International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Detecting Malicious Social Networks Applications using FRAppE

Avinash Adhav[1], Pravin Masal[2], Suraj Ghodake[3], Abhilash Lokhande[4], Chaitanya Bhosale[5]

[1234] *Bachelor of Computer Engineering, Department of Computer Engineering, MMIT, Maharashtra, India.*
[5]*Professor, Dept. of Computer Engineering, MMIT, Maharashtra, India.*

Abstract - *Online Social Networks applications are one of the reasons for Online Social Networks attractiveness. Unluckily, many user are not alert of the fact that many malicious Online Social Networks applications survive. With 20 million installs a day, third party applications are a major reason for the attractiveness and addictiveness of Online Social Networks. But, cyber criminals have realized the probable of using applications for spreading malware and spam like unsolicited mail. The problem is already important, as we find that at least 13% of applications in the model datasets are malicious. Since, the research community has paying attention on discovering malicious posts and campaign. Online social networks services like Online Social Networks eyewitness an exponential boost in consumer action while an incident takes place in the actual world. This activity is a mixture of high-quality content similar to information, private views, opinions, comments, as well as poor quality content like spam, rumors, and other malicious content. Although, the high-quality content makes online social networks a wealthy source of information, use of poor quality content can degrade user understanding, and have unsuitable blow in the real globe. In addition, the huge attractiveness, reach and promptness of online social networks services across the world makes it essential to monitor this reduce and activity the invention and spread of poor quality content. Numerous studies in the past have analyzed the content spread on social networks throughout real world events. We also go to recognize the boundaries posed by Online Social Networks in terms of availability of data for collection, and investigation, and try to recognize if presented techniques can be used to recognize and study deprived quality content on Facebook.*

Key Words: **Malicious Apps, Privacy, Online Social Networks, Security, Social Networking Applications, Facebook Apps, Naïve Bayes, Machine Learning.**

1. INTRODUCTION

In the Internets last 2 decades, multinetworks content is especially formed and spread. In order to professionally position content in Online Social Networks. Online social networks have stamped its power as one of the major information propagators on the Internet. OSN services have all local, cultural, and language limits, and provided each Internet user on the earth with an identical chance to talk, and be heard. Almost 25% of the world's people use at least one social networks service today. People across the globe actively use social networks platforms like Twitter and Facebook for spreading learning or information about real world events these days. A recent study revealed that social networks activity increases up to 200 times throughout key events like elections, sports, or natural calamities. This activity contains a lot of information about the events, but is also severe abuse like spammer, rumor propagation, and misinformation, and has thus drawn huge concentration from the computer science research community. So far this stream of information is generated and consumed in real time, and by ordinary users, it is tough to take out helpful and actionable content. Twitter, in exacting, has been widely studied by researchers during real-world events [Becker et al. 2011; Hu et al. 2012; Sakaki et al.. 2010; Kwak et al. 2010; Weng and Lee 2011]. However, few studies have looked at the content increase on social networks platforms other than Twitter to study real-world events [Hille and Bakker 2013; Chen and Roy 2009; Osborne et al. 2012]. Surprisingly, there has been little work on studying content on Facebook for the period of actual world events [Westling 2007], which is 5 times bigger than Twitter in conditions of the number of monthly active users. In this survey, we seem at the existing work done in the space of identification and analysis of malicious content on Facebook, and event analysis on online social networks in general.

Lately, hackers and malicious users have on track of taking advantage of the popularity of these third-party applications Platform and deploying malicious applications. Malicious applications can give a profitable commerce for hackers, given the status of OSN, with Facebook most significant the way with 900M lively users. There are many ways that hackers can take advantage from a malicious app:

a) The app can attain huge number of users and their friends to increase spam.

b) The app can get users private information such as residence town, e-mail address and gender, and

c) The app can “make a replica” by making other malicious applications popular.

In other language, there is motive and chance, and as a result, there are many malicious applications spreading on Facebook every day.

Regardless of the above doubts, today a user has very incomplete information at the instance of installing an app on his Facebook profile. In other words, the difficulty is the following: specified an app’s identity number (the unique identifier assigned to the app by Facebook), can we discover if the app is malicious?

1.1 Problem Statement

Presently, malicious applications frequently do not include a category, corporation, or explanation in their app review. To discover the malicious facebook applications which may affects to user private information on his/her profile. As we know user did not get a large amount of information about application imagine name of that application while installing as a result no security available on Facebook.

