ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 3, March 2016

FRAPPE - For Identifying Third Party Application on Facebook

Deepa C
M.phill (Research Scholar)
School of computer science
VELS University, Chennai, India.
Dr.S.Prasanna,
Assoc.Prof. Department of MCA
School of Computer Science,
VELS University, Chennai, India.

Abstract*:* 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. The botheration is already significant, as we acquisition that at atomic apps in our dataset are malicious. 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. Finally, we analyze the ecosystem of awful Facebook apps and analyze mechanisms that these apps use to propagate. We see FRAppE as a footfall against creating an absolute babysitter for app appraisal and ranking, so as to acquaint Facebook users afore installing apps.

I. INTRODUCTION

ONLINE amusing networks (OSNs) accredit and encourage third-party applications (apps) to enhance the user acquaintance on these platforms. Such enhancements include interesting or entertaining ways of communicating among online friends and diverse activities such as playing games or listening to songs. Recently, hackers accept started demography advantage of the acceptance of this third-party apps belvedere and deploying awful applications. Awful apps can accommodate a advantageous business for hackers, accustomed the acceptance of OSNs, with Facebook arch the way with 900M alive users. There are abounding means that hackers can account from a awful app: 1) the app can ability ample numbers of users and their accompany to advance spam; 2) the app can access users' claimed advice such as e-mail address, home town, and gender; and 3) the app can "reproduce" by authoritative added awful apps popular. To accomplish affairs worse, the deployment of awful apps is simplified by ready-to-use toolkits starting at $25. In added words, there is motive and opportunity, and as a result, there are abounding awful apps overextension on Facebook every day. A recent work studies how app permissions and community ratings correlate to privacy risks of Facebook apps. Finally, there are some community-based feedback-driven efforts to rank applications, such as WhatApp? ; Though these could be very powerful in the future, so far they have received little adoption. In this paper, we advance FRAppE, an apartment of able allocation techniques for anecdotic whether an app is awful or not. To body FRAppE, we use abstracts from MyPageKeeper, an aegis app in Facebook that monitors the Facebook profiles of 2.2 actor users. We assay 111K apps that fabricated 91 actor posts over 9 months. This is arguably the aboriginal absolute abstraction absorption on awful Facebook apps that focuses on quantifying, profiling, and compassionate awful apps and synthesizes this advice into an able detection approach.13% of observed apps are malicious**:**We appearance that awful apps are accustomed in Facebook and ability a ample amount of users. We acquisition that 13% of apps in our dataset of 111K audible apps are malicious. Also, 60% of awful apps endanger added than 100K users anniversary by acceptable them to chase the links on the posts fabricated by

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 3, March 2016

these apps, and 40% of awful apps accept over 1000 account alive users each. Malicious and amiable app profiles decidedly differ we systematically contour apps and appearance that awful app profiles are decidedly altered than those of amiable apps. A arresting ascertainment is the "laziness" of hackers; abounding awful apps accept the aforementioned name, as 8% of altered names of awful apps are anniversary acclimated by added than 10 altered apps (as authentic by their app IDs).Overall, we contour apps based on two classes of features: 1) those that can be acquired on-demand accustomed an application's identifier (e.g., the permissions appropriate by the app and the posts in the application's contour page), and 2) others that crave a cross-user appearance to accumulated advice beyond time and beyond apps (e.g., the announcement behavior of the app and the affinity of its name to added apps).The actualization of app-nets: Apps coact at massive scale. We conduct a forensics analysis on the awful app ecosystem to analyze and quantify the techniques acclimated to advance awful apps. We acquisition that apps coact and coact at a massive scale. Apps advance added apps via posts that point to the "promoted" apps. If we call the bunco accord of promoting–promoted apps as a graph, we acquisition 1584 apostle apps that advance 3723 added apps.Furthermore, hackers use fast-changing indirection: Applications posts accept URLs that point to a Web site, and the Web website dynamically redirects to abounding altered apps; we acquisition 103 such URLs that point to 4676 altered awful apps over the advance of a month. These empiric behaviors announce able crime: One hacker controls abounding awful apps, which we will alarm an app-net, back they assume a alongside abstraction to botnets.Malicious hackers impersonate applications: we were afraid to acquisition accepted acceptable apps, such as Farm Ville and Facebook for iPhone, announcement awful posts. On added investigation, we begin a lax affidavit aphorism in Facebook that enabled hackers to accomplish awful posts arise as admitting they came from these apps.

FRAppE can ascertain awful apps with 99% accuracy: We advance FRAppE (Facebook's Rigorous Application Evaluator) to analyze awful apps application either application alone appearance that can be acquired on-demand or application both on-demand and aggregation-based app information. FRAppE Lite, which alone uses advice accessible on-demand, can analyze awful apps with 99.0% accuracy, with low apocryphal positives (0.1%) and top accurate positives (95.6%). By abacus aggregation-based information, FRAppE can ascertain awful apps with 99.5% accuracy, with no apocryphal positives and college accurate positives (95.9%).

