Detecting Malicious Face book Applications

[1]B Mariamma [2] K Abdul Basith, [3] Prasad B
[1]II/IV, [2] [3] Associate Professor
[1][2][3] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM)
Hyderabad
[1] jolimariyam@gmail.com [2] hodcse@mlritm.ac.in [3] bprasad@gmail.com

Abstract: **With 20 million installs a day third-party apps are a major reason for the popularity and addictiveness of Face book. Unfortunately, hackers have realized the potential of using apps for spreading malware and spam. The problem is already significant, as we find that at least 13% of apps in our dataset are malicious. So far, the research community has focused on detecting malicious posts and campaigns. In this paper, we ask the question: given a Face book application, can we determine if it is malicious? Our key contribution is in developing FRAppE—Facebook's Rigorous Application Evaluator arguably the first tool focused on detecting malicious apps on Face- Finally, we explore the ecosystem of malicious Face book apps and identify mechanisms that these apps use to propagate. Interestingly, we find that many apps collude and support each other; in our dataset, we find 1,App piggybacking example. Finally, we explore the ecosystem of malicious Face book apps and identify mechanisms that these apps use to propagate. Interestingly, we find that many apps collude and support each other; in our dataset, we find App piggybacking example.**

Keywords: Face book Apps, Malicious Apps, Profiling Apps, and Online Social Networks.

I. INTRODUCTION

Online social networks (OSN) enable and encourage third party applications (apps) to enhance the user experience on these plat- forms. Such enhancements include interesting or entertaining ways of communicating among online friends, and diverse activities such as playing games or listening to songs. For example, Face book provides developers an API that facilitates app integration into the Face book user-experience. There are 500K apps available on Face- book , and on average, 20M apps are installed every day. Furthermore, many apps have acquired and maintain a large user- base. For instance, Farmville and City Ville apps have 26.5M and42.8M users to date. Recently, hackers have by combining information obtained from all posts containing that URL. Examples of features used in My Page Keeper classifier include a) the presence of spam keywords such as 'FREE', 'Deal', and 'Hurry' (malicious posts are more likely to include such keywords than normal posts), b) the similarity of text messages (posts in a spam campaign tend to have similar text messages across posts containing the same URL), and c) the number of 'Like's and comments (malicious posts receive fewer 'Like's and comments). Once a URL is identified as malicious, My Page Keeper marks all posts containing the URL as malicious. Classifier include a) thpresence of spam keywords such as 'FREE', 'Deal', and 'Hurry' (malicious posts are more likely to include such keywords than normal posts), b) the similarity of text messages (posts in a spam campaign tend to have similar text messages across posts containing the same URL), and c) the number of 'Like's and comments (malicious posts receive fewer 'Like's and comments). Once a URL is identified as malicious, My Page Keeper marks all posts containing the URL as malicious. Classifier include a) the presence of spam keywords such as 'FREE', 'Deal', and 'Hurry' (malicious posts are more likely to include such keywords than normal posts), b) the similarity of text messages (posts in a spam campaign tend to have similar text messages across posts containing the same URL), and c) the number of 'Like's and comments (malicious posts receive fewer 'Like's and comments). Once a URL is identified as malicious, My Page Keeper marks all posts containing the URL as malicious.

Started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Facebook leading the way with 900M active users. There are many ways that hackers can benefit from a malicious app: (a) the app can reach large numbers of users and their friends to spread .spam, (b) the app can obtain users' personal information such as email address, home town, and gender, and (c) the app can "re-produce" by making other malicious apps popular. To make matters worse, the deployment of malicious apps is simplified by ready-to-use toolkits starting at. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Face book every day.

II. FACE BOOKS APPS

Face book enables third-party developers to offer services to its users by means of Face book applications. Unlike typical desktop and Face book Apps Face book enables third-party developer to offer services My Page Keep is a Face book app designed for detecting malicious posts on Face book. Once a Facebook user installs My-Page Keeper, it periodically crawls posts from the user's wall and news feed. My Page Keeper then applies URL blacklists as well as custom classification techniques to identify malicious posts. Our previous work shows that My Page Keeper detects malicious posts with high accuracy 97% of posts flagged by it indeed point to malicious websites and it incorrectly flags only 0.005% of be- nigh posts.post does not take in an account the application responsible for the post. Indeed, a large fraction of posts (37%) monitored by My Page- Keeper are not posted by any application; many posts are made manually by a user or posted via a social plug-in (e.g., by a user clicking 'Like' or 'Share' on an external website). Even among malicious posts identified by My Page Keeper, 27% do not have an associated application. My Page Keeper's classification primarily relies on a Support Vector Machine (SVM) based classifier that evaluates every URL by combining information obtained from all posts containing that URL. Examples of features used in My Page Keeper's classifier include a) thpresence of spam keywords such as 'FREE', 'Deal', and 'Hurry' (malicious posts are more likely to include such keywords than normal posts), b) the similarity of text messages (posts in a spam campaign tend to have similar text messages across posts containing the same URL), and c) the number of 'Like's and comments (malicious posts receive fewer 'Like's and comments). Once a URL is identified as malicious, My Page Keeper marks all posts containing the URL as malicious.

