International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

Detecting fake apps and restricting access to app store using Malware code detection and rating review analysis

Sunkari Shekar, Department of CSE, Malla Reddy College of Engineering & Technology, Telangana - 500014
Mrs. R. Sujatha, Assistant Professor, Department of CSE, Malla Reddy College of Engineering & Technology, Telangana - 500014

Abstract - Fraudulent behaviors in Google Play, the most popular Android app market, fuel search rank abuse and malware proliferation. To identify malware, previous work has focused on app executable and permission analysis. In this paper, we introduce FairPlay, a novel system that discovers and leverages traces left behind by fraudsters, to detect both malware and apps subjected to search rank fraud. FairPlay correlates review activities and uniquely combines detected review relations with linguistic and behavioral signals gleaned from Google Play app data (87K apps, 2.9M reviews, and 2.4M reviewers, collected over half a year), in order to identify suspicious apps. FairPlay achieves over 95% accuracy in classifying gold standard datasets of malware, fraudulent and legitimate apps. We show that 75% of the identified malware apps engage in search rank fraud. FairPlay discovers hundreds of fraudulent apps that currently evade Google Bouncer's detection technology. FairPlay also helped the discovery of more than 1,000 reviews, reported for 193 apps that reveal a new type of "coercive" review campaign: users are harassed into writing positive reviews, and install and review other apps.

1. INTRODUCTION

The commercial success of Android app markets such as Google Play and the incentive model they offer to popular apps, make them appealing targets for fraudulent and malicious behaviors. Some fraudulent developers deceptively boost the search rank and popularity of their apps (e.g., through fake reviews and bogus installation counts), while malicious developers use app markets as a launch pad for their malware. The motivation for such behaviors is impact: app popularity surges translate into financial benefits and expedited malware proliferation.

Fraudulent developers frequently exploit crowdsourcing sites (e.g., Freelancer, Fiverr, BestAppPromotion) to hire teams of willing workers to commit fraud collectively, emulating realistic, spontaneous activities from unrelated people (i.e., "crowdturfing"), see Figure 1 for an example. We call this behavior "search rank fraud". In addition, the efforts of Android markets to identify and remove malware are not always successful. For instance, Google Play uses the Bouncer system to remove malware. However, out of the 7, 756 Google Play apps we analyzed using Virus Total, 12%

(948) were flagged by at least one anti-virus tool and 2% (150) were identified as malware by at least 10 tools.

Previous mobile malware detection work has focused on dynamic analysis of app executables as well as static analysis of code and permissions. However, recent Android malware analysis revealed that malware evolves quickly to bypass anti-virus tools. In this paper, we seek to identify both malware and search rank fraud subjects in Google Play. This combination is not arbitrary: we posit that malicious developers resort to search rank fraud to boost the impact of their malware. Unlike existing solutions, we build this work on the observation that fraudulent and malicious behaviors leave behind telltale signs on app markets. We uncover these nefarious acts by picking out such trails. For instance, the high cost of setting up valid Google Play accounts forces fraudsters to reuse their accounts across review writing jobs, making them likely to review more apps in common than regular users. Resource constraints can compel fraudsters to post reviews within short time intervals. Legitimate users affected by malware may report unpleasant experiences in their reviews. Increases in the number of requested permissions from one version to the next, which we will call "permission ramps", may indicate benign to malware (Jekyll-Hyde) transitions.

2. LITERATURE SURVEY

Crowdroid: Behavior-Based Malware Detection System for Android

In this paper we capitalize on earlier approaches for dynamic analysis of application behavior as a means for detecting malware in the Android platform. The detector is embedded in a overall framework for collection of traces from an unlimited number of real users based on crowdsourcing. Our framework has been demonstrated by analyzing the data collected in the central server using two types of data sets: those from artificial malware created for test purposes, and those from real malware found in the wild. The method is shown to be an effective means of isolating the malware and alerting the users of a downloaded malware. This shows the potential for avoiding the spreading of a detected malware to a larger community.