Our recommendations to Facebook: The most important bulletin of the plan is that there seems to be a abject eco-system of awful apps aural Facebook that needs to be accepted and stopped. However, even this antecedent plan leads to the afterward recommendations for Facebook that could potentially as well be advantageous to added amusing platforms.

II. Literature Survey

Detecting Spam on OSNs: Gaoet al. analyzed posts on the walls of 3.5 million Facebook users and showed that 10% of links posted on Facebook walls are spam. They also presented techniques to identify compromised accounts and spam campaigns. In other work, Gao et al. [9] and Rahmanet al.[10] develop efficient techniques for online spam filtering on OSNs such as Facebook. While Gaoet al.[5] rely on having the whole social graph as input, and so is usable only by the OSN provider, Rahmanet al.[1] develop a third-party application for spam detection on Facebook. In contrast to all of these efforts, rather than classifying individual URLs or posts as spam, we focus on identifying malicious applications that are the main source of spam on Facebook. Detecting Spam Accounts: Instead of focusing on accounts created by spammers, our work enables detection of malicious apps that propagate spam and malware by luring normal users to install them. Chiaet al. [3] investigate risk signaling on the privacy intrusiveness of Facebook apps and conclude that current forms of community ratings are not reliable indicators of the privacy risks associated with an app. Also, in keeping with our observation, they found that popular Facebook On the contrary, we quantify the prevalence of malicious apps and develop tools to identify malicious apps that use several features beyond the required permission set WhatApp? [6] Collects community reviews about apps for security, privacy, and openness. However, it has not attracted many reviews (47 reviews available) to date. To the best of our knowledge, we are the first to provide a classification of Facebook apps into malicious and benign categories.

III. Major Contribution

In this paper, aiming at efficiently solving the problem of Malicious Facebook applications. Operation of Awful Applications: Malicious Facebook applications about accomplish as follows.

Step 1: Hackers argue users to install the app, usually with some affected affiance (e.g., chargeless iPads).

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 3, March 2016

Step 2: Once a user installs the app, it redirects the user to a Web page area the user is requested to accomplish tasks, such as commutual a survey, afresh with the allurement of affected rewards.

Step 3: The app thereafter accesses claimed advice (e.g., bearing date) from the user's profile, which the hackers can potentially use to profit.

Step 4: The app makes awful posts on account of the user to allurement the users accompany to install the aforementioned app (or some added awful app, as we will see later). This way the aeon continues with the app or colluding apps extensive added and added users. Claimed advice or surveys can be awash to third parties to eventually accumulation the hackers.

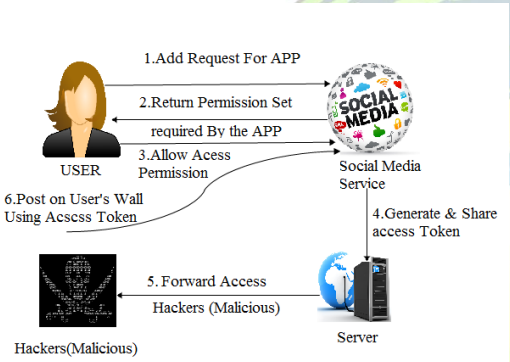

Fig 1. Steps complex in hackers using malicious applications to get admission tokens to column awful agreeable on victims' walls.

IV. FRAPEE FRAMEWORK

A. FRAppE Lite

FRAppE Lite is a lightweight version that makes use of only the application features available on demand. Given a specific app ID, FRAppE Lite crawls the on-demand features for that application and evaluates the application based on these features in real time. We envision that FRAppE Lite can be incorporated, for example, into a browser extension that can evaluate any Facebook application at the time when a user is considering installing it to her profile. All of these features can be collected on demand at the time of classification and do not require prior knowledge about the app being evaluated. We use the Support Vector Machine (SVM) classifier for classifying malicious apps. SVM is widely used for binary classification in security and other disciplines .We use the D-Complete dataset for training and testing the classifier. We use 5-fold cross validation on the D-Complete dataset for training and testing FRAppE Lite's classifier. In 5-foldcross validation, the dataset is randomly divided into five segments, and we test on each segment independently using the other four segments for training. We use accuracy, false positive (FP) rate, and true positive (TP) rate as the three metrics to measure the classifier's performance. Accuracy is defined as the ratio of correctly identified apps (i.e., a benign/malicious app is appropriately identified as benign/malicious) to the total number of apps. False positive rate is the fraction of benign apps incorrectly classified as malicious, and true positive rate is the fraction of benign and malicious apps correctly classified (i.e., as benign and malicious, respectively).

