



CYBERSECURITY

FRAUDULENT APP PROMOTION ON THE GOOGLE PLAY STORE

Namodh Edirisinghe

nedi1968

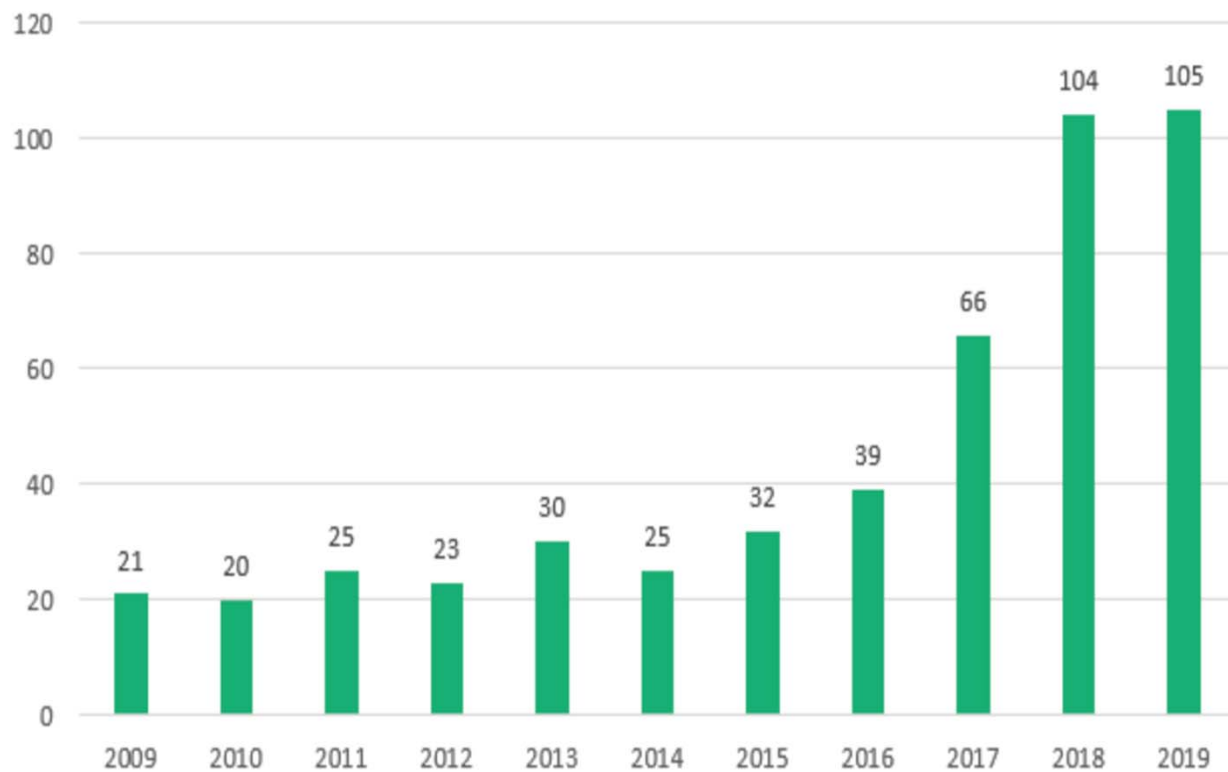


How Important is Cybersecurity?

- Cybersecurity aims to protect electronic data and devices from criminal activities.
- Consists of cryptography, network security, smart grid security etc.
- The advancement of processing power and the growth of the internet have caused major issues.
- Differs from other associated topics due to the vast number of factors to be considered when tackling cybersecurity issues.

Severity of present-day cyber attacks

Cyber Attack Incidents with \$1M+ in Reported Losses



As illustrated in [2, Fig. 1]

Further,

- 1 million cyber crimes are reported daily.
- Cyber attacks on US state departments resulted in \$1 trillion of damage in 2015
- Every electronic device is a potential victim of attacks.






Current state of the Google Play Store

- 2.8 million apps are available for download in the Google Play Store
- The 5-star rating system heavily affects whether or not users tend to download applications (via the search rank of apps)
- However, vulnerabilities in the store have questioned the legitimacy of certain ratings and reviews.
- One such vulnerability had revealed details about 198 million reviews, of which 9942 reviews were fake.



The Art and Craft of Fraudulent App Promotion in Google Play

- 
- This paper explores the personnel, methods and devices used in posting fake reviews and ratings on the Play Store.
 - Furthermore, it identifies vulnerabilities in the defense mechanisms of the store exploited by fraudsters.
 - Whether the fraudulent reviews affect the overall rating of apps is also investigated.
 - Potential fixes to Google Play to reduce such fraudulent reviews are given.