1.2 Attack techniques

In order to recognize and contain malicious posts on Facebook, or any OSN, it is essential to search and understand the techniques that are, or can potentially be deployed by attackers to spread such content. To this end, Patsakis et al. [Patsakis et al. 2009] described how Facebook can be exploited and transformed into an attack platform, in order to gain some responsive data, which can complete a ideal attacking against a user. Authors created a Facebook application for demonstration purposes so as to on the exterior was a simple application, but on the background it composed useful data. This app executed malicious code on the victim's browser, and collected the IP address of the user-victim, the browser version, the OS platform and whether some unique ports are open or closed. This data was then transmitted to the authors over email. Authors also pointed out that their app was indexed on the main list of Facebook applications, regardless of the fact that the explanation of app obviously declared that it was generating malicious app, and had been formed for penetration testing purposes. Huber et al. presented a friend-in-the-middle attack during hijacking session cookies. Authors explained how it was possible to pretend to be the victim using this technique, and interact with the network without appropriate authorization. However, this technique was projected in 2011, when using HTTPS to connect to the website was elective.

1.3 BACKGROUND

To discover malicious post MyPage-Keeper is used, a security app which was launched by Facebook in June 2011. It monitors the Facebook profiles of 2.2 million users. It crawls user's wall post and news feed constantly and discovers malicious posts and notifies the infected users. Over 111K applications are analyzed that ended 91 million posts over 9 months. This review paper presents a complete study concentrating on malicious Facebook applications that focuses on quantifying, profiling, and understanding malicious applications and synthesizes this information into an effective discoverion approach. MyPageKeeper mainly discovers malicious posts in Facebook and inform victims. The Sample dataset contains applications for which the ground fact is, they are malicious or not. For collecting sample malicious applications, we use a heuristic: if a post is flagged by MyPageKeeper as malicious which is posted by an app, they app is malicious. Then same amount of benign applications are composed to make the comparison fair. Benign applications are those applications who are not part of malicious applications and also vetted by socialbaker.com, a website that collects app statistics. But the major enabling factor is malicious Facebook app.

Fig -1: Malicious Applications

ss

1.4 PROCEDURE OF MALICIOUS APPLICATIONS:

Malicious Facebook applications characteristically work as follows.

1) Hackers encourage users to install the app, typically with some fake promise (e.g., free iPads).

2) Once a user installs the app, it redirects the user to a Web page where the user is requested to complete tasks, such as completing a survey, yet again with the lure of fake rewards.

3) The app after that accesses private information (e.g., birth date) from the user's profile, which the hackers can potentially use to earnings.

4) The app makes malicious posts on behalf of the user to attract the user's friends to install the same app.

This way the sequence continues with the app or colluding applications getting more and more users. individual information or surveys can be sell to third parties to ultimately profit the hackers. Malicious hackers create posts into compromised user's wall. Their friends see the post, click the link which leads to the malicious app installation page as shown in Fig. Once installed, they forward users to different pages for collecting victims special information and Make her whole surveys so that they can make money. Once the app is installed, hackers get authorization to post any time on the victims wall. So, they make the similar post and become visible to victims friend's news feed and thus the cycle repeats and the app spreads in Facebook.

Facebook enables third-party developers to present services to its users by means of Facebook applications. Unlike typical desktop and smart phone applications, installation of a Facebook application by a user does not involve the user downloading and executing an application binary. Instead, when a user adds a Facebook application to her profile, the user grants the application server:

1) Permission to access a subset of the information scheduled on the user's Facebook profile (e.g., the user's e-mail ad-dress).
2) Permission to execute certain events on behalf of the user (e.g., the ability to post on the user's wall). Facebook grants these permissions to any application by handing an token to the application server for each user who installs the application.

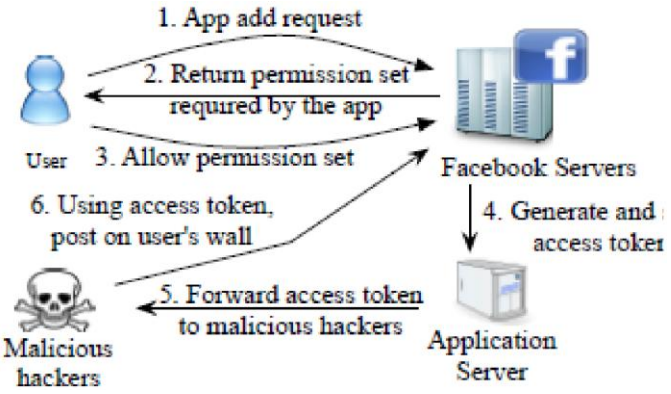

Fig -2: Steps involved in hackers using malicious applications to get access tokens to post malicious content on victims' walls.

