Detecting Malicious Facebook Applications

Sreeja Krishna V R[1], Lavannya Varghese[2]

[1]Student Dept of computer science St.Joseph's college irinjalakkuda
[2]Professer Dept of computer science St.Joseph's college irinjalakkuda

---***---

Abstract - *With daily installs, third-party Apps can be a important cause for the popularity and attractiveness of Facebook or any online social media. Sadly, cyber criminals get came to the realization that the capability of using apps for spreading spam and malware. We realize that at the least 13% of Facebook apps in the dataset are usually malevolent. However with their findings , several issues like faux profiles, malicious application have conjointly full-grown. There aren't any possible method exist to regulate these issues. During this project, we tend to came up with a framework with that automatic detection of malicious applications is feasible and is efficient. Suppose there's Facebook application, will the Facebook user verify that the app is malicious or not. In fact the Facebook user cannot establish that therefore The key contribution is in developing FRAppE-Facebook's Rigorous Application Evaluator is the first tool focused on detecting malicious apps on Facebook. To develop FRAppE, we tend to use data gathered by the posting behavior of Facebook apps seen across million users on Facebook. First we identify a set of features that help us to analyze malicious from benign ones. Second, leveraging these distinguishing features ,where we show that FRAppE can detect malicious apps with 95.9% accuracy. Finally, we explore the ecosystems of malicious Facebook apps and identify mechanisms that these apps use to spread.*

Key Words: apps, malicious, Online social networks.

1.INTRODUCTION

The new battleground for cybercrime is Online Social Networks (OSNs), which provides a new, fertile, and unexplored environment for the dissemination of malware. A social networking website may be a web site wherever every user contains a profile and might keep contact with friends, share their updates, meet new people that have a same interests. . Moving beyond spam email, the spread of malware on OSNs takes the form of postings and communications between friends. We use the term social malware to describe damaging behaviour including identity theft, distribution of malicious URLs, spam, and malicious apps that utilizes OSNs. The use of posts from friends adds a powerful element in the propagation of social malware: it comes implicitly with the endorsement of a friend who reputedly posts the information. These Online social networks (OSN) enable third party apps to enhance the user experience on the platforms. Such enrichment includes interesting or entertaining ways of communicating among online friends and different activities such as playing games , listening songs.

Recently, hackers have started taking advantage of the recognition of this third-party apps platform and deploying malicious applications. There are many ways that hacker can benefit from a malicious apps. Some of the ways are: the app can reach large numbers of users and their friends to spread spam, the app can obtain users' personal information such as email address, home town, and gender, and the app can "re-produce" by making other malicious apps popular. Therefore, it is becoming increasingly important to understand social malware better and build better defences to protect users from the crime underlying this social malware. Detecting social malware needs novel approaches since hackers use extremely different approaches in its distribution compared to email-based spam. For example, reputation-based filtering is insufficient to finf social malware received from friends and the keywords used in email spam significantly differ from those used in social malware. We also find that URL blacklists designed to detect phishing and malware on the web do not suffice, e.g., because a large fraction of social malware (26% in our dataset) points to malicious applications hosted on Facebook. Although such malicious apps are widespread in Facebook, as we show later, currently there is no commercial service, publicly-available information, or research-based tool to advise a user about the risks of an app.

In this paper we develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. 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. The basis of our study is a dataset. We classify url as social spam if it points to a web page that spread malware, attempts to phish, request to carry a task, false promises etc. We systematically profile apps and show that malicious app profiles are significantly different than those of benign apps. A striking observation is the laziness" of hackers; many malicious apps have the same name, as 8% of unique names of malicious apps are each used by more than 10 different apps (as defined by their app IDs). Overall, we profile apps based on two classes of features: (a) those that can be obtained on-demand given an application's identifier (e.g., the permissions required by the app and the posts in the application's profile page), and (b) others that require a cross-user view to aggregate information across time and across apps. We develop FRAppE (Facebook's Rigorous Application Evaluator) to identify malicious apps either using only features that can be obtained on-demand or using both on-demand and aggregation-based app information. FRAppE Lite, which only uses information avail- able on-demand, can identify malicious apps with more accuracy This paper is mainly for detecting malicious application on facebook, currently there is no commercial service, publicly-available information, or research-based tool to advise a user about the risks of an app.

