ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Detection of Malicious Application on Online Social Network

Gaurav Parsewar[1], Lalit Kothawade[2], Yogesh Dalvi[3]

BE Student, Department of Computer Engineering, DY Patil Inst. of Engineering, Ambi, Pune, India[1]

BE Student, Department of Computer Engineering, DY Patil Inst. of Engineering, Ambi, Pune, India[2]

BE Student, Department of Computer Engineering, DY Patil Inst. of Engineering, Ambi, Pune, India[3]

ABSTRACT: In on-line Social Networking (OSN), with immeasurable installs every day, third-party apps ar a significant reason for the recognition and effectiveness of Facebook. sadly, hackers have complete the potential of victimization apps for spreading malware and spam, that ar harmful to Facebook users. within the gift generation, the social lifetime of everybody has become related to the net social networks. These sites have created AN extreme amendment within the method we tend to follow our social life. creating friends and keeping connected with them and their updates has become easier. however with their rapid climb, several issues like pretend profiles, malicious application have conjointly big. There are not any possible answer exist to manage these issues. during this project, we tend to came up with a framework with that automatic detection of faux applications or malicious applications is feasible and is efficient.This framework uses the varied classification techniques like FRAppE low-cal and FRAppE to observe the malicious applications. Suppose there's a Facebook application, will the Facebook user confirm that the app is malicious or not. in fact the Facebook user cannot determine that thus our key contribution to developing the FRAppE (Facebook's Rigorous Application Evaluator) are the primary tool that focuses on detective work malicious application on Facebook. To develop FRAppE, we tend to use info gathered by perceptive the posting behavior of 111K Facebook apps seen across a pair of.2 million users on Facebook.

KEYWORDS: Third party applications (TPA), Online Social Network, Malicious apps, Profiling apps, Privacy, Social apps.

I. INTRODUCTION

A Social networking webpage could be a web site wherever each consumer includes a profile and might keep in reality with companions, share their upgrades, meet new people World Health Organization have identical hobbies. These on-line Social Networks (OSN) use web2.zero innovation, which allows shoppers to join forces with one another. These long vary social communication destinations have become quickly and dynamic the approach people keep in reality with one another. the web teams carry people with identical hobbies along, that makes shoppers easier to form new companions. within the gift era, the social existence of everyone has gotten to be connected with the web informal communities. These locales have unrolled Associate in Nursing intense improvement within the approach we tend to look for when our social life. together with new companions and staying in reality with them and their upgrades has gotten to be less hard-to-please.

The larger a part of the OSN ar free but some charge the participation expense and uses this for business functions and no matter remains of them raise money by utilizing the marketing. this will be utilised by the assembly to induce the feelings of individuals generally quickly. The cases of those informal communication locales ar sixdegrees.com, The Sphere, Nex-Opia that is employed as a region of North American country, Bebo, Hi5, Facebook, MySpace, Twitter, LinkedIn, Google+, Orkut, Tuentiutilised as a region of European country, Nasza-Klasa in Polska, Cyworld for the foremost half utilised as a region of Asia, so on ar a share of the documented long vary social communication sites.Online informal organizations (OSN) empower and urge outsider applications to upgrade the consumer expertise on these stages like FACEBOOK. Such enhancements incorporate fascinating or entrancing strategies for transference

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

among on-line companions, and numerous exercises, as an example, taking part in recreations or paying attention to melodies. As of late, programmers have begun exploiting the prominence of this outsider applications stage and causation malignant applications. Malevolent applications will provides a profitable business to programmers, given the prevalence of OSNs, with Facebook driving the route with 900M dynamic shoppers.
There area unit various ways in which programmers will profit by a malevolent application:

- The app will reach massive numbers of users and their friends to unfold spam,
- The app will acquire users' personal data like email address, home town, and gender, And
- The app will "re-produce" by creating alternative malicious apps in style.