Riskranker: Scalable and Accurate Zero-day Android Malware Detection

In this paper, we propose a proactive scheme to spot zero-day Android malware. Without relying on malware samples and their signatures, our scheme is motivated to assess potential security risks posed by these untrusted apps. Specifically, we have developed an automated system called *RiskRanker* to scalably analyze whether a particular app exhibits dangerous behavior (e.g., launching a root exploit or sending background SMS messages). The output is then used to produce a prioritized list of reduced apps that merit further investigation. When applied to examine 118,318 total apps collected from various Android markets over September and October 2011, our system takes less than four days to process all of them and

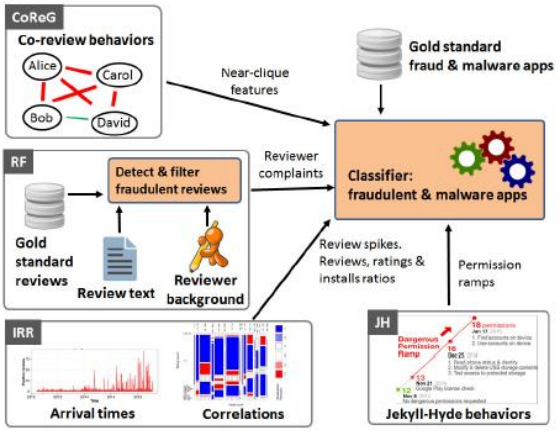
International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

effectively reports 3281 risky apps. Among these reported apps, we successfully uncovered 718 malware samples (in 29 families) and 322 of them are zero-day (in 11 families). These results demonstrate the efficacy and scalability of RiskRanker to police Android markets of all stripes.

Android Permissions: a Perspective Combining Risks and Benefits

In this paper, we investigate the feasibility of using both the permissions an app requests, the category of the app, and what permissions are requested by other apps in the same category to better inform users whether the risks of installing an app is commensurate with its expected benefit. Existing approaches consider only the risks of the permissions requested by an app and ignore both the benefits and what permissions are requested by other apps, thus having a limited effect. We propose several risk signals that and evaluate them using two datasets, one consists of 158,062 Android apps from the Android Market, and another consists of 121 malicious apps. We demonstrate the effectiveness of our proposal through extensive data analysis.

3. SYSTEM ANALYSIS:



System Architecture

3.1 Existing System

- Zhou and Jiang collected and characterized 1, 200 Android malware samples, and reported the ability of malware to quickly evolve and bypass the detection mechanisms of anti-virus tools.
- Burguera et al. used crowdsourcing to collect system call traces from real users, then used a "partitional" clustering algorithm to classify benign and malicious apps.
- Google has deployed Bouncer, a framework that monitors published apps to detect and remove malware.

3.1.1 Disadvantages

- Some fraudulent developers deceptively boost the search rank and popularity of their apps. While malicious developers use app markets as a launch pad for their malware.

- Bouncer is not sufficient - our results show that 948 apps out of 7,756 apps that we downloaded from Google Play are detected as suspicious.

3.2 Proposed System

- We propose FairPlay, a system that leverages the above observations to efficiently detect Google Play fraud and malware.

- We use linguistic and behavioral information to (i) detect genuine reviews from which we then (ii) extract user-identified fraud and malware indicators.

- Resource constraints can compel fraudsters to post reviews within short time intervals. Legitimate users affected by malware may report unpleasant experiences in their reviews. Increases in the number of requested permissions from one version to the next, which we will call "permission ramps", may indicate benign to malware (Jekyll-Hyde) transitions.

- By monitoring new apps, we aim to capture in real-time the moments when such search rank fraud campaigns begin.

3.2.1 ADVANTAGES

- FairPlay detected suspicious behavior for apps that were not removed by Bouncer during a more than 6 months long interval.
- FairPlay identifies and exploits a new relationship between malware and search rank fraud.
- FairPlay combines the results of this approach with behavioral and linguistic clues, extracted from longitudinal app data, to detect both search rank fraud and malware apps.

