Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 4, 2020

Review Article

GOOGLE PLAY STORE BASED APPLICATIONS FOR SEARCH RANK FRAUD AND MALWARE DETECTION

K. Tharageswari[1]*, Dr.S. Arul Antran Vijay[2], P.N. Ramesh[3]

[1*]Asso Professor, Department of CSE, Karpagam Academy of Higher Education, India. tharageswari.k@kahedu.edu.in
[2]Asst Prof., Dept of CSE, Karpagam College of Engineering, India.
[3]Asst Prof., Dept of CSE, Karpagam Institute of Technology, India.

Received: 03.12.2019 *Revised: 12.01.2020* *Accepted: 07.02.2020*

Abstract
Google play store contains million of apps and thousands of applications are published on every day. To promote the app and make the users to download is becoming complicated; the published try to increase the visibility of the app on the search console. Also it becomes difficult for the users to identify the malware app and download the good one. Few publishers on the play store try to increase their apps rank with fraud and black hat methods. The publishers increase their ranking by create fake bot reviews; provide fake rating through fake accounts. This misleads the users to download the malware apps from the store. In the proposed model, we try to identify the fair reviews and fake reviews by mining the reviewer profile, their rating patterns. With help of fair play detection we also identify that most of the malware apps use fraud ranking strategies to improve their downloads.

Keywords: Search Fraud Detection, Google Play Store Ranking and Malware App Detection.

DOI: http://dx.doi.org/10.31838/jcr.07.04.163

INTRODUCTION

The popularity of Android phones and its commercial success of the google play store have attracted millions of developers to develop and market their apps on the play store. There are millions of android users download & use android apps regularly. This popularity and user base has also provides a platform for malware

developers to use app markets as a platfrom for their malware [1]. The primary idea for such behaviors is impact: app popularity for translating into financial benefits and expedited malware proliferation. Malware developers frequently exploit Freelancer and crowd funding websites (Freelancer [2], Fiverr [3], BestAppPromotion [4]) to hire teams of willing freelancers to involve in fraud collectively, emulating realistic, misleading activities from unrelated people. The Fraudulent developers use the crow sourcing sites to promote their apps and recruit freelancers to work on their idea to fraud rank the apps in figure1. We term this behaviour as "search rank fraud". Additionally, Google's efforts of Android markets to find, identify and delete malware are not always successful.

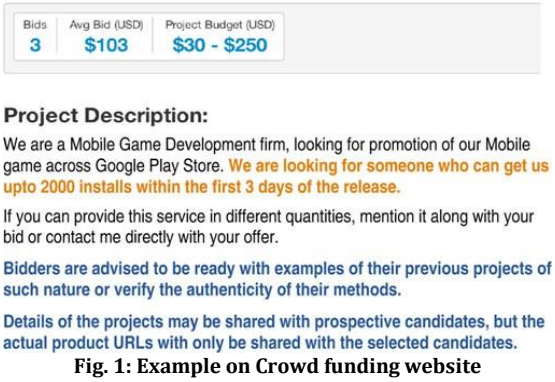

Fig. 1: Example on Crowd funding website

The bouncer systems used by google to remove malware apps are not so successful. We used virus Total scanner to analyse 7,756 Google Play apps and 12 percent (948) were flagged as malicious and by other anti-virus tools 2 percent (150) were identified as malware by at least 10 tools.

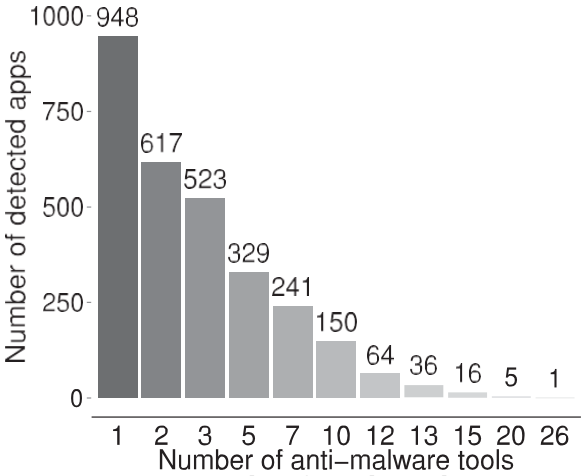

Fig. 2: Number of apps detected

Existing bouncer system by google play store does not effectively scan the apps and identify the fraudulent apps in the play store. There is a need for a better framework to identify and remove the malicious apps and also to find the search fraud in the google playstore.