Malicious apps area unit widespread and that they simply unfold, as associate infected user loses the protection of all its friends. So the analysis community has paid very little attention to social apps specifically. Most analysis associated with spam and malware on Facebook has centered on sleuthing malicious posts and social spam campaigns. A recent work studies however app permissions and community ratings correlate to privacy risks of Online social networking apps. Finally, there area unit some community-based feedback driven efforts to rank applications, like Whatsapp; these can be terribly powerful within the future, up to now they need received very little adoption.

II. RELATED WORK

This section provides an overview of OSN platforms, describes the privacy issues in those platforms, and reviews the previous literature on these issues.

1. **Social Networking Platform:** several of the popular online social networking sites have free internet API's to permit third-party developers and websites to implement their own services, which might utilize and combination user data and activities in OSNs. on top of designrepresents a typical architecture of current social networking platforms, wherever TPAs square measure designed in accordance with API's and might access user information through API's. Typically, these applications square measure integrated in associate OSN web site however admit their own external server for running the appliance. The Facebook Platform and Google's OpenSocial square measure 2 of the leading forces within the business of social networking platforms. The Facebook Platform may be a proprietary computer code atmosphere for launching TPAs in Facebook. The core of Facebook Platform is that the Graph API, that forms the first method of retrieving and posting information in Facebook. It permits developers to define objects and actions within the social graph, and to form new instances of objects and actions. Google's Open Social is associate open supply cross-platform rival to the Facebook Platform for building social applications. It defines a typical API for applications across multiple websites, through that OSNs will grant applications access to the social graph also as electronic messaging service and update feeds. Its greatest blessings over Facebook Platform is its ability inside the context of multiple OSN.
2. **Privacy problems with Current Platforms:** On current platforms, for associate OSN user to put in associate application, a dialog is showed her showing that the appliance requests associate access to an inventory of her profile information. totally different from access management policies for user-to-user interactions, the user cannot specific her privacy preferences for information that square measure accessed by applications. In fact, several OSNs presently solely offer associate all-or-nothing policy once it involves application-to-user interactions, while not rental OSN users specify that data TPAs will access. Thus, even though the appliance solely wants one piece of profile information, the user needs to comply with grant the appliance full access to her profile information otherwise, she cannot use the appliance in the least. Recently, some OSNs supply users additional custom-made privacy management relating to TPAs than before, wherever users square measure allowed to opt-in or opt-out some classes of profile information. However, the essential drawback still remains. First, the coarse-grained privacy management doesn't support users to specify access management policies for every piece of knowledge users own, nor will it distinguish differing types of actions application will exercise on information. Second, users don't seem to be responsive to what reasonably information the appliance very wants. Applications will still fire additional information than they actually need, that merely violates the principle of least privilege. we tend to believe it's additional acceptable to mediate access on a per

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

request basis instead of approve access prior to throughout the time of installation. Third, some permissions square measure given by user's friend United Nations agency put in the appliance, while not user's information. This poses a heavy exposure to those users United Nations agency don't seem to be willing or interested to use the applications.

3. **Related Work:** There has been considerable work seeking to resolve the privacy problems relating to TPAs. In on-line Social network, third party applications square measure used worldwide currently a days however range of fraud cases square measure additional conjointly. one thing needs to build to forestall such application. Frappe comes here into image.In this project, we tend to develop Frappe, a collection of economical classification techniques for characteristic whether or not associate app is malicious or not. therefore we tend to planned a system that contains:

- Check statistics of the domain, if there square measure range of malicious applications under it domain then frappe will block that domain.
- If application posts some malicious or abusive contents then we must always warn that user and if limit exceeds then we are able to block that Application.
- If Application posting some external URL's into their post then we are able to conjointly block that user.
- If user accepts app request from application he will see app statistics conjointly, in order that he should responsive to application.

All communication between applications and information in OSNs is encapsulate by API's. However, current API's don't seem to be designed with the aim of access management in mind, rental TPAs access user information while not obstruction. to forestall TPAs from directly interacting with user information through API's, many planned proxy styles intercept all requests from TPAs, exert users' privacy preference on information retrieved from the OSN, and so come back the alter or dummy information to TPAs. The social control of such styles varies from server-side proxy to client-side plug-in, in line with the sure entities the styles admit.

