International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 04, April 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

DETECTING MALICIOUS APPLICATIONS ON OSN's

Pranav Shukla[1],Ganesh Tekale[2],Raviraj Shedage[3],

Tabassum Biradar[4], Prof. Yogesh Lonkar[5]

[1,2,3,4]Department of Computer Engineering,

GSMCOE, Balewadi, Pune (India)

[5]Assistant Prof. Gsmcoe Balewadi, Department of Computer Engineering, (India)

ABSTRACT

In this paper, we develop FRAppeR, a web app for efficient classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from MyPage Keeper, a security app in Facebook that monitors the Facebook profiles of users. This is arguably the rest comprehensive study focusing on malicious apps that focuses on quantifying, profiling, and understanding malicious apps and synthesizes this information into an effective detection approach. FRAppE can detect malicious apps high accuracy. We develop FRAppeR (Facebooks Rigorous Application Evaluator using Reviews) to identify malicious apps using and also by using features that can be obtained on-demand or using both on-demand and aggregation-based app information. FRAppeR Lite, which only uses information available on-demand, can identify malicious apps with low false positives and high true positives. By adding aggregation-based information, FRAppE can detect malicious apps with We conduct a forensics investigation on the malicious app ecosystem to recognise and quantify the techniques used to promote malicious apps. We nd that apps collide and collaborate at a massive scale. Apps promote other apps via posts that point to the promoted apps. If we describe the collusion relationship of promoting promoted apps as a graph, we nd 1584 promoter apps that promote other apps. Furthermore, these apps form large and highly dense connected components. Furthermore, hackers use fast-changing indirection: Applications posts have URLs that point to a Web site, and the Web site dynamically redirects to many different apps; we send such URLs that point to different malicious apps over the course of a month. These observed behaviours indicate well-organized crime: One hacker controls many malicious apps, which we will call an app-net, since they seem a parallel concept to botnets.

Keywords: Facebook rigorous application evaluator, malicious Facebook application, third-party apps, malware, computer spam, FRAppeR, FRAppeR

I INTRODUCTION

As of the surveys conducted the number of active monthly users for Facebook is 1.79 million [1].Out of these 1.79 billion users around 989 million users use the mobile app for accessing it. The OSN (On-line Social Network) particularly Facebook gathers users private information while creating account. This private information forms a attractive target for marketing companies, identity thieves, spammers and phishers [2].The

ISSN (O) 2454-9665
ISSN (P) 2454-0663

OSN's are aware of the arising out of private information stealing and they provide the user with many kind of settings to hide ones identity.

The Smartphone market has been boosted. Since smartphone satisfies the terms of Pervasive Computing i.e. computing for anyone, anywhere; has led to increase in total number of people using apps. According to a survey the average amount of time spent by using apps in US is around 81 minutes[3][see fig. 1] .Thus the social networking sites also provide the mobile apps for accessing their site. The number of apps present on the Facebook is 550,000[2], mostly provided by Third-Party developers. The personal information includes the Date of Birth, Contacts of the user, email, etc. The app development needs the spreading of information of the app such that the number of people using the app increases. The OSN's are one of the best places to share the apps and increase the number of downloads. While sharing the apps, the owner of apps can collect the user information and ask to share with the same to its contact or will itself use the contacts and propagate the app. Sometimes the app gathers information and will be used for some illegitimate purposes.

The OSN's apply strict terms and conditions on the developer which are to be accepted by the developer. The Third-party developer is provided with libraries to smoothly embed the software into the OSN. The integration between the Social Network and the third-party applications gives rise to the problem of privacy and security issues especially w.r.t user's private information. The OSN applies rules for accessing information; but once the information is accessed the OSN has no restrictions on how the gathered information is processed and used.