Hackers have on track of taking advantage of the attractiveness of this third-party applications and deploying malicious applications. Malicious applications can give a beneficial commerce for hackers, given the fame of OSNs, with Facebook in vital way with 900 Million active users. There are numerous ways that hackers can benefit from a malicious app.

2. LITERATURE SURVEY

2.1 A Large Scale Study on Application Permissions and Risk Signals

Authors: Pern Hui Chia, Yusuke Yamamoto, N. Asokan
Description: Third-party applications capture the popularity of web and platforms providing mobile application. a lot of of these platforms allow a decentralized control approach, relying on unambiguous user permission for soft Permissions that the applications require. Users have to rely mainly on community ratings as the signals to categorize the potentially unsafe and inappropriate applications even though community ratings classically reflect opinions regarding Supposed functionality or performance rather than regarding risks. To study the compensation of user-consent permission systems through a huge data collection of Facebook applications, Chrome extensions and Android applications. The study confirms that the present forms of community ratings used in app markets today are not reliable for representing confidentiality risks an app creates. It is found with some evidences, representing attempts to misinform or attract users for yielding permissions: free applications and applications with mature content request; "look alike" applications which have same names as that of well-liked applications also request more permissions than is typical. Authors find that across all three platforms popular applications request more permissions than average.

2.2 Online Social networks Applications: Exploring a More secure Framework

Authors: Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, Gorrell Cheek
Description: OSNs such as Orkut, Facebook and others have grown-up quickly, with hundreds to millions of active users. A new feature provided on numerous sites is social applications and services provided by third party developers that supply additional functionality linked to a user's profile. However, present application platforms put users at risk by permitting the discoverion of massive amounts of private data and information to these applications and their developers.

3. PROPOSED FRAMEWORK

We are going to implement the system of efficient categorization technique for identifying whether an app is malicious or not. To build this system, we employ data from MyPageKeeper. This is possibly the first complete revision focusing on malicious applications. Our base data source MyPageKeeper is a facebook security application which can discovers only malicious posts. That's why we are going to implement system which will discover the malicious applications on online social networks, where the malicious applications are bunch of malicious post.

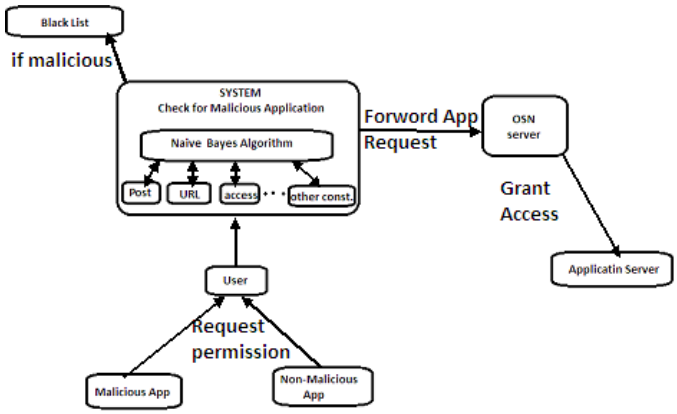

Fig -3: Architecture Diagram

3.1 IMPLEMENTATION MODULES

a) Malicious and benign app profiles drastically differ
b) The emergence of AppNets: applications collude at huge scale
c) Malicious hackers pretend to be applications.
d) FRAppE can discover malicious applications with 99% correctness

a) Malicious and normal app profiles significantly differ:

We scientifically profile applications and show that malicious app profiles are considerably dissimilar than those of normal applications. A striking inspection is the "laziness" of hackers; many malicious applications have the identical name, as 8% of unique names of malicious applications are each used by more than 10 dissimilar applications. generally, we profile applications based on two classes of features:(a) those that can be obtained on-demand given an application's identifier (e.g., the permissions necessary for the app and the posts in the application's profile page), and (b) others that require across-user view to collect information across time and across applications (e.g., the posting activities of the app and the comparison of its name to other applications).

b) The appearance of AppNets: applications collude at huge scale:

