ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Detection of Malicious Users in Facebook Applications Using Frappe

S.Sreekanth [1], G.Sravya [2], K.Soujanya Sravya [3], K.Chandana [4].

Associate Professor, Department of CSE, Guru Nanak Institutions, Ibrahimpatnam, Hyderabad, India [1]

B.Tech Student, Department of CSE, Guru Nanak Institutions, Ibrahimpatnam, Hyderabad, India [2]

B.Tech Student, Department of CSE, Guru Nanak Institutions, Ibrahimpatnam, Hyderabad, India [3]

B.Tech Student, Department of CSE, Guru Nanak Institutions, Ibrahimpatnam, Hyderabad, India [4]

ABSTRACT: Nowadays, Facebook applications are being used by massive users because these can be considered as one of the reasons for Facebook attractiveness. They enable the users to experience various online social networks and enhance them to use these applications. Users may also find it interesting to communicate with other people and play online games. But unfortunately, they could not differentiate between good applications and malicious applications. With 20 million installs a day, the hackers have found a way to spread malware and spam through these apps. In this paper, our major aim is surveying and developing FRAppE-Facebook's rigorous Application Evaluator, a tool which is used for detecting malicious Facebook applications, thus helping a user to detect malicious apps with 99% accuracy. There are about 2.2 million people using facebook, so in order to develop FRAppE, we need to gather information by observing the posting behavior of approximately 111K Facebook apps. Firstly we identify features that are used to differentiate malicious and benign apps and then identify the mechanisms that these apps used to propagate. It is fascinating that many of these apps collude and assist each other. In this we find 1584 apps enable the viral propagation of 3723 other apps through posts. In a long term, we see FRAppE as an step to warn users before installing any apps.

KEYWORDS: Facebookapps, malicious, spam, FRAppE

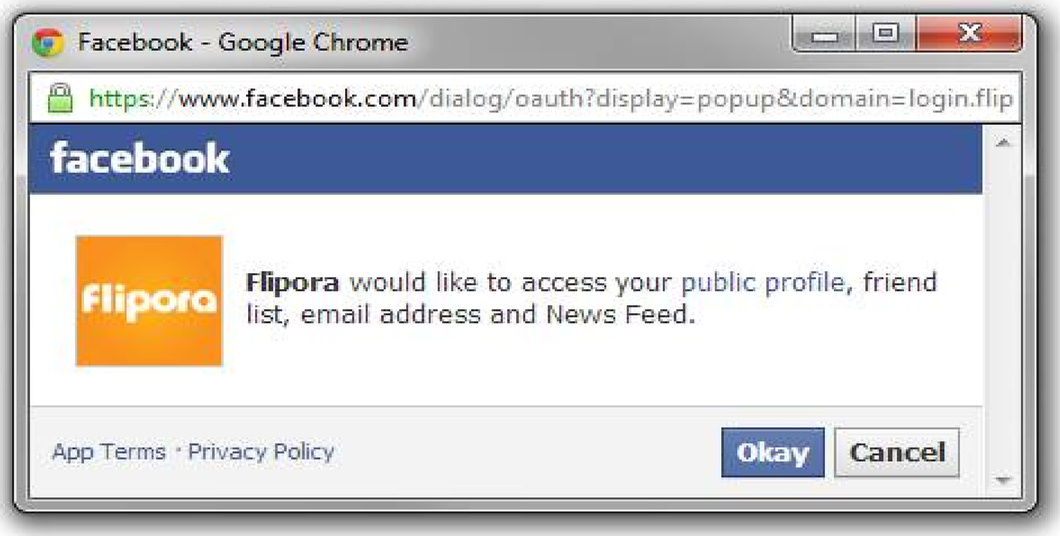
I. INTRODUCTION

Generally, Online Social Networks enable and inspirit the third party applications to enrich the user experience on these platforms. Users therefore find it interesting to communicate with online friends, share information, play games, listen to music, etc. Apart from these, there are 500K apps which are available on Facebook[1] and 20M apps are installed everyday[2]. For example, Candy Crush and Farm ville apps have 26M to 45.6M users presently. Cyberpunks have started taking this as an advantage and they are trying to deploy malicious applications[3]-[5]. Though this has become a profitable business for these hackers, there are also certain other ways that hackers can benefit from :

1. The app can reach to maximum number of users and their friends through spam.
2. It can generate users personal information like e-mail id, mobile no,etc.
3. The app can be used to make other malicious apps popular.