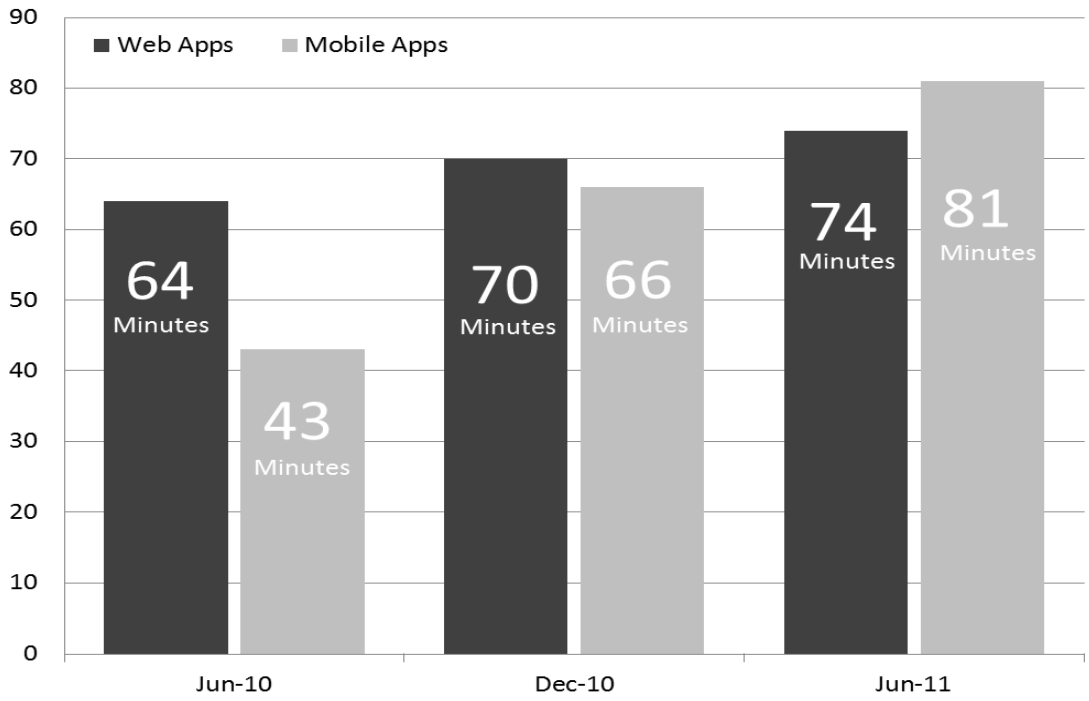

Fig.1: Time spent by users on mobile apps. (US)

Moreover, sometimes the apps propagate each other. The Third-party app downloaded asks users to download an app to use the intended application. Thus increasing the number of downloads for the app and increasing the app ranking. The deployment of apps is made far easier as the toolkits required are easily available for a meagre cost [5] and there is no any commercial software which can detect them.

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 04, April 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

II BACKGROUND

Before classifying whether an application is malicious or not we need to understand the working of applications on Facebook.

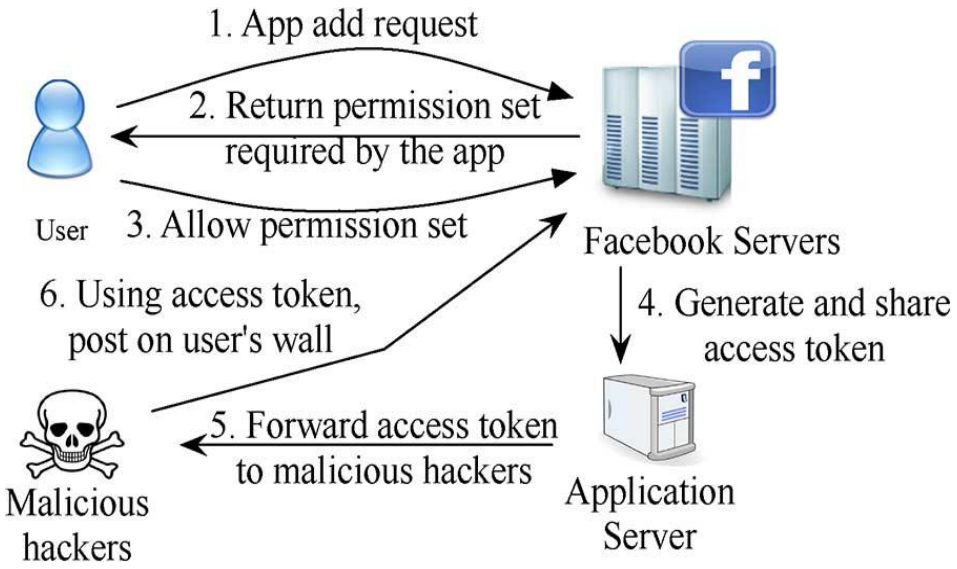

Fig.2: Steps involved in propagation of malicious apps

Step 1:- The user is tempted to download the app by giving good grounds.