4. **Advantages:**

- Facebook Rigorous Application authority is arguably is that the tool to notice malicious apps.
- It provides security to users profiles from malicious applications on online social sites.
- It is a lot of correct classifier than the the other classifiers like SVM.

III. ARCHITECTURE OVERVIEW

The architecture for detection of malicious application is designed for providing the more security than any other classifiers like SVM. We develop a frappe a suit of efficient classification techniques which is used for providing a security to the user by the use of architecture. This architecture shows the working of detection of malicious application on online social network.. It contains various components like user, Facebook server, Application server, FRAppE. This architecture is as shown below:

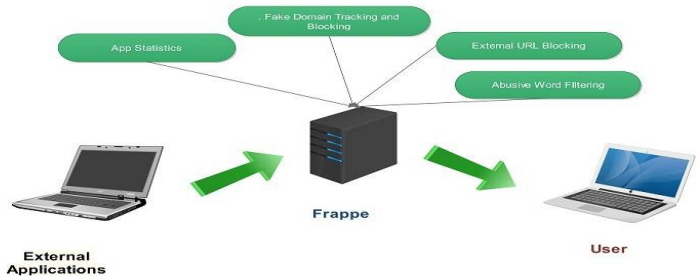


Figure 1 System Architecture

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

This architecture shows that if user wants to install particular application on users wall then it send the request to the server then server gives set of permissions to user to install application on users wall. But before installing application on user's wall the application is checked under the various modules which are used in our architecture. If the application gentle then it directly install on users wall. If the application is not gentle that means if the application is malicious then our system blocked that application permanently. Here the frappe is suit of efficient classification techniques that checks the application by the various modules like Application Statistics, Fake Domain tracking and blocking, Abusive word filtering and External URL blocking.

Modules: The modules are nothing but the part of program. Programs are composed of one or more independently modules that are not combined until the program is linked. A single module can contain one or several routines. The modules are listed below which are them as:

- Detecting malicious apps.
- Malicious apps ecosystem
- App collaboration
- Hosing domains
- Cross promotion as a sign of malicious intentions.

IV. EXPERIMENTAL RESULTS

Here the working of frappe is displayed on different kindfs of features. The frappe is classifier which is used to detect the malicious application on fabebook or other social networking sites. Here we use FRAppE a malicious app detector that utilizes aggregation-based features in addition to the ondemand features. The table shows two features that FRAppE uses in addition to those used in SVM and these features are also used with the additional features for providing better accuracy for detection of malicious application. Since the aggregation- based features for an app require a cross-user and cross-app view over time, in contrast to SVM, we envision that FRAppE can be used by OSN or by third-party security applications that protect a large population of users. The features are explained in table below:

Feature	Description
App name similarity	Is app's name identical to a known malicious app?
External link to post ratio	Fraction of app's posts that contain links to domains outside Facebook

These are two on demand features which are used in FRAPPE for detection of application on OSN. These are explained below:

1) **App Name:** eighty seven of malicious apps have associate degree app name the image of that of a minimum of one different malicious app. associate degree application's name is designed by the app's developer at the time of the app's creation on Facebook. Since the app ID is that the distinctive symbol for each application on Facebook, Facebook doesn't impose any restrictions on app names. Therefore, though Facebook will warn app developers to not violate the trademark or different rights of third parties throughout app configuration, it's attainable to make multiple apps with constant app name. Hackers can even conceive to "typo-squat" on the names of fashionable benign applications. as an example, the malicious application "FarmVile" makes an attempt to require advantage of the popular "FarmVille" app name, whereas the "Fortune Cookie" malicious application precisely copies the popular "Fortune Cookie" app name. However, it's found that an outsized majority of malicious apps in sample dataset show little or no similarity with the one hundred hottest benign apps in our dataset.So the sample information looks to point that hackers making many apps with constant

