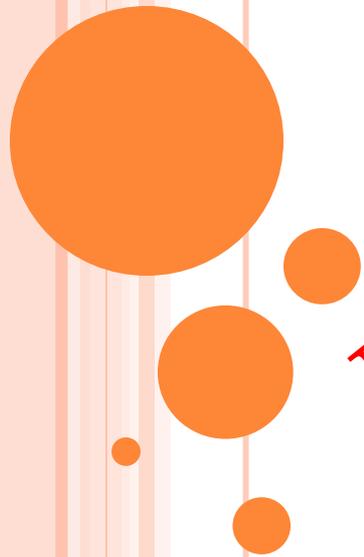# SEARCH RANK FRAUD AND MALWARE DETECTION IN GOOGLE PLAY

MICANS INFOTECH

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 (87 K apps, 2.9 M reviews, and 2.4M reviewers, collected over half a year), in order to identify suspicious apps.

EXISTING SYSTEM

- Fraudulent developers frequently exploit crowdsourcing sites (e.g., Freelancer [7], Fiverr [8], BestAppPromotion [9]) to hire teams of willing workers to commit fraud collectively, emulating realistic, spontaneous activities from unrelated people (i.e., "crowdturfing" [10]), see Fig. 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 [11] to remove malware.

- However, out of the 7,756 Google Play apps we analyzed using VirusTotal [12], 12 percent (948) were flagged by at least one anti-virus tool and 2 percent (150) were identified as malware by at least 10 tools.

DISADAVANTAGE

- FairPlay correlates review activities and uniquely combines detected review relations with linguistic and behavioral signals gleaned from Google Play app data (87 K apps, 2.9 M reviews, and 2.4M reviewers, collected over half a year),

- In order to identify suspicious apps. FairPlay achieves over 95 percent accuracy in classifying gold standard

- 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.

PROPOSE SYSTEM

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

- Our major contributions are:A Fraud and Malware Detection Approach. To detect fraud and malware, we propose and generate 28 relational, behavioral and linguistic features, that we use to train supervised learning algorithms .

- an efficient algorithm to identify temporally constrained, co-review pseudo-cliques—formed by reviewers with substantially overlapping co-reviewing activities across short time windows.

ADVANTAGES

- FairPlay achieves over 95 percent accuracy in classifying gold standard datasets of malware, fraudulent and legitimate apps.

- Fraudulent behaviors in Google Play, the most popular Android app market, fuel search rank abuse and malware proliferation.

SOFTWARE REQUIREMENT

- **HARDWARE REQUIREMENT:**
- System   :   Pentium IV 2.4 GHz.
- Hard Disk   :   40 GB.
- Floppy Drive   :   1.44 Mb.
- Monitor   :   15 VGA Colour.
- Mouse   :   Sony.
- Ram   :   512 Mb.

Cont..

- **SOFTWARE REQUIREMENT:**
- Operating system   :   Windows XP.
- Coding Language   :   ASP. Net with C#
- Data Base   :   SQL Server 2005.

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