There is an opportunity and risk that many facebook applications are eventually spreading day by day and the user can hardly know about the app, when installing it. In other words the user cannot know about the app whether it is malicious or not. Most research related to spam and malware on Facebook has focused on detecting malicious posts and social spam campaigns[6][7].Currently there is no commercial service, any research based tool to advise a user about the risks of an app. In this paper, we develop FRAppE, an efficient tool for detecting any malicious application which is persistently the first app to study and analyze 111K apps and their posts. This focuses on quantifying, profiling and understanding malicious apps and synthesis this information into effective detective approach.

DOI: 10.15680/IJIRCCE.2017. 05032264


Facebook - Google Chrome
https://www.facebook.com/dialog/oauth?display=popup&domain=login.flip
facebook
Flipora
App Terms · Privacy Policy
Okay
Cancel

Flipora would like to access your public profile, friend list, email address and News Feed.

Fig 1- An example of a malicious app trying to obtain user's details

II. RELATED WORKS

1. Detecting and Characterizing Social Spam Campaigns

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

Description : Authors presented a primary study to calculate and analyze spam campaigns launched on online social networks. They calculated a huge anonymous dataset of asynchronous "wall" messages in between Facebook users. System detected generally 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts. Authors found that extra than 70% of all malicious wall posts advertise phishing sites. To study the distinctiveness of malicious accounts, and see that more than 97% are compromised accounts, rather than "fake" accounts formed solely for the principle of spamming. Finally, when adjusted to the local time of the sender, spamming dominates actual wall post in the early morning hours when users are normally asleep.

2. FRAPPE - For Identifying Third Party Application on Facebook

Authors : Dr.S.Prasanna

Description : Third-party apps are an above acumen for the popularity and addictiveness of Facebook. Unfortunately, hackers accept accomplished the abeyant of application apps for overextension malware and spam. So far, the analysis association has focused on audition awful posts and campaigns. In this paper, we propose FRAppE—Facebook's Rigorous Application Evaluator—arguably the first tool focused on detecting malicious apps on Facebook. To develop FRAppE, we use information gathered by observing the posting behavior of 150K Facebook apps seen across 2 million users on Facebook. First, we analyze a set of appearance that advise us analyze awful apps from amiable ones. For example, we acquisition that awful apps generally allotment names with added apps, and they about appeal beneath permissions than benign apps. Second, leveraging these appropriate features, we show that FRAppE can ascertain awful apps with 99.5% accuracy, with no apocryphal positives and a top accurate absolute rate.

III. EXISTING SYSTEM

In Existing system the hackers have been started taking advantage of popularity in using the third party applications. Through that third party applications the hackers can easily attack on social sites and they are developing malicious applications[9]. As the hackers found 900million active users in the facebook[10] so as to hack the user's information the hacker creates a malicious apps and they get the benefit from that malicious applications by making the other malicious apps popular.

As in existing system it cannot detect the malicious apps it can only identify the spammers, it mainly focuses on the accounts created by the spammers instead of the malicious apps.
In existing system there is no application developed to protect the users from hackers, it mainly concentrated on classifying individual spam but not focused on identifying malicious apps. They also presented techniques to identify compromised accounts and spam campaigns.