In this paper we propose a methodology to identify and analyse the search fraud ranking and also the malicious apps on the playstore. It is very arbitrary that malicious app developers tend to use search fraud to improve their ranking on google play store and intend to create a impact on their apps on the user base.

There are tons of apps in the play store with different categories. See Fig 3. for number of apps and the popular categories.

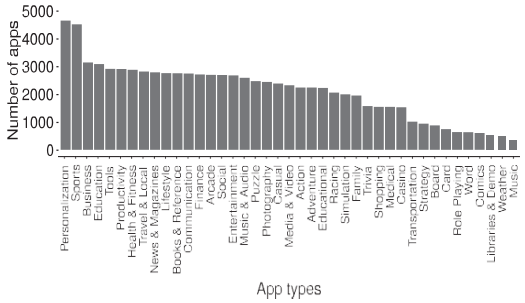

Fig. 3: Number of Apps and their categories

Since there are millions of apps on different categories, it very difficult for the users to differentiate the apps and download the right one. User intend to download top ranked apps and it provides a opportunity for the malware app developers to user ranking system to increase e their downloads. Also it becomes difficult for the users to identify the malware app and download the good one. Few publishers on the play store try to increase their apps rank with fraud and black hat methods. The publishers increase their ranking by create fake bot reviews provide fake rating through fake accounts. This misleads the users to download the malware apps from the store. In the proposed model, we try to identify the fair reviews and fake reviews by mining the reviewer profile, their rating patterns. With help of fair play detection we also identify that most of the malware apps use fraud ranking strategies to improve their downloads.

Google's ranking system are completed based on the search results, reviews and number downloads of the app. By creating better search visibility and providing good rating, reviews for the apps, the developers can able to increase their apps rank on the play store.

BACKGROUND STUDY

In recent years mobile phones are becoming more smart and these smartphone markets is becoming more popular and increasing popularity among the users. The user base for the smartphones is very large and many new brands are in the market.

A) The increase and popularity among the smartphones provides opportunities for new apps developers and many mobile app developing companies are developing new applications. On day today basis the size of google play store has become very larger. Making a mobile app popular and make it successful becomes more challenging. This makes the apps developer to find new ways to reach the users and make them to download the apps. Certain developers use un ethical ways of promoting their apps, they tend to create fake reviews and increase the popularity.

B) To increase the visibility of the mobile applications to google play store users, few developers try to boost theirs apps visibility on google play store search. To increase their search rank, the developers create fake reviews with help of freelancer's sites. As mentioned in the Fig. 1. developers use the crowd funding sites and outsource fake review jobs to freelancer. With less time and money the freelancers, with their fake accounts created for reviewing apps, provide reviews to the apps and try to increase the popularity of the apps among the users. The users are mislead with these reviews and download the apps.

C) In the work "Static Analysis using similarity Distance" - Anthony Denos, author of this paper. Provides the important of developing algorithms and applications to secure the users data and applications from piracy and injection attacks. The author describes the drawback of android applications that is by extracting the apk files the attackers can easily extract the source code and this will help the hackers to tampering the application with vulnerable code injecting.
In this paper the author provides a distance similarity method to calculate the vulnerable code and the app protecting the piracy of the users. With help of this method, we can find the similarity of the original android apps and vulnerable applications on the play store.