Step 2:- The user is asked to complete some tasks by completing some surveys with a lure for something

Step 3:-In this way the developer gets the different private information of the user and this can be used to make profit.

Step 4:-The malicious app will make use of the information and make malicious apps on behalf of user post on the walls of user friends for same app or some other app. [4]

III RELATED WORK

As mentioned in the introduction the proposed design elaborate about what the actual system is. As shown in diagram Our system will detect weather the submission is malicious or not By using naive Bayes classifier algorithm .As shown in fig App is popped to user and user gives request to server to use this app but before this request is going to proceed we will check whether the application is malicious or not by applying constraints on app (constraints such as is that app have suspicious redirecting url?, app post contents, app close functions etc.). Otherwise it will pass that app request to server. Then server gives authorization to user to access that app.

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 04, April 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

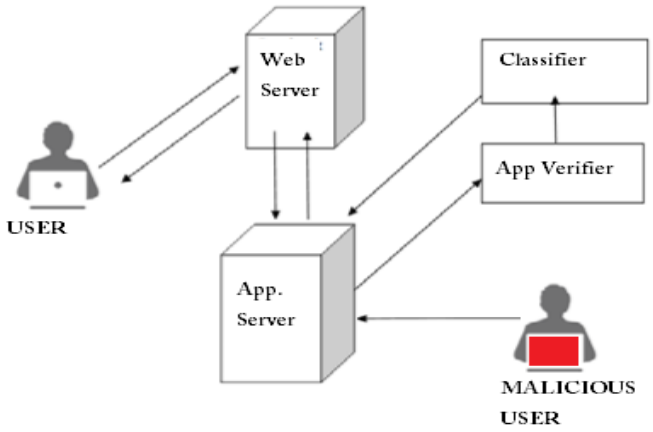

Fig.3 Basic Block Diagram Of Propsed System

The proposed FRAppeR will be having following

1. The classification based on the RANKING.
2. The classification based on the RATING
3. The classification based on the REVIEW
4. Application can classify the app into suspicious and malicious

We have developed new framework FRAppeR, a set of efficient techniques for figuring out whether or not an app is malicious or no longer. To build FRAppeR, we use statistics from MyPage- Keeper, a safety app in Facebook. We locate that malicious applications extensively differ from benign applications with appreciate to two lessons of features: On-Demand Features and Aggregation-Based Features. We gift variations of our malicious app classifier— FRAppeR Lite and FRAppeR. FRAppeR Lite is a lightweight model that uses handiest the utility features available on call for. Given a particular app ID, FRAppeR Lite crawls the on-demand functions for that application and evaluates the utility based totally on these features in real time. FRAppeR—a malicious app detector that makes use of our aggregation-based totally functions similarly to the on-demand functions. The proposed work is arguably the primary complete observe specializing in malicious Facebook apps that specializes in quantifying, profiling, and information malicious apps and synthesizes this information into an effective detection approach. Several capabilities used by FRAppeR, along with the popularity of redirect URIs, the wide variety of required permissions, and the use of different customer IDs in app set up URLs, are robust to the evolution of hackers. Not using one of a kind patron IDs in app installation URLs might restrict the ability of hackers to instrument their applications to propagate each other