Outcomes of Previous Research

- **Former research projects have mainly identified fraudulent accounts and observed inconveniences faced by real users, without concentrating on methods used and vulnerabilities. (Mainly focused on social media platforms)**
- **One study analyzed likes on Facebook ads generated by “like farms” based on various characteristics of the fake accounts used.**
- **Another study observed the usage of hijacked Google accounts, relating to this study.**
- **Machine Learning and NLP methodologies were used to explore various fraudulent advertisements on sites like Craigslist.**



The Research Methods

- **Qualitative Study**

- 18 experienced ASO Workers recruited from freelancing sites
- In-depth interviews carried out via Skype
- Questions based on demographic data, methods of operation, devices, etc.
- Data made anonymous abiding to ethical considerations, and analyzed accordingly (Using Grounded Theory)





The Research Methods (cont.)

- **Quantitative Study**

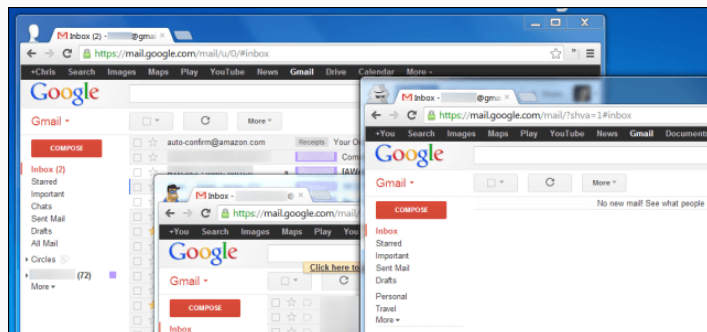
- 1164 accounts used by 39 ASO workers analyzed.
- Various APIs were used to obtain information on the apps reviewed by the workers and other such details.
- Google Play's queries were used to discover the various devices used for the fraudulent reviews. Other websites were used to obtain manufacturer information for devices. (Year of Make, Cost etc.)





Findings

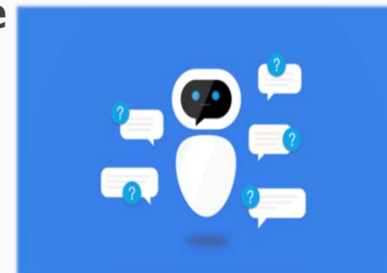
- Fraudsters either use many fake accounts themselves, use organic accounts or use both.
- Many represented a superior who undertook orders. Hierarchical structure seen.
- The amount of fake accounts varied between workers, but they had at least a few hundred.





Findings (cont.)

- The accounts were mostly bought, but were hand-made periodically in some instances.
- 93.8% of fake reviews were posted using cellular phones.
- These phones varied in type, price, year, but tend to be older and cheaper.
- Bots were used in these processes but are not as effective
- Workers recruited mainly from Social Media platforms





Findings (cont.)

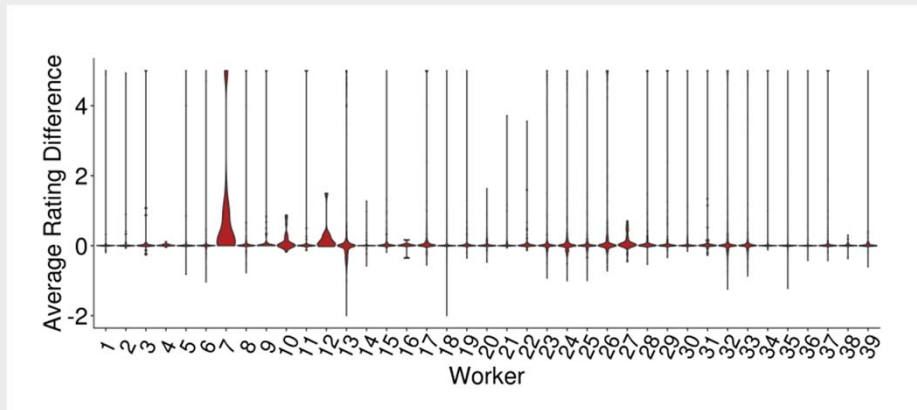
- **It was revealed the fraudsters already know the main triggers for fraud detection systems and that they already have bypass mechanisms:**
 - Singleton Accounts
 - Upvoting, Downvoting
 - Actual Installations
 - Maximum Daily Reviews
- **Reviews are 'ordered' during pre-production and when negative reviews come up (Re- hiring).**
- **Review 'bursts' are risky and unlikely to succeed.**
- **Specific patterns in accounts used seen among workers (lockstep behavior)**