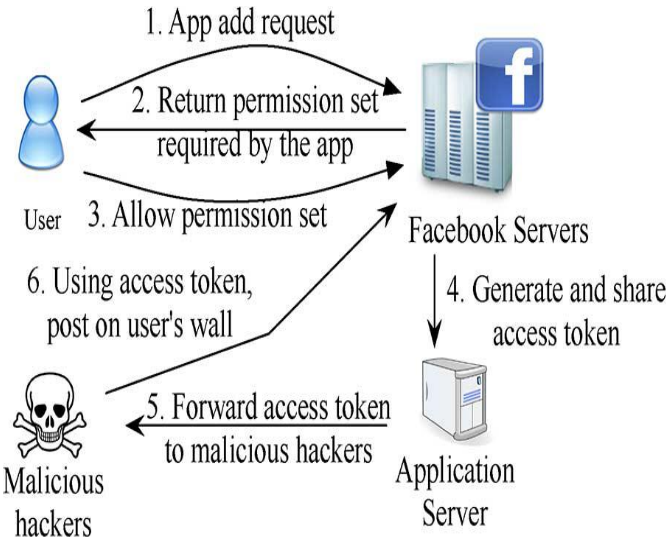
2 EXISTING SYSTEM

So far, the research community has paid little attention to Online social network apps specifically. Most study related to spam and malware on Facebook has concentrated on detecting malicious posts and social spam campaigns. Gao et al. analyzed posts on the walls of million Facebook users and presented that 10% of links posted on Facebook walls are spam. They also presented method to identify compromised accounts and spam campaigns. Yang et al. and Benevenuto et al. developed techniques to identify accounts of spammers on Twitter. Others have put forward a honey-pot-based approach to detect spam accounts on online social networks. Yardi et al. examined behavioral patterns among spam accounts in Twitter. Chia et al. studied risk signaling on the privacy intrusiveness of Facebook apps. The main disadvantages of existing system is , the work focused only classifying a single url as spam but not for the malicious apps. The work focused only finding the accounts created by spammers. Finally the existing system gives an overview about the threat on Facebook.

3. PROPOSED SYSTEM

In the proposed system ,we can detect malicious applications in the facebook and also we can block such type of applications before using it. This is done by the help of FRAppE. FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. We find that malicious applications outstandingly differ from good apps with respect to two classes of features: On-Demand Features and Aggregation-Based Features. The main merit of the proposed system is , the work 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. the features used by FRAppE, such as the reputation of redirect URIs, the number of required permissions, and the use of different client IDs in app installation URLs, are robust to the evolution of hackers. Not using different client IDs in app installation URLs would limit the ability of hackers to instrument their applications to spread each other

3.1 System model


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

3.2 Data collection

This module describes about the collection of all facebook application. The basis of our study start with the collection of data. It has two subcomponents they are: the collection of facebook apps with URLs and crawling for URL redirections. Whenever this component obtains a facebook app with a URL, it accomplish a crawling thread that follows all redirections of the URL and looks up the corresponding IP addresses. The crawling thread merge these retrieved URL and IP chains to the tweet information and pushes it into a queue. As we have seen, our crawler cannot reach malicious landing URLs when they use conditional redirections to evade crawlers. However, because our detection system does not rely on the features of landing URLs, it works solo of such crawler evasions.

3.3 Feature extraction

we divide features into two subsets: on-demand features and aggregation based features. We know that malicious applications are entirely different from benign apps. On-demand feature includes : 1)App summary: the malicious apps usually have incomplete application summaries.2)Requested permission set : in the case of malicious apps ,most of the malicious apps require only one permission set that is permission for posting on users wall. 3)Redirect URL : malicious apps redirect user to domain with poor reputation. 4)client ID in app installation URL : mainly malicious apps trick users into installing other apps by using a different client ID in theit app installation URl. 5)Post in apps profile : There is no post in malicious apps wall.