MODULES:

1. **User Module:**
2. **Server Module/Admin Module:**
3. **CoReG,RF,IRR Analysis Module:**
4. **JH Malicious app and User Detection Module:**
5. **App Developer Module:**

User Module:

- USER: user has to register to get login.
- MY PROFILE: User can check his/her Profile Details
- SEARCH MOBILE APPS: User can search Mobiles Applications By giving keyword and result will come based on priority(rank) and User can View the applications and can download application , he/she can give comment also.
- Normal User: Normal user will give single review for all apps.
- Malicious User: Malicious user will give multiple reviews at same time to increase rank.

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

- Normal USER: user searches on same keyword but search results are changed as malicious app is ranked to zero.

App Developer Module:

- Developer has to register to get login.
- MY PROFILE: developer can check his/her Profile Details
- ADD MOBILE & O.S : developer can add mobiles and O.s
- ADD APP DETAILS: Developer can add the details of Application.
- VIEW APPILCATIONS: Developer can view the uploaded Applications.

Server Module/Admin Module:

- Server has to login**.**
- **VIEW APP DEVELOPER :** Server can view registered developers and he can activate the developer
- **VIEW APP USE:** Server can view registered users and he can activate the users.
- **VIEW UPLOADED APPS WITH RANKS:** Server can view all the apps which were uploaded by developers.

CoReG,RF,IRR Analysis Module:

- **Finding Malicious user and APP:**
- **CO-REG,RF,IRR :** select app name and Time to find out list of users who gave review for respective app name at different times.

JH Malicious app and User Detection Module:

- **JH:** JH to find malicious user and malicious appname and block user and set malicious app rank to zero

4. OUTPUT RESULTS:

Fig 4.1: View Developers Page

Fig 4.2: View users and Activate them Page

Fig 4.3: Server All Applications Page

5. CONCLUSION

We have introduced FairPlay, a system to detect both fraudulent and malware Google Play apps. Our experiments on a newly contributed longitudinal app dataset, have shown that a high percentage of malware is involved in search rank fraud; both are accurately identified by FairPlay. In addition, we showed FairPlay's ability to discover hundreds of apps that evade Google Play's detection technology, including a new type of coercive fraud attack.

REFERENCES

[1] Google Play. https://play.google.com/.
[2] Ezra Siegel. Fake Reviews in Google Play and Apple App Store.Appentive, 2014.
[3]Zach Miners. Report: Malware-infected Android apps spike in the Google Play store. PCWorld, 2014.
[4] Stephanie Mlot. Top Android App a Scam, Pulled From Google Play. PCMag, 2014.
[5] Daniel Roberts. How to spot fake apps on the Google Play store. Fortune, 2015.
[6] Andy Greenberg. Malware Apps Spoof Android Market To Infect Phones. Forbes Security, 2014.
[7] Freelancer. http://www.freelancer.com.
[8] Fiverr. https://www.fiverr.com/.
[9] BestAppPromotion. www.bestreviewapp.com/.
[10] Gang Wang, Christo Wilson, Xiaohan Zhao, Yibo Zhu, Manish Mohanlal, Haitao Zheng, and Ben Y. Zhao. Serf and Turf: Crowdturfing for Fun and Profit. In *Proceedings of ACM WWW*. ACM, 2012.
[11] Jon Oberheide and Charlie Miller. Dissecting the Android Bouncer. *SummerCon2012, New York*, 2012.
[12] VirusTotal - Free Online Virus, Malware and URL Scanner. https: //www.virustotal.com/, Last accessed on May 2015.
[13] Iker Burguera, Urko Zurutuza, and Simin Nadjm-Tehrani. Crowdroid: Behavior-Based Malware Detection System for Android. In
Proceedings of ACM SPSM, pages 15–26. ACM, 2011.
[14] Asaf Shabtai, Uri Kanonov, Yuval Elovici, Chanan Glezer, and Yael Weiss. Andromaly: a Behavioral Malware Detection Framework =for Android Devices. *Intelligent Information Systems*, 38(1):161–190, 2012.
[15] Michael Grace, Yajin Zhou, Qiang Zhang, Shihong Zou, and Xuxian Jiang. Riskranker: Scalable and Accurate Zero-day AndroidMalware Detection. In *Proceedings of ACM MobiSys*, 2012.