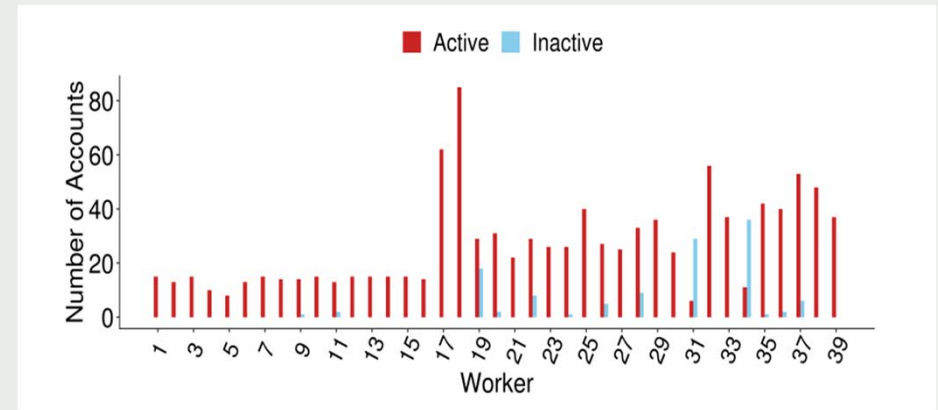
Findings (cont.)

- The text for the review is often given by the developer. Otherwise, small reviews around 10 words or less used.
- Most workers tend to go with 5- or 4-star ratings, while bad ratings are used to make these ratings less obvious to the fraud detection system.
- To show the validity of the study, the number of fraudulent accounts currently active were checked.
- The findings showed that fraudulent projects, on average, increased the rating of the application at hand.

Findings (cont.)



Change of Rating after Fraudulent Campaign
As illustrated in [1, Fig. 16]



No. of Active vs. Inactive Worker Accounts
As illustrated in [1, Fig. 15]



Pros



- The paper has covered a sensitive topic with no ethical issues.
- Addresses vulnerabilities of the software itself, unlike other papers.
- Provides many implementable options to increase the security of the Play Store:
 - *Device Fingerprinting*
 - *Organic Fraud Detection*
- This paper builds on previous work and explores a large variety of questions regarding fraudulent app promoters and their strategies.



Cons

- Only small, extremely selected samples were taken for both methods. The sample isn't representative of all ASO workers.
- Due to the industry in which the subjects are involved in, cannot be certain of all the results.
- As this study concentrates solely on the Google Play Store, the results cannot be inferred to other App Stores or any other sites.





Conclusion

- The paper shows the findings from the interviews and observations carried out on the ASO workers recruited from freelancing sites.
- Vulnerabilities in the Play Store were found and reported.
- New techniques and other information about Black Hat ASO workers was presented.
- Due to the limited sample, we cannot generalize these findings.
- Future research should aim to cut off this limitation. Gather ASO workers from various demographics, with different skill levels etc. in order to obtain a generalized conclusion.

References

- [1] M. Rahman, N. Hernandez, R. Recabarren, S. I. Ahmed, and B. Carbunar, "The Art and Craft of Fraudulent App Promotion in Google Play," presented at the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, Nov. 11-15, 2019, p.p. 2437-2454.
<https://doi.org/10.1145/3319535.3345658>
- [2] Sectigostore.com, '42 Cyber Attack Statistics by Year: A Look at the Last Decade', 2020. [Online]. Available: <https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/>. [Accessed: 21- Aug- 2020].
- [3] H. Saini, Y. S. Rao, T. C. Panda, "Cyber-Crimes and their Impacts: A Review," in *International Journal of Engineering Research and Applications*, vol. 2, no. 2, pp. 202-209, 2012.
- [4] J. White, *Terrorism and Homeland Security*. Belmont, CA, USA: Wadsworth Publishing, 2014.
- [5] E. D. Cristofaro, A. Friedman, G. Jourjon, M. A. Kaafar, and M. Z. Shaq, "Paying for Likes?: Understanding Facebook like Fraud Using Honeypots," presented at the 2014 Conference on Internet Measurement, New York, NY, USA, 2014, p.p. 129-136. <https://doi.org/10.1145/2663716.2663729>
- [6] E. Bursztein et al., "Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild," presented at the 2014 Conference on Internet Measurement, New York, NY, USA, 2014, p.p. 347-358.
<https://doi.org/10.1145/2663716.2663749>