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

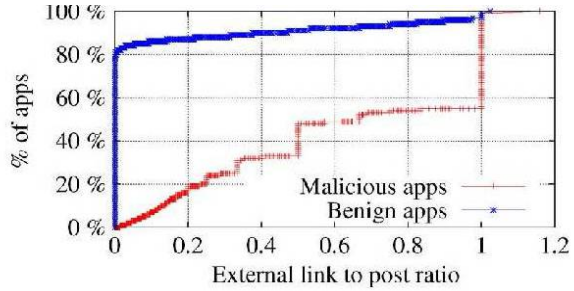
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

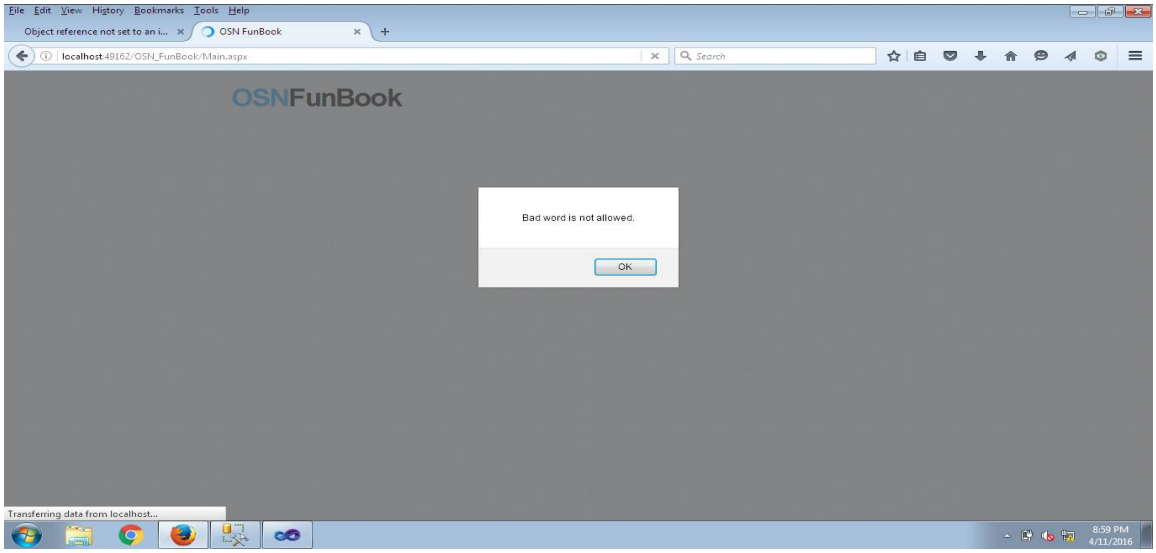
name to conduct a campaign is a lot of common than malicious apps typo-squatting on the names of fashionable apps.

2) **External Link to Post Ratio:** Malicious apps usually post links inform to domains outside Facebook, whereas benign apps seldom do thus. Any post on Facebook will optionally embody associate degree address. once the URLs enclosed in posts created by malicious and benign apps square measure analyzed, for each app in our sample dataset, the posts seen by MyPageKeeper and therefore the URLs seen across these posts square measure aggregative. each address inform to a site out-side of facebook.com is termed as associate degree external link.The external link to post magnitude relation is displayed below: The "external-link-to- post magnitude relation" live is outlined for each app because the ratio of range|theamount|the quantity} of external links announce by the app to the full number of posts created by it.



The results which are obtained while using FRAPPE a malicious app detector that utilizes aggregation-based features which are shown above. The results are displayed as :

1)



This result show that when a user tries to post a malicious word on his timeline using post block ,resulting social site will warn him about posting updates using a bad words.Bad words are of different kind like some traditional bad words,social bad words etc.