2.1 Our Datasets

In the absence of a central directory of Facebook apps , the basis of our study is a dataset obtained from 2.2M Face book users, who are monitored by My Page Keeper.Our dataset contains 91 million posts from 2.2 million walls monitored by My Page Keeper over nine months from June 2011 to March 2012. These 91 million posts were made by 111K apps, which forms our initial dataset D-Total, as shown in Table 1. Note that, out of the 144M posts monitored by My Page Keeper during this period, here we consider only those posts that included a non- empty "application" field in the metadata that Face book associates with every post. The D-Sample dataset: Finding malicious applications. To identify malicious Face book applications in our dataset, we start with a simple heuristic: if any post made by an application was flagged as malicious by My Page Keeper, we mark the application as malicious; as we explain later in Section 5, we find this to be an effective technique for identifying malicious apps. By applying this heuristic, we identified 6,350 malicious apps. Interestingly, we find that several popular applications such as 'Face book for Android' were also marked as malicious in this process. This is in fact the result of hackers exploiting Face book weaknesses as we describe later in Section 6.2. To avoid such mis classifications, we verify applications using a white list that is created by considering the most popular apps and significant manual effort. After white listing, we are left with 6,273 malicious applications (D-Sample dataset in Table 1). Table 2 shows the top five malicious applications, in terms of number of posts per application. The D-Sample dataset: Including benign applications. To select an equal number of benign apps from the initial D-Total dataset, we use two criteria: (a) none of their posts were identified as malicious by My Page Keeper, and (b) they are "vetted" by Social Bakers, which monitors the "social marketing success" of apps. This process yields 5,750 applications, 90% of which have a user rating of at least 3 out of 5 on Social Bakers. To match the number of malicious apps, we add the top 523 applications in D- Total (in terms of number of posts) and obtain a set of 6,273 benign applications.

2.2 My Page Keeper

My Page Keeper is a Face book app designed for detecting malicious posts on Face book. Once a Face book user installs My- Page Keeper, it periodically crawls posts from the user's wall and news feed. My Page Keeper then applies URL blacklists as well as custom classification techniques to identify malicious posts. Our previous work shows that My Page Keeper detects malicious posts with high accuracy—97% of posts flagged by it indeed point to malicious websites and it incorrectly flags only 0.005% of benign posts The key thing to note here is that My Page Keeper identifies so- post does not take into account the application responsible for the post. Indeed, a large fraction of posts (37%) monitored by My Page Keeper are not posted by any application; many posts are made manually by a user or posted via a social plug in (e.g., by a user clicking 'Like' or 'Share' on an external website). Even among malicious posts identified by My Page Keeper, 27% do not have an associated application.My Page Keeper's classification primarily relies on a Support Vector Machine (SVM) based classifier that evaluates every URL by combining information obtained from all posts containing that URL. Examples of features used in My Page Keeper classifier include a) the presence of spam keywords such as 'FREE', 'Deal', and 'Hurry' (malicious posts are more likely to include such keywords than normal posts), b) the similarity of text messages (posts in a spam campaign tend to have similar text messages across posts containing the same URL), and c) the number of 'Like's and com- ments (malicious posts receive fewer 'Like's and comments). Once a URL is identified as malicious, My Page Keeper marks all posts containing the URL as malicious.

III. PREVALENCE OF MALICIOUS APPS

The driving motivation for detecting malicious apps stems from the suspicion that a significant fraction of malicious posts on Fbook are posted by apps. We find that 53% of malicious posts flagged by My Page Keeper were posted by malicious apps. We fuquantify the prevalence of malicious apps in two different ways.60% of malicious apps get at least a hundred thousand clicks on the URLs they post. We quantify the reach of malicious apps by determining the number of clicks on the the links included in malicious posts. For each malicious app in our D-Sample dataset, we identify all bit.ly URLs in posts made by that application. We focus on bit.ly URLs since bit.ly offers an API for querying the number of clicks received by every bit.ly link; thus our estimate of the number of clicks received by every application is strictly a lower bound. On the other hand, each bit.ly link that we consider here could potentially also have received clicks from other sources on web (i.e., outside Face book); thus, for every bit.ly URL, the total number of clicks it received is an upper bound on the number clicks received via Facebook.Across the posts made by the 6,273 malicious apps in the DSample dataset, we found that 3,805 of these apps had posted 5,700 bit.ly URLs in total. We queried bit.ly for the click count of each URL. The distribution across malicious apps of the total number of clicks received by bit.ly links that they had posted. We see that 60% of malicious apps were able to accumulate over 100K clicks each, with 20% receiving more than 1M clicks each. The application with the highest number of bit.ly clicks in this experiment—the 'What is the sexiest thing about you?' app— received 1,742,359 clicks.40% of malicious apps have a median of at least 1000 monthly active users. We examine the reach of malicious apps by inspecting the number of users that these applications had. To study this, we use the Monthly Active Users (MAU) metric provided by Fac4.

