application platform as the major target to extract the user sensitive information from the smartphones. This lead to the development of fake apps by many attackers to easily extract the sensitive information. This paper provides a clear study of the fake apps and the types of the fake apps used by the hackers or attackers. Finally based on the existing studies and recommendations from the Google this paper provides the possible defences and measures to protect the users private data from the fake apps. The detection of fake apps has a future scope in development of behavioural patterns of the fake apps by which the detection can be more effective.

REFERENCES

1. D. Sbîrlea, M.G. Burke, Salvatore Guarneri " Automatic detection of inter– application permission leaks in android applications, technical report tr13-02,dept of cse, Rice university, Research Report, IBM Journal of Research and Development, Volume: 57 , Issue: 6 ,Nov.-Dec. 2013, DOI**:** 10.1147/JRD.2013.2284403.

2. D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, K. Rieck, and C. Siemens, " Drebin: Effective and explainable detection of android malware in your pocket," in Proceedings of the Annual Symposium on Network and Distributed System Security (NDSS), 2014.

3. W. Wang, X. Wang, D. Feng, J. Liu, Z. Han, and X. Zhang, " Exploring permission-induced risk in android applications for malicious application detection," Informa-tion Forensics and Security, IEEE Transactions on, vol. 9, no. 11, pp. 1869– 1882, 2014.

4. L. K. Yan and H. Yin, " Droidscope: seamlessly reconstructing the os and dalvik semantic views for dynamic android malware analysis," in Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), 2012, pp. 569– 584.

5. Min Zheng, Mingshen Sun, John C.S. Lui: DroidAnalytics: A Signature Based Analytic System to Collect, Extract, Analyze and Associate Android Malware. In: 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, pp. 163– 171 (2013).

6. C. Tang *et al.*, "A Large-Scale Empirical Study on Industrial Fake Apps," *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, 2019, pp. 183-192, doi: 10.1109/ICSE-SEIP.2019.00028.

7. M.Kireet, Pavithra rachala, Meda Sreenivasa Rao, Rukmini Sreerangam Investigation Of Contemporary Attacks In Android Apps International Journal Of Scientific & Technology Research Volume 8, Issue 12, December 2019 ISSN 2277-8616.

8. Muppavaram K., Sreenivasa Rao M., Rekanar K., Sarath Babu R. (2018) How Safe Is Your Mobile App? Mobile App Attacks and Defense. In: Bhateja V., Tavares J., Rani B., Prasad V., Raju K. (eds) Proceedings of the Second International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and Computing, vol 712. Springer, Singapore. https://doi.org/10.1007/978-981-10-8228-3_19, July 208, online ISBN:978-981-10-8228-3.

9. Martens, D., Maalej, W. Towards understanding and detecting fake reviews in app stores. Empire Software Eng **24,** 3316– 3355(2019).Springer, 10 May 2019. https://doi.org/10.1007/s10664-019-09706-9.

10. P. Wu, D. Liu, J. Wang, B. Yuan and W. Kuang, "Detection of Fake IoT App Based on Multidimensional Similarity," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7021-7031, Aug. 2020, doi: 10.1109/JIOT.2020.2981693.

https://www.ijsdr.org/pubguide.php

http://www.ijeast.com/who-we-are.php