We perform a forensics inquiry on the malicious app bionetwork to spot and quantify the techniques used to encourage malicious applications. The most motivating result is that applications plan and work together at a huge scale. Applications support other applications via posts that point to the "promoted" applications. If we explain the collusion relationship of promoting-promoted applications as a graph, we find 1,584 advertiser applications that support 3,786 other applications. Furthermore, these applications form large and highly-dense connected components, furthermore, hackers use fast-changing indirection: applications posts have URLs that spot to a website, and the website dynamically redirects to a lot of different applications; we find 121 such URLs that point to 4,556 different malicious applications over the course of a month. These observed behaviors point to well-ordered offense: one hacker control a lot of malicious applications, which we will call an AppNet, since they seem a parallel concept to virus.

c) Malicious hackers impersonate applications:

We were amazed to find well-liked good applications, such as 'Farmville' and 'Facebook for iPhone', posting malicious posts. On additional inquiry, we found a slack of authentication rule in Facebook that enabled hackers to make malicious posts come into view as though they came from these applications.

d) FRAppE can spot malicious applications with 99% accuracy:

We develop FRAppE (Facebook's Rigorous Application Evaluator) to discover malicious applications either by means of only features that can be obtained on-demand or using both on-demand and aggregation based app information. FRAppE Lite, which only uses information available on-demand, can discover malicious applications with 99.0% accuracy, with low false positives (0.1%) and false negatives (4.4%). By adding aggregation-based information, FRAppE can discover malicious applications with 99.5% accuracy, with no false positives and lower false negatives (4.1%).

4. CONCLUSIONS

OSN Applications present a suitable means for spammers to spread harmful content on Social networks. In this project, using a huge amount of malicious social applications observed more than a nine month period, we showed that malicious applications differ drastically from normal applications with respect to a number of features. That's Why we are using naïve bayes classifier to classify the applications with respect to their feature for Example, post, URL, access permissions etc.

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on Detecting Malicious Social Networks Applications using FRAppE We would like to take this opportunity to thank my internal guide Prof. C. S. Bhosale for giving me all the help and guidance we needed. We are really grateful to them for his kind support. Their valuable suggestions were very helpful.

We are also grateful to Prof. P. M. Daflapurkar, Head of Computer Engineering Department, Marathwada Mitra Mandals Institute of Technology for her indispensable support, suggestions.

In the end our special thanks to Prof. G. V. Mane for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

REFERENCES

[1] G. Magno, T. Rodrigues, and V. Almeida., "Detecting spammers on Twitter." In CEAS,2010.

[2] Hongyu Gao, Yan Chen, Kathy Lee† Northwestern University Evanston, ILUSA "Online Spam Filtering System On Social Network"In NDSS,2012.

[3] Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, Gorrell Cheek,"Social Applications: Exploring a More Secure Framework." In SOUPS,2009.

[4] Sundus Hassan, Muhammad Rafi, Muhammad Shahid Shaikh "Comparing SVM and Naïve Bayes Classifiers for Text Categorization with Wikitology as knowledge enrichment"

[5] C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2, 2011

[6] Chia, Y. Yamamoto, and N. Asokan. Is this app safe? A large scale study on application permissions and risk signals. In WWW, 2012.

[7] 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

[8] J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? In SOUPS, 2011.

BIOGRAPHIES

Avinash Adhav received the diploma in Information Technology from Government Polytechnic Awsari and currently pursuing Bachelor of Computer Engineering form Marathwada Mitra Mandal's Institute of Technology affiliated to Savitribai Phule Pune University.

Pravin Masal received the diploma in Computer Engineering from Government Polytechnic Awsari and currently pursuing Bachelor of Computer Engineering form Marathwada Mitra Mandal's Institute of Technology affiliated to Savitribai Phule Pune University

Suraj Ghodake received the diploma in Information Technology from Government Polytechnic Awsari and currently pursuing Bachelor of Computer Engineering form Marathwada Mitra Mandal's Institute of Technology affiliated to Savitribai Phule Pune University.

Abhilash Lokhande received the diploma in Information Technology from Government Polytechnic Awsari and currently pursuing Bachelor of Computer Engineering form Marathwada Mitra Mandal's Institute of Technology affiliated to Savitribai Phule Pune University.

Prof. Chaitanya Bhosale M.E. (CE) is a lecturer of computer department in Marathwada Mitra Mandal's Institute of Technology affiliated to Savitribai Phule Pune University with a total experience of 1.5 years. His areas of interest are Database, Data Mining.