The aggregation based feature includes the following.1)App name :malicious apps have an app name identical to at least one other malicious apps. 2)External link post ratio : significantly this ration is high for malicious apps.

3.4 Link handling

The main function of this Link handling is to identify the outside and inside link available in your application(url) and notify you in order to take correct action. Whenever this application identify such link item it will automatically redirect to that section, either it may be internal link or external link upon your final confirmation. Another important point is that, you cancheck out the coding section through the external link and its unique phishing system will identify the websites who are trying to theft your information or trying to make you fool.

3.5 Training

The training part includes two subcomponents: accessing the account statuses and training of the classifier. Because we use an offline supervised learning algorithm, the feature vectors for training are relatively older than feature vectors for classification. To label the training vectors, we use the account status; URLs from suspended accounts are considered malicious whereas URLs from active accounts are considered benign. We repeatedly update our classifier using labeled training vectors.

3.6 Classification and detection

The classification component starts our classifier using input feature vectors to classify suspicious URLs. The classification module accept a URL and the related social context features extracted in the previous step. These URLs, detected as suspicious, will be delivered to security experts or more sophisticated dynamic analysis environments for an in-depth investigation.

5. CONCLUSIONS AND FUTURE WORKS

The emergence of Online Social Networks (OSNs) has opened up new possibilities for the dissemination of malware. As Facebook is becoming the new web, hackers are expanding their territory to Online Social Networks (OSNs) and spread social malware. Social malware is a new kind of cyber-threat, which requires novel security approaches. Cyber-fraud is an immediate and expensive problem that affects people and business through identity theft, the spread of viruses, and the creation of botnets, all of which are interconnected manifestations of Internet threats.

In this paper, In this work, utilizing a huge corpus of pernicious Facebook applications saw over a nine month time span, we demonstrated that malignant applications contrast essentially from considerate applications as for a few elements. For instance, noxious applications are a great deal more prone to impart names to different applications, and they normally ask for less consents than kind applications. Utilizing our perceptions, we created FRAppE, an exact classifier for distinguishing noxious Facebook applications. Most curiously, we highlighted the rise of AppNets—expansive gatherings of firmly associated applications that advance each other. We will keep on digging further into this biological system of noxious applications on Facebook, and we trust that Facebook will profit by our proposals for diminishing the hazard of hackers on their platform.

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

I am highly indebted to MS Lavanya assistant professor of St. Joseph's college irinjalakuda for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

I would like to express my gratitude towards my parents & member of DCinfotec for their kind co-operation and encouragement which help me in completion of this project.

REFERENCES

[1].Facebook Open graph API. http://developers. facebook.com/docs/reference/api/.
[2].MyPageKeeper.https://www.facebook.com/apps/application.php?id=167087893342260.
[3].Profile stalker: rogue Facebook application. https://apps.facebook.com/mypagekeeper/ ?status=scam_report_fb_survey_scam_ pr0file_viewer_2012_4_4.
[4].Which cartoon character are you - rogue Facebook application.
[5].https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_whiich_cartoon_character_are_you_2012_03_30
[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].M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos. Efficient and Scalable Socware Detection in Online Social Networks. In USENIX Security, 2012.
[9].Stay Away From Malicious Facebook Apps. http://bit.ly/b6gWn5.
[10]. Pr0_le stalker: rogue Facebook application. https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_pr0file_viewer_ 2012_4_4.

[11].LatestPromotions.https://www.facebook.com/apps/application.php?id=174789949246851.
[12]. How to spot a Facebook Survey Scam. http://facecrooks.com/Safety-Center/Scam-Watch/How-to-spot-a-Facebook-Survey-Scam.html.
[13]. Hackers selling $25 toolkit to create malicious Facebook apps. http://zd.net/g28HxI.
[14].Games.https://www.facebook.com/apps/application.php?id=121297667915814.