D) Patrik Lantz [7], the author of paper "Analysis of Malicious and Benign Android Applications", From the day the android apps launched for the first time in the android play store market, it the apps store has becoming larger on day to day basis. And the number of users using android apps also has been dramatically increased in the past few years. The authors a present a very effective and simple method to analyse and find the malicious apps on the play store by a sandbox Droid box. This method helps to generate a graphical representation of the behavioural samples of the based on the apps permissions and the patterns to help in identifying the vulnerable apps. This method acts as similar as anti-virus applications and provides a mechanism to identify the apps that affects user's piracy.

B) Emre Erturk [6], author of paper "A Case Study in Open Source Software Security and Privacy: Android Adware", The authors in the paper proposes a techniques to analyse the behaviour and the type of piracy, privacy that affecting the users of the apps. With a deep analysis the authors presents a reviews the security of the android operating system. The author also addresses the positive and negative of the open source operating system such as android and other open source mobile operating systems.
The goal of this paper is to analyse and reviews the security concerns related to android operating system and the application used in the android devices. With this case study on open source operating system, the author also discusses about the privacy issues that caused by the mobile applications and that make the users to lose their privacy and become a victim for the hackers.

PROBLEMS IDENTIFIED

Fake reviews and malware apps on the play store huge threat to google play store users. Malwares are developed with an intension to promote the apps among the users and when users download and use the apps, users while download provide permissions to access the data in the devices.
These apps break the privacy and steal the files and data of the users on the mobile device. This is a major issue among the smart phone users.

PROPOSED MODEL

In the proposed model, we develop a mechanism to identify Fraud search ranked apps and malware apps on the google play store.

Malware detection is a very important for securing the app store users to protect their data and files on the mobile device. We use deep learning methods to deeply analyse and identify the malware apps, by identifying the apps functionality, the apps permissions and comparing the permissions and functionality of the app. We try to identify the apps behaviour and identify the apps trustness to use the app by the users.

With our methodology we identify that certain apps uses permissions that not required performing the actual functionality of the app. With these techniques are able to differentiate the app with malware apps and trust full apps.

Apart from analysing the malware detection apps we also detect the search fraud detection by co-review behaviour, using classifiers of fraudulent and malware apps. Based on the user reviews and his review behaviour prediction mechanism, the review of frequent reviewers are analysed, with their review patterns and rating mechanisms.

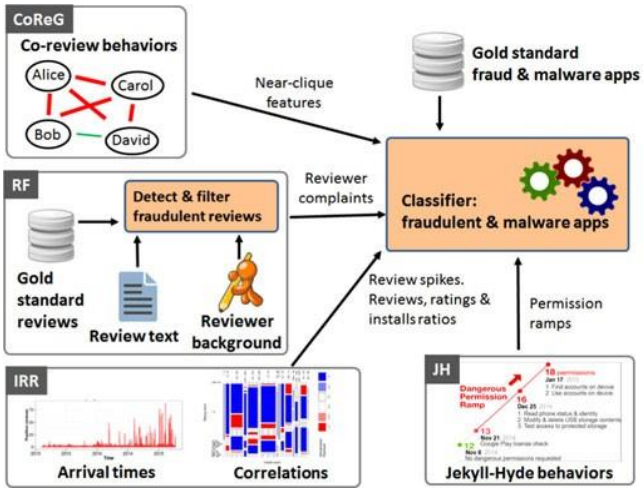

Fig. 4: Fairplay Model

Fair Play organizes the analysis of longitudinal app data into the following 4 modules, illustrated in Fig 4. The Co-Review Graph (CoReG) module identifies apps reviewed in a contiguous time window by groups of users with significantly overlapping review histories. As illustrated in fig 4. We analyse the history of reviewers and the time between each reviews they take to review the apps on the playstore. As a example the reviewers can review to many apps in a short time. The reviewer has to download the app and explore it before reviewing a app. He should have used at least a few versions of the apps to review it better. If a reviewer is rating only the initial verisons frequently then he may not use the apps completly with its features.