IV. PROPOSED SYSTEM

- We implement and develop FRAppE , is an application it identifies the malicious application by using on-demand function and aggregation-based functions. As we build this FRAppE application by using the data from the MyPage-Keeper.
- FRAppE application is used to calculate the efficiency for identifying the malicious application in the social sites.
- FRAppE is used to detect the malicious apps here we use the data from MyPage-Keeper[8] it is a security application in facebook were it manages all the facebook profiles of users as it consists of more than 2.2 million users.
- This is first absolute study where it focuses on malicious facebook applications and also it locus on discern, compute and delineate malicious apps and integrate this information into an adequate detection approach.
- The FRAppE consists of malicious application classifiers such as FRAppE Lite and FRAppE in it.
- As the FRAppE Lite is a version where in it consists of light weight version is make use of the on demand.
- To detect the malicious apps the FRAppE uses several features such as reputation of deflect URI's are used for evolution of hackers.

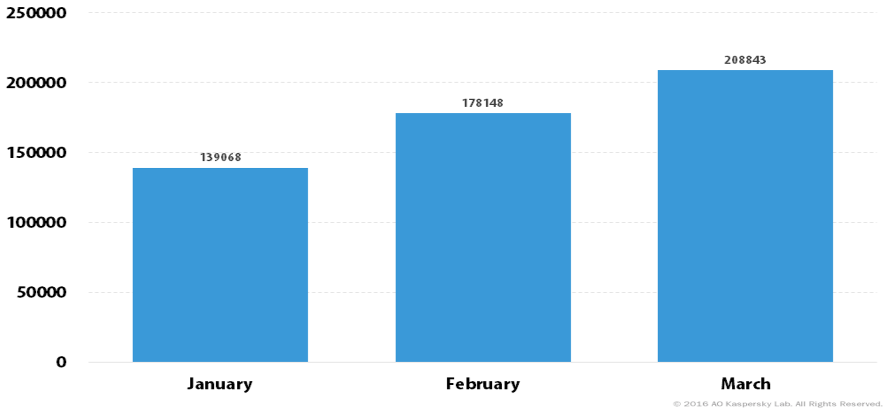


Fig.2 shows the number of users in facebook application which are increasing drastically in each and every month. In the month of January the number of users are 139068 as it has increased gradually in the month of February is 178148 as it has increased when it comes to the month of march is 208843, compare to all the 3 months the users of facebook are increasing day by day.

V. SYSTEM ARCHITECTURE

The nodes which are involved are sender, moderate, receiver. It consists of user, facebook server, application server, hackers. In order to send the file to the receiver, the sender has to check the list of all the nodes which are connected with the sender. In that list he can choose the receiver. In the next step the sender has to analyze the performance of each and every node which are connected with the sender. As in this the performance analysis list will return the result of priority based so that the sender can choose and send the file to moderate node. The file which is received from the sender to the moderate user will analyze the performance so that it can send the data to the other intermediate or the receiver[11]. In the receiver side, the receiver has to select the file path to receive the file from the moderate. So that the receiver can see the received file.

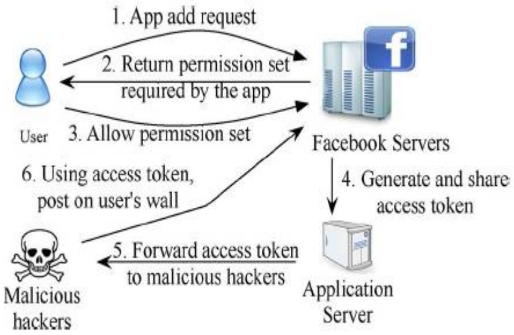

1. App add request
2. Return permission set required by the app
User
3. Allow permission set
Facebook Servers
6. Using access token, post on user's wall
4. Generate and share access token
5. Forward access token to malicious hackers
Malicious hackers
Application Server

Fig 3-Steps involved for hackers to obtain access token and post on user's wall

VI. METHODOLOGY

1. AUTHENTICATION - The user has to register Email ID by providing necessary details. After successful completion of sign up, the user has to login into the application as they provide username and exact password. After the registration the admin sends the generated OTP to the registered Email ID.