IV RESULTS

data size in kb	Current System
01-03-2017	25
02-03-2017	44
03-03-2017	40

ISSN (O) 2454-9665
ISSN (P) 2454-0663

04-03-2017	62
05-03-2017	75
06-03-2017	95

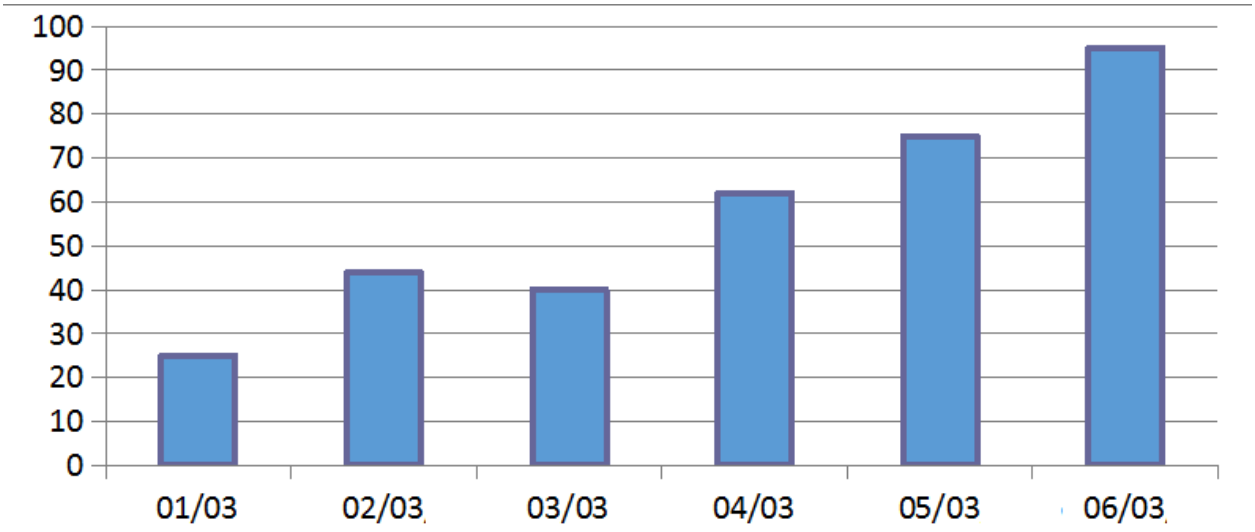

Fig. 4 Different ranking phases of a leading Event

Session based event details of Fraud app Identification, In each leading event, an App's ranking first increases to a peak position in the leader board (i.e., rising phase), then keeps such peak position for a period (i.e., maintaining phase), and finally decreases till the end of the event (i.e., recession phase). Fig. shows an example of different ranking phases of a leading event. Indeed, such a ranking pattern shows an important understanding of leading event.

V APPLICATIONS

Fraud Detection System is a Web-based security solution that can signal the threat of fraud apps before user fall prey to the perpetrators. It analyses suspicious behaviour and produces reports for security and risk mitigation purposes.

VI ADVANTAGES AND LIMITATION

Advantages

1. It classifies apps into suspicious and malicious
2. It can be applied on various platforms (on Facebook, Play Store or other OSN's)
3. It uses the comments, user reviews to classify

Limitations

The classification usually takes a long time to classify as it has to check every review. Thus it is a point of technical improvement.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

VII CONCLUSION

Our system proposes a convenient approach for user to identify hackers, who spread malicious apps on fb. However, little is tacit about the characteristics of malicious apps and how they function. In this work, making use of a enormous physique of malicious Facebook apps discovered over a 9 month dated, we exhibited that malicious apps differ significantly from benign apps with admire to a few elements. For example, malicious apps are much more possible to share names with different apps, and they often request fewer permissions than benign apps. Leveraging our explanations, we developed FRAppeR, a proper classifier for detecting malicious fb purposes. Most curiously, we painted the emergence of App Nets colossal corporations of tightly linked functions that promote each other. We will be able to continue to dig deeper into this approach of malicious apps on fb, and we optimism that fb will benefit from our endorsements for reducing the menace of hackers on their podium.

REFERENCES

[1] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[2] PoX: Protecting Users from Malicious Facebook Applications By Manuel Egele, Andreas Moser, Christopher Kruegel Engin Kird

[3] PROFESSIONAL Mobile Application Development by Jeff McWherter,Scott Gowella

[4] Detecting Malicious Facebook Applications by Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos

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