DETECTING MALICIOUS APP IN FACEBOOK THROUGH FRAPPE CLASSIFIER

MOHAMMED RIYAZ PASHA: BTech (computer science & engineering), having hands on experience as professional sap business one consultant in Qatar doha

M DATTATREYA GOUD: MTech, Dep of CSE and working as a Assistant Professor in Arjun Engineering college and Had 6 years of experience in Teaching

ABSTRACT:

Online social media services like Facebook witness an exponential increase in user activity when an event takes place in the real world. This activity is a combination of good quality content like information, personal views, opinions, comments, as well as poor quality content like rumours, spam, and other malicious content. Although, the good quality content makes online social media a rich source of information, consumption of poor quality content can degrade user experience, and have inappropriate impact in the real world. In addition, the enormous popularity, promptness, and reach of online social media services across the world makes it essential to monitor this activity, and minimize the production and spread of poor quality content. Multiple studies in the past have analysed the content spread on social networks during real world events. However, little work has explored the Facebook social network. Two of the main reasons for the lack of studies on Facebook are the strict privacy settings, and limited amount of data available from Facebook, as compared to Twitter. With over 1 billion monthly active users, Facebook is about times bigger than its next biggest counterpart Twitter, and is currently, the largest online social network in the world. In this literature survey, we review the existing research work done on Facebook, and study the techniques used to identify and analyse poor quality content on Facebook, and other social networks. We also attempt to understand the limitations posed by Facebook in terms of availability of data for collection, and analysis, and try to understand if existing techniques can be used to identify and study poor quality content on Facebook.

Keywords: *Online social networks, Spam, Malicious Campaigns, Security and Protection : Access controls, Verification.*

I. INTRODUCTION:

Online social networks (OSN) enable and encourage third party applications to enhance the user experience on these platforms like FACEBOOK. Such enhancements include interesting or entertaining ways of communicating among online friends, and diverse activities such as playing games or listening to songs. For example, Facebook provides developers an API that facilitates app integration into the Facebook user-experience. There are 500K apps available on Facebook, and on average, 20M apps are installed every day. Furthermore, many apps have acquired and maintain a large user base. We have observed that , FarmVille and CityVille apps have 26.5M and 42.8M users to date. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Facebook leading the way with 900M active users. A. FRAppE Lite: FRAppE Lite is a lightweight version that makes use of only the application features available on demand. Given a specific app ID, FRAppE Lite

crawls the on-demand features for that application and evaluates the application based on these features in real time. We envision that FRAppE Lite can be incorporated, for example, into a browser extension that can evaluate any Facebook application at the time when a user is considering installing it to her profile. All of these features can be collected on demand at the time of classification and do not require prior knowledge about the app being evaluated. We use the Support Vector Machine (SVM) classifier for classifying malicious apps. SVM is widely used for binary classification in security and other disciplines. We use accuracy, false positive (FP) rate, and true positive (TP) rate as the three metrics to measure the classifier's performance. Accuracy is defined as the ratio of correctly identified apps (i.e., a benign/malicious app is appropriately identified as benign/malicious) to the total number of apps. False positive rate is the fraction of benign apps incorrectly classified as malicious, and true positive rate is the fraction of benign and malicious apps correctly classified (i.e., as benign and malicious, respectively).

II. LITERATURE SURVEY

1) Detecting and Characterizing Social Spam Campaigns

Authors: Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao.

Description: In this paper, authors presented an initial study to quantify and characterize spam campaigns launched using accounts on online social networks. They studied a large anonymized dataset of asynchronous ―wall‖ messages between Facebook users. We analyze all wall messages received by roughly 3.5 million Facebook users (more than 187 million messages in all), and use a set of automated techniques to detect and characterize coordinated spam campaigns. System detected roughly 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts. Authors found that more than 70% of all malicious wall posts advertise phishing sites. They study the characteristics of malicious accounts, and see that more than 97% are compromised accounts, rather than ―fake‖ accounts created solely for the purpose of spamming. Finally, when adjusted to the local time of the sender, spamming dominates actual wall post activity in the early morning hours, when normal users are asleep.

2) Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals

Authors: Pern Hui Chia, Yusuke Yamamoto, N. Asokan

Description: Third-party applications (apps) drive the attractiveness of web and mobile application platforms. Many of these platforms adopt a decentralized control strategy, relying on explicit user consent for granting permissions that the apps request. Users have to rely primarily on community ratings as the

signals to identify the potentially harmful and inappropriate apps even though community ratings typically reflect opinions about perceived functionality or performance rather than about risks. With the arrival of HTML5 web apps, such user-consent permission systems will become more widespread. We study the effectiveness of user-consent permission systems through a large scale data collection of Facebook apps, Chrome extensions and Android apps. The analysis confirms that the current forms of community ratings used in app markets today are not reliable indicators of privacy risks of an app. We find some evidence indicating attempts to mislead or entice users into granting permissions: free applications and applications with mature content request more permissions than is typical; ―lookalike‖ applications which have names similar to popular applications also request more permissions than is typical. Authors find that across all three platforms popular applications request more permissions than average.

III. SURVEY OF PROPOSED SYSTEM

Currently, malicious apps often do not include a category, company, or description in their app summary. To detect the malicious facebook applications which may affects to user's private information on his/her profile. As we see user did not get much information about application expect name of that application while installing as a result no security available on facebook. Recently, hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications which can provide a lucrative business for hackers, given by the popularity of OSNs, with Facebook leading the way with 900M active users. There are many ways that hackers can benefit from a malicious app. To make matters worse, the deployment of malicious apps is simplified by ready-to-use toolkits. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day

IV. THE PROPOSED FRAMEWORK

In this work, we develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from MyPageKeeper. To build FRAppE, we use data from MyPageKeeper, a security app in Facebook that monitors the Facebook profiles of 2.2 million users. We analyse 111K apps that made 91 million posts over nine months. This is arguably the first comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and understanding malicious apps, and synthesizes this information into an effective detection approach. We have introduced two features i.e. classifiers to detect the malicious apps FRAppE Lite and FRAppE . In first classifier it detect the initial level detection e.g. apps

identity number , name and source etc. and in second level detection the actual detection of malicious app has been done.

Advantageous

Facebook Rigorous Application Evaluator is arguably is the tool to detect malicious apps.

It provides security to users profiles from malicious apps.

VI. CONCLUSION

In this survey, we explored various research attempts towards exploring the Facebook network, analyzing malicious content on it, and analyzing events on online social media in general. The aim of this survey was to look at relevant literature, which could aid in studying and combating malicious user generated content spread on Facebook during events. In order to keep this survey focused, we did not cover a variety of possibly relevant research areas including detection of compromised / fake accounts, and sybil nodes in the Facebook network, detection of spam on other social networks like Twitter, credibility / trustworthiness of information of user generated content, and event detection in online social media. We also looked at the various challenges and limitations posed by Facebook (as discussed in Section 3). Apart from technical limitations, there exist various research gaps in existing literature, which are yet to be addressed and explored.

VI REFERENCES

1. C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2, 2011
2. 2. Chia, Y. Yamamoto, and N. Asokan. Is this app safe? A large scale study on application permissions and risk signals. In WWW, 2012.
3. 3. H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary. Towards online spam filtering in social networks. In NDSS, 20124. J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? In SOUPS, 2011
4. 4. J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? In SOUPS, 2011.
5. 5. Lee, J. Caverlee, and S. Webb. Uncovering social spammers: social honeypots + machine learning. In SIGIR, 2010
6. 6. Lee and J. Kim. Warningbird: Detecting suspicious urls in twitter stream. In NDSS, 2012.
7. 7. Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: user expectations vs. reality. In IMC, 2011.

8 R. Naraine, ―Hackers selling $25 toolkit to create malicious Facebook apps,‖ 2011 [Online]. Available: http://zd.net/g28HxI

9 HackTrix, ―Stay away from malicious Facebook apps,‖ 2013 [Online]. Available: http://bit.ly/b6gWn5

10 M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, ―Efficient and scalable socware detection in online social networks,‖ in Proc. USENIX Security, 2012, p. 32.

11 H. Gao et al., ―Detecting and characterizing social spam campaigns,‖ in Proc. IMC, 2010, pp. 35–47.

12 H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, ―Towards online spam filtering in social networks,‖ in Proc. NDSS, 2012.

Author Details:

MOHAMMED RIYAZ PASHA: BTech (computer science & engineering), having hands on experience as professional sap business one consultant in Qatar doha

M DATTATREYA GOUD: MTech, Dep of CSE and working as a Assistant Professor in Arjun Engineering college and Had 6 years of experience in Teaching