IV. PROFILING APPLICATIONS

Given the significant impact that malicious apps have on Face- book, we next seek to develop a tool that can identify malicious applications. Towards developing an understanding of how to build such a tool, in this section, we compare malicious and benign apps with respect to various features. As discussed previously in Section 2, we crawled Face book and obtained several features for every application in our dataset. We divide these features into two subsets: on-demand features and aggregation-based features. We find that malicious applications significantly differ from benign applications with respect to both classes of features

V. APPLICATION SUMMERY

Malicious apps typically have incomplete application summaries. First, we compare malicious and benign apps with respect to attributes present in the application's sapp description, company name, and category. Description and company are free-text attributes, either of which can be at most 140 characters. On the other hand, category can be selected from a predefined (by Face book) list such as 'Games', 'News', etc. that matches the app functionality best. Application developers can also specify the company name at the time of app creation. For example, the 'Mafia Wars' app is configured with description as 'Mafia Wars: Leave a legacy behind', company as 'Zynga', and category as 'Games', fraction of malicious and benign apps in the D- Summary dataset for which these three fields are non-empty. We see that, while most benign apps specify such information, very rarely malicious apps do so. For example, only 1.4% of malicious apps have a non-empty description, whereas 93% of benign apps configure their summary with a description. We find that the benign.

5.1 Detecting Malicious Apps

Having analyzed the differentiating characteristics of malicious and benign apps, we next use these features to develop efficient classification techniques to identify malicious Facebook applications. We present two variants of our malicious app classifier Frappe Lite and Frappe. It is important to note that My Page- Keeper, our source of "ground truth" data, cannot detect malicious apps; it only detects malicious posts on Face book. Though mal cious apps are the dominant source of malicious posts, My Page-Keeper is agnostic about the source of the posts that it classifies. In contrast, Frappe Lite and Frappe are designed to detect malicious apps. Therefore, given an app ID, My Page Keeper cannot say whether it is malicious or not, whereas Frappe Lite and Frappe.

VI. IMPLEMENTATION

We have to login as shown in fig 1 in the page as given in the page ,and according to that we have to fill the details of the users and than we have to procced to next page.

Fig 1: login page

IFERP connecting engineers... developing research

Fig 2: Applicatons of page

Application page is a page which includes the different forms of applications og login page as shown in fig 2.

Fig 3: add applications of login

.

Fig 4: website applications

Here we have to add some applications to the existing applications and than add some more information to the application. And than it should be link to the login page as shown in fig 3.

Website applications, here we should upload applications in the website so that it should used by so many users who are registered in the login page as shown in fig 4.

.

Fig 5: viewing the applications

Here all the applications will be viewing the users applications and we can see all the applications and than the applications will be viewing to every one page as shown in fig 5.

.

Fig 6: detecting the applications

At last it detect the all the applications of facebook and than detect the malicious applications in the facebook and than the applications wiil be viewd.

VII. CONCLUSIONS AND FUTURE WORK

Applications present a convenient means for hackers to spread malicious content on Face book. However, little is understood about the characteristics of malicious apps and how they operate. In this work, using a large corpus of malicious Face book apps observed over a nine month period, we showed that malicious apps differ significantly from benign apps with respect to several features. For example, malicious apps are much more likely to share names with other apps, and they typically request fewer permissions than be- nign apps. Leveraging our observations, we developed FRAppE, an accurate classifier for detecting malicious Facebook applications. Most interestingly, we highlighted the emergence of AppNets—large groups of tightly connected applications that promote each other. We will continue to dig deeper into this ecosystem of ma- vicious apps on Face book, and we hope that Face book will benefit from our recommendations for reducing the menace of hackers on their platform.

REFERENCES

[1] 100 social media statistics for 2012. http://thesocialskinny.com/ 100-social-media-statistics-for-2012/.

[2] Million Bulk email addresses for sales SalePrice$90. http://www.allhomebased.com/ BulkEmailAddresses.htm.

[3]Apppiggy backing example. https://apps.facebook.com/My Page Keeper/ status=scam_report_fb_survey_scam_Converse_shoes_2012_05_17_boQ

[4] Application authentication flow using oath 2.0. http://developers.facebook.com/docs/ authentication/.

[5] Bit defender Safe go. http: //www.facebook.com/bitdefender.safego.

[6] bit.ly API. http://code.google.com/p/ bitly-api/wiki/Api Documentation.

[7]Defense Social Web Security. http://www.facebook. com/apps/application.php?id=177000755670.

[8] Facebook developers. https://developers.facebook.com/docs/ appsonfacebook/tutorial/.

[9] Face book kills App Directory, wants users to search for apps. http://zd.net/MkBY9k.

[10] Face book Open graph API. http://developers. facebook.com/docs/reference/api/.

[11] Face book softens its app spam controls, introduces better tools for developers. http://bit.ly/LLmZpM.

[12] Face book tops 900 million users. http://money.cnn.com/2012/04/23/ technology/facebook-q1/index.htm.

IFERP connecting engineers... developing research