The Review Feedback (RF) module exploits feedback left by genuine reviewers, while the Inter Review Relation (IRR) module leverages relations between reviews, ratings and install counts. The Jekyll-Hyde (JH) module monitors app permissions, with a focus on dangerous ones, to identify apps that convert from benignto malware. Each module produces several features that are used to train an app classifier. Fair Play also uses general features such as the app's average rating, total number of reviews, ratings and installs, for a total of 28 features.

CONCLUSION

This work showcases the impact of search fraud ranking and also analysis the impact of ranking that tens the user to download the apps from the play store. The malicious apps are downloaded that are influenced by the developers by fraud ranking methods. Thus using the proposed fair play model can help to reduce the search fraud ranking.

REFERENCES

1. Wong, L. (2005). Potential Bluetooth vulnerabilities in smartphones. Retrieved from http://citeseerx.ist.psu.edu.
2. Freelancer. [Online]. Available: http://www.freelancer.com
3. Fiverr. [Online]. Available: https://www.fiverr.com/
4. BestAppPromotion. [Online]. Available: www.bestreviewapp.com/
5. Brown, B. (2009). Beyond Downadup: Security expert worries about smart phone, TinyURL threats: Malware writers just waiting for financial incentive to strike, F-Secure exec warns. Retrieved from http://business.highbeam.com/409220/article-1G1-214585913/beyond-downadup-security-expert-worries-smartphone
6. Emre Erturk, 2012, IEEE, A Case Study in Open Source Software Security and Privacy: Android Adware.
7. Anthony Desnos, 2012, Android : Static Analysis Using Similarity Distance, IEEE publications
8. Bhattacharya, D. (2008) Leardership styles and information security in small businesses: An empirical investigation (Doctoral dissertation, University of Phoenix). Retrieved from www.phoenix.edu/apololibrary
9. Rash, W. (2004). Latest skulls Trojan foretells risky smartphone future. Retrieved from www.eweek.com.
10. Baldi A. "Computational Approaches for Drug Design and Discovery: An Overview." Systematic Reviews in Pharmacy 1.1 (2010), 99-105. Print. doi:10.4103/0975-8453.59519
11. Becher, M., Freiling, F., & Leider, B. (2007, June) On the effort to create smartphone worms in Windows Mobile. Proceedings of the 2007 IEEE workshop on Information Assurance. United States Military Academy. West Point, NY. Retrieved from http://pi1.informatik.unimannheim.de/filepool/publications/on-the-effort-to-createsmartphone-worms-in-windows-mobile.pdf. .
12. Portokalidis, G., Homburg, P., Anagnostakis, K., & Bos, H. (2009). Paranoid Android: Zero-day protection for smartphones using the cloud. Retrieved from www.cs.vu.nl/~herbertb/papers/trpa10.pdf.
13. Morgado, M., Rolo, S., MacEdo, A.F., Castelo-Branco, M.Association of statin therapy with blood pressure control in hypertensive hypercholesterolemic outpatients in clinical practice(2011) Journal of Cardiovascular Disease Research, 2 (1), pp. 44-49. DOI: 10.4103/0975-3583.78596
14. Schmidt, A-D., Peters, F., Lamour, F., Scgeel, C., Camtepe, S., & Albayrak, S. (2009). Monitoring smartphones for anomaly detection. Mobile Networks and Applications, 14(1), 92-106.
15. Xie, L., Zhang, X., Chaugule, A., Jaeger, T., & Zhu, S. (2009). Designing system-level defenses against cellphone malware. Retrieved from www.cse.psu.edu
16. Salkind, N. J. (2004). Statistics for people who (think they) hate statistics. Retrieved from http://search.barnesandnoble.com/Statistics-for-People-Who/Neil-JSalkind/e/9781412979597/?cm_mmc=AFFILIATES-_-Linkshare-_-je6NUbpObpQ-_-10:1.