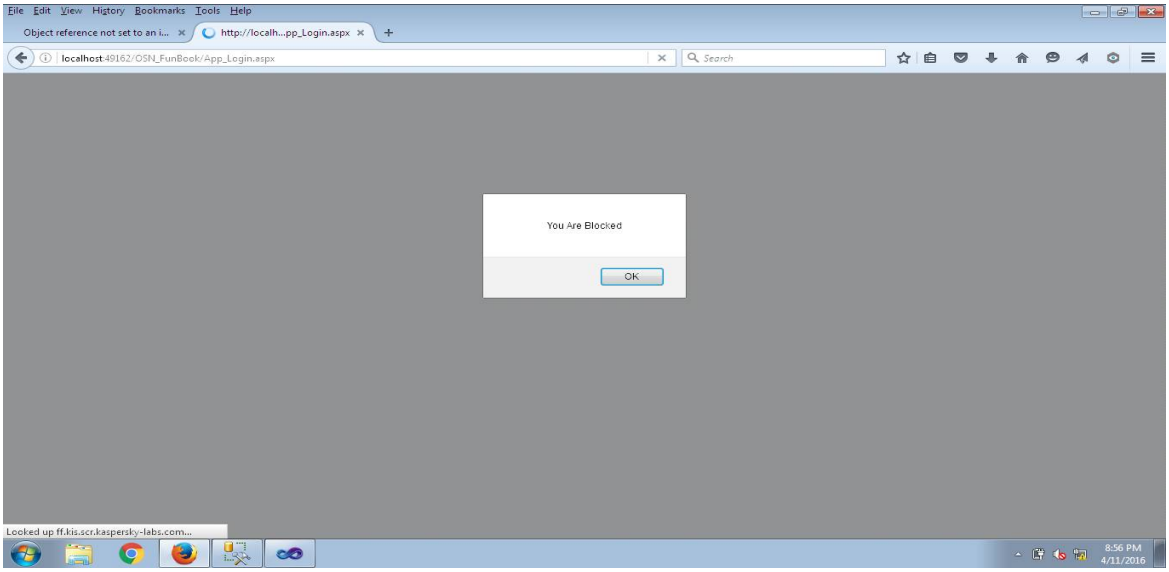
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