2. ACCOUNT REGISTRATION - In this if the user doesn't have Gmail account then they can create a new Gmail account. If the user has a Gmail account then the user can register his account in the Facebook.

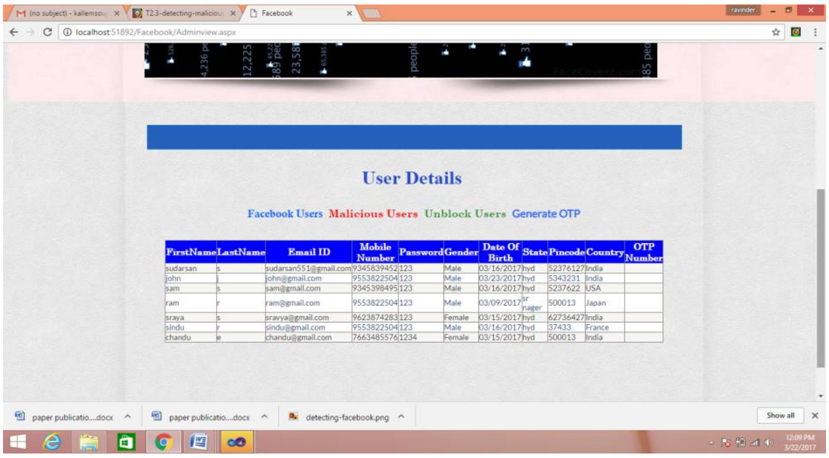
3. OTP VALIDATION - If a user has a Facebook account then the user has to login with provided OTP password and email, if the user is new to the Facebook then the user has to create the account by entering all the fields and register. Once the user have registered it will send the OTP to the email id.

4. FACEBOOK URL - After the successful creation of email id by the user, then the user should enter the FACEBOOK URL to login in Facebook, if already registered with Facebook user can login with generated otp and email id.

5. CHECK FOR MALICIOUS APPS - The user when logs into the Facebook it checks for the malicious apps and links it to attack the user details.

VII. RESULTS

In this paper, we discuss about the detection of any malicious applications using FRAppE. This usually consists of both the user's side and the admin side. The activities of both are discussed as follows:



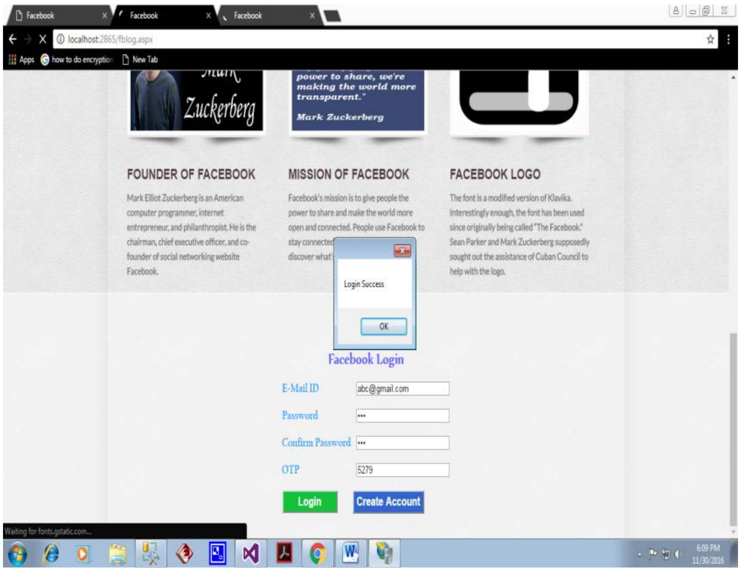
User Details

Facebook Users Malicious Users Unblock Users Generate OTP

FirstName	LastName	Email ID	Mobile Number	Password	Gender	Date Of Birth	State	Pincode	Country	OTP Number
sudarsan	s	sudarsan551@gmail.com	9345839452	123	Male	03/16/2017	hyd	52376127	India	
john	j	john@gmail.com	9553822504	123	Male	03/23/2017	hyd	5343231	India	
sam	s	sam@gmail.com	9345398495	123	Male	03/16/2017	hyd	5237622	USA	
ram	r	ram@gmail.com	9553822504	123	Male	03/09/2017	sr nager	500013	Japan	
sraya	s	sravya@gmail.com	9623874283	123	Female	03/15/2017	hyd	62736427	India	
sindu	r	sindu@gmail.com	9553822504	123	Male	03/16/2017	hyd	37433	France	
chandu	e	chandu@gmail.com	7663485576	1234	Female	03/15/2017	hyd	500013	India	

a) Admin activities

The admin when logged into his account can control all the activities of the user like maintain the details of the user, malicious users and generate OTP for the new users.



power to share, we're making the world more transparent."
Mark Zuckerberg

FOUNDER OF FACEBOOK

Mark Elliot Zuckerberg is an American computer programmer, internet entrepreneur, and philanthropist. He is the chairman, chief executive officer, and co-founder of social networking website Facebook.

MISSION OF FACEBOOK

Facebook's mission is to give people the power to share and make the world more open and connected. People use Facebook to stay connected ... discover what'...

FACEBOOK LOGO

The font is a modified version of Klavika. Interestingly enough, the font has been used since originally being called "The Facebook." Sean Parker and Mark Zuckerberg supposedly sought out the assistance of Cuban Council to help with the logo.

Login Success

OK

Facebook Login

E-Mail ID abc@gmail.com
Password •••
Confirm Password •••
OTP 5279

Login   Create Account

Waiting for fonts.gstatic.com...

b) User activities

Here the user can login into the facebook account and can perform various activities like sending any friend requests, sending and receiving messages, playing games, etc.

VIII. CONCLUSION

The social media applications such as facebook applications are the convenient way to spread the malicious content. The characteristics of the malicious apps is somewhat understood and also how they operate. As we observed over a 9 month period using a large corpus of malicious apps we showed that the malicious apps differ significantly from favorable applications with respect to several functions. We develop the FRAppE application, an accurate classifier to find out the malicious apps in the facebook apps. As we promote this app so as many users can be aware of it. The FRAppE app identifies the 99% of malicious apps in the facebook. We will continue to dig out deeper into the ecosystem of the malicious apps on facebook. We hope that all the facebook users will benefit by reducing the hackers.

ACKNOWLEDGEMENT

We felt great pleasure in submitting this paper on “Detection of Malicious Users in Facebook Applications using Frappe”, first and foremost we express our deep sense of gratitude, sincere thanks to Associate professor S.Sreekanth for the best support ,views, comments and thoughts have really helped us.

REFERENCES

[1] “Wiki:Facebookplatform,”2014[Online].Available:http://en.wikipedia.org/wiki/Facebook_Platform
[2] C. Pring, “100 social media statistics for 2012,” 2012 [Online].
[3] “Pr0file stalker: Rogue Facebook application,” 2012 [Online].
[4] “Which cartoon character are you—Facebook survey scam,” 2012 [Online].
[5] G. Cluley, “The Pink Facebook rogue application and survey scam,” 2012 [Online].
[6] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary. Towards online spam filtering in social networks. In NDSS, 2012.
[7] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. Detecting and characterizing social spam campaigns. In IMC, 2010.
[8]“MyPageKeeper,”[Online]Availablehttps://www.facebook.com/apps/application.php?id=167087893342260
[9]Facebook,PaloAlto,CA,USA,“Facebookplatformpolicies,”[Online].Available:https://developers.facebook.com/policy/
[10] “11 million bulk email addresses for sale Saleprice$90,” [Online].
[11] Facebook, Palo Alto, CA, USA, “Application authentication flow using OAuth 2.0,” [Online].

DOI: 10.15680/IJIRCCE.2017. 05032264