B. FRAppE

Next, we consider FRAppE—a malicious app detector that utilizes our aggregation-based features in addition to the on-demand features. Since the aggregation-based features for an app require a cross-user and cross-app view over time, in contrast to FRAppE Lite, we envision that FRAppE can be used by Facebook or by third-party security applications that protect a large population of users. Here, we again conduct a 5-fold cross validation with the D-Complete dataset for various ratios of benign to malicious apps. In this case, we find that, with a ratio of 7:1 in benign to malicious apps, FRAppE's additional features improve the accuracy to 99.5% (true positive rate 95.1% and true negative rate 100%), as compared to 99.0% with FRAppE Lite. Furthermore, the true positive rate increases from 95.6% to 95.9%, and we do not have a single false positive.

V. RESULTS

Given the significant impact that malicious apps have on Facebook, we next seek to develop a tool that can identify malicious applications. Toward developing an understanding of how to build such a tool.

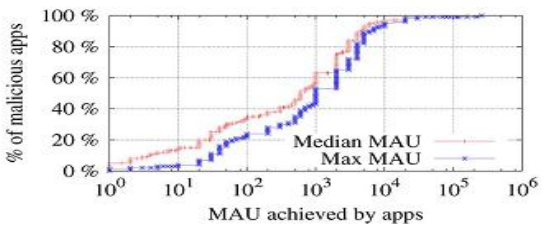

Fig 2.Median and maximum MAU achieved by malicious apps

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 3, March 2016

In this section, we compare malicious and benign apps with respect to various features. We crawled Facebook 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.

On-Demand Features: The on-demand features associated with an application refer to the features that one can obtain on demand given the application's ID. Such metrics include app name, description, category, company, and required permission set. A set of permissions that it requires. These permissions are chosen from a pool of 64 permissions predefined by Facebook. Example permissions include access to information in the user's profile (e.g., gender, e-mail, birthday, and friend list), and permission to post on the user's wall.

Aggregation-Based Features:

Next, we analyze applications with respect to aggregation based features. Unlike the features we considered so far, aggregation-based features for an app cannot be obtained on demand. Instead, we envision that aggregation-based features are gathered by entities that monitor the posting behavior of several applications across users and across time. Entities that can do so include Facebook security applications installed by a large population of users, such as MyPageKeeper, or Facebook itself. Here, we consider two aggregation-based features: similarity of app names, and the URLs posted by an application over time. We compare these features across malicious and benign apps.

VI. Discussion

Robustness of Features: Among the various features that we use in our classification, some can easily be obfuscated by malicious hackers to evade FRAppE in the future. For example, we showed that, currently, malicious apps often do not include a category, company, or description in their app summary. However, hackers can easily fill in this information into the summary of applications that they create from here on. Similarly, FRAppE leveraged the fact that profile pages of malicious apps typically have no posts. Hackers can begin making dummy posts in the profile pages of their applications to obfuscate this feature and avoid detection. Therefore, some of FRAppE's features may no longer prove to be useful in the future, while others may require tweaking, e.g., FRAppE may need to analyze the posts seen in an application's profile page to test their validity. In any case, the fear of detection by FRAppE will increase the onus on hackers while creating and maintaining malicious applications.

VII. Conclusion

Applications present acceptable agency for hackers to advance awful agreeable on Facebook. However, little is accepted about the characteristics of awful apps and how they operate. In this paper, application a ample bulk of awful Facebook apps empiric over a 9-month period, we showed that awful apps alter decidedly from amiable apps with account to several features. For example, awful apps are abundant added acceptable to allotment names with added apps, and they about appeal beneath permissions than amiable apps. Leveraging our observations, we developed FRAppE, an authentic classifier for audition awful Facebook applications. Most interestingly, we accent the actualization of app-nets—large groups of deeply affiliated applications that advance anniversary other. We will abide to dig added into this ecosystem of awful apps on Facebook, and we achievement that Facebook will account from our recommendations for abbreviation the annoyance of hackers on their platform.

Reference

[1]. C. Pring, "100 social media statistics for 2012," 2012 [Online]. Available: http://thesocialskinny.com/100-social-media-statistics-for-2012

[2]. Facebook, Palo Alto, CA, USA, "Facebook Opengraph API," [Online].Available:http://developers.facebook.com/docs/reference/api

[3]. "Wiki: Facebook platform," 2014 [Online]. Available: http://en.wikipedia.org/wiki/Facebook_Platform

[4]. "Pr0file stalker: Rogue Facebook application," 2012 [Online]. Available:https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_pr0file_viewer_2012_4_4

[5]. "Which cartoon character are you—Facebook survey scam," 2012 [Online].Available:https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_whiich_cartoon_character_are_you_2012_03_30

[6]. G. Cluley, "The Pink Facebook rogue application and survey scam," 2012 [Online]. Available:http://nakedsecurity.sophos.com/2012/02/27/pink-facebook-survey-scam/

[7]. D. Goldman, "Facebook tops 900 million users," 2012 [Online]. Available:http://money.cnn.com/2012/04/23/technology/facebookq1/index.html

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

[9]. HackTrix, "Stay away from malicious Facebook apps," 2013 [Online]. Available: http://bit.ly/b6gWn5

[10]. M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, "Efficient and scalable socware detection in online social networks," in Proc. USENIX Security, 2012, p. 32.