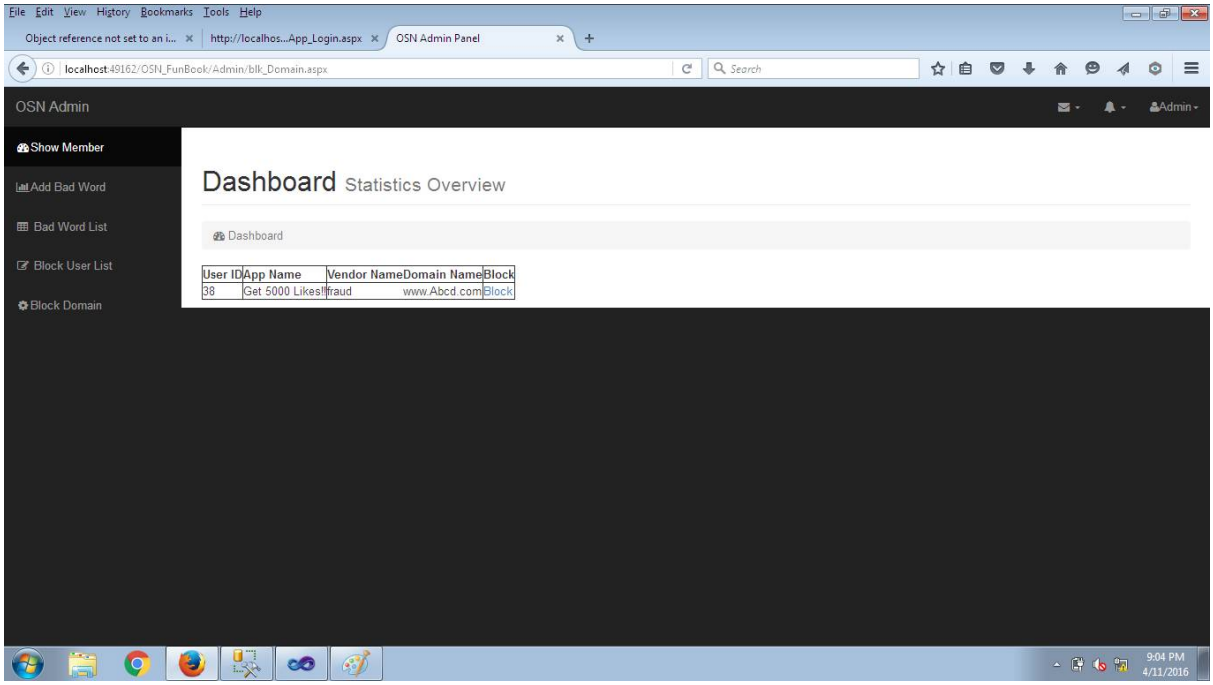
Vol. 5, Issue 5, May 2016

2)



This result is showing that when an application from same domain name trying to post a malicious post.when an applications from same domain name who has already crossed specified limit of posting malicious or bad post will not be able to post anything furthermore,the social site is blocking the domain directly.

3)



This result is showing the stastistical overview of an application running currently on online social network.this is shows that generated stastics in application id,which get generated when application get created.applicationname,it is the actual name of an application.Domain name is the name under which application is running,Block is the current status of application whis is always either blocked or unblocked.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

V. CONCLUSION

In this work, employing a great deal of malicious Facebook applications we tend to shows that malicious applications square measure considerably take issue from mild apps with the many options. for instance, malicious apps square measure possible to share names with different applications, and that they usually request fewer permissions than mild apps. investment our observations, we tend to developed Frappe, AN correct classifier for detective work malicious Facebook applications. Most curiously, we tend to highlighted the emergence of AppNets giant teams of tightly connected applications that promote one another. we'll still dig deeper into this scheme of malicious apps on Facebook, and that we hope that Facebook can benefit from our recommendations for reducing the menace of hackers on their platform.

Applications gift a convenient suggests that for hackers to unfold malicious content on Facebook. However, very little is known concerning the characteristics of malicious apps and the way they operate. during this work, employing a giant corpus of malicious Facebook apps discovered over a 9 month amount, we tend to showed that malicious apps take issue significantly from benign apps with relevancy many options. for instance, malicious apps square measure far more possible to share names with different apps, and that they usually request fewer permissions than benign apps. investment our observations, we tend to developed Frappe, AN correct classifier for detective work malicious Facebook applications. Most curiously, we tend to highlighted the emergence of AppNets giant teams of tightly connected applications that promote one another. we'll still dig deeper into this scheme of ma- licious apps on Facebook, and that we hope that Facebook can benefit from our recommendations for reducing the menace of hackers on their platform.

REFERENCES

1. App piggybacking example. https://apps.facebook.com/mypagekeeper/status=scam_report_fb_survey_scam_ Converse_shoes_2012_05_17_boQ.
2. BitdefenderSafego. http: //www.facebook.com/bitdefendeR.
3. bit.ly API. http://code.google.com/p/bitly-api/wiki/ApiDoc.
4. Profile stalker: rogue Facebook application. https://apps.facebook.com/mypagekeeper/ ?status=scam_report_fb_survey_scam_ pr0file_viewer_2012_4.
5. The Pink Facebook - rogue application and survey scam. http://nakedsecurity.sophos.com/2012/02/ 27/pink-facebook-survey-scam/
6. Whatapp- A Stanford Center for Internet and Society website with support from the Rose Foundation. https://whatapp.org/facebook/.
7. Which cartoon character are you - rogue Facebook application. https://apps.facebook.com/ mypagekeeper/?status=scam_report_fb_ survey_scam_whiich_cartoon_character_ are_you_2012_03_3.
8. Wiki: Facebook Platform. http://en.wikipedia.org/wiki/Facebook_Platform.
9. H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary.Towards online spam filtering in OSN. In NDSS,2012.