Unmasking Malignant Facebook Applications - A survey

Geetanjali A N*, Arpitha T, Deepti V Bhat, Kavya L R, Kavya M S

Dept of CSE, VKIT, Bangalore, India

DOI: https://doi.org/10.21467/proceedings.1.40

* Corresponding author email: geethu.avanthkar@gmail.com

Abstract

Facebook applications are the reasons for Facebook attractiveness. Unfortunately, many users are still not aware of the fact that many malicious Facebook applications exist. Each app having 20 million installs per day, third party apps have become major reason for the popularity and addictiveness of Facebook. But, cyber criminals have realized the potential of using apps for spreading malware and spam like unsolicited mail. The problem is already considered, as we find that at least 13% of apps in the sample dataset are malicious. As per the research community, it is mostfocused on detecting malicious posts and campaigns. In this paper, we try to answer a question: Given a Facebook application, Would the people be able to detect whether a application is malicious or not? Our key contribution is surveying, FRAppE—Facebook's Rigorous Application Evaluator—being the primary tool focused on detecting malicious apps on Facebook. There are 2.4 million of people using Facebook. So, in order to develop FRAppE, the information about the posting behavior of the app users is observed and collected. FRAppE is shown that it can detect malicious apps with 99.5% accuracy, with no false positives and a low false negative rate. Long term, we see FRAppE as a step towards creating an independent watchdog for app assessment and ranking.

Index Terms- Facebook, Malicious, OnlineSocialNetworks, spam, detection.

1 INTRODUCTION

Online Social Networks (OSN's) enable and give chance to third party applications in order to enhance the user experience on the platforms like Facebook, Twitter. For example, Facebook provides developers an API [2] that facilitates app integration into the Facebook user experience. There are 200K apps available on Facebook [3], and calculating average in general it has, 20 million apps are installed day to day [1]. Further, many applications have taken their places and are maintaining a really large user database. It has been observed that FarmVille and CityVille apps have 26.5M and 42.8M users to date. Nowadays, hackers and cyber criminals have began taking advantage of the popularity of this third-party applications and deploying malicious applications [4]–[6]. These malicious and spam apps can provide a money-making business for the cyber criminals, having given the status of Online Social

 ISBN: 978-81-936820-0-5

Network's, with Facebook leading the way with 920M active users [7] on the app. Collective ways that cyber criminals can benefit from a non-genuine app are as follows:

a) These malicious apps can reach huge number of users and their friends to spread junk (spam).
b) They can also capture user's private information such as e-mail address, home town, and gender, and
c) They can "reproduce" by making other malignant apps pleasing.

2 LITERATURE SURVEY

2.1 Detecting and Characterizing Social Spam Campaigns

Authors Hongyu Gao , Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao. had presented a dominant study in order to estimate amount and scrutinize malicious campaigns launched on social networks. They estimated a huge unknown dataset of non-parallel "wall" messages in between Facebook users. System unmasked generally 200,000 malignant wall posts with embedded URLs, originating from more than 57,000 user accounts. Surveyers found that more than 70% of all malignant wall posts advertise phishing sites. To review about the subject and the distinctiveness of malignant 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 the major wall posts being done in the early morning hours when users are normally asleep.

2.2 Social Applications: Exploring A More Secure Framework

Authors Andrew Besmer, Heather Richter Lipford, Mohamed Shehab, Gorrell Cheek- Online Social Network's such as Twitter, Orkut, Facebook and lot others have grown-up expeditiously, with hundreds to millions of active users. A unique feature provided on diverse sites is social applications and services written by third party application builders that surplus additional service linked to a user's profile.

2.3 Is this App Safe? A Large-Scale Study on Application Permissions and Risk Signals

Authors Pern Hui Chia, Yusuke Yamamoto, N. Asokan- Third-party applications capture the allurement of web and platforms providing mobile application. Many of these platforms obtain a disseminate control scenario, awaiting on definitive user concurrence for yielding permissions that the apps demand. Users have to await principally on community ratings as the signals to classify the potentially unstable and untrustworthy applications even though community ratings classically reflect opinions regarding supposed services or achievement rather than concerning risks. To study the advantages of user-consent permission systems through a large data collection of Facebook apps, Chrome extensions and Android apps. The analyzed data confirms that the current forms of community ratings used in app markets today are not reliable for indicating privacy risks an app creates. It is found with some evidences,

indicating attempts to mislead or entice users for granting permissions: free applications and applications with mature content request; "look alike" applications which have similar names as that of popular applications also request more permissions than is typical. Authors find that across all three platforms popular applications request more permissions than average.

2.4 Die Free or Live Hard? Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers

Yang et al. - In order to diagnose accounts of spammers on Twitter, it enables detection of malignant applications that proliferate spam and malware by luring fake promises and forcing normal Users to install them . Process is too difficult to implement.

2.5 Facebook Immune System

Stein et al. - A measurable real-time adversarial analyzing system deployed in Facebook to save users from malignant movements. It appears that Facebook has recently softened their controls for handling malicious apps. It has not attracted many reviews to date.

2.6 WARNINGBIRD: Detecting Suspicious URLs in Twitter Stream

Sangho Leey and Jong Kimz - WARNINGBIRD, a mistrustful URL identification system for Twitter. Instead of focusing on the landing pages of individual URLs in each tweet, considered collated swerve chains of URLs in a number of tweets. Because cyber criminals have limited resources and thus have to reiterate them, a portion of their re-iterating chains will be shared.

2.7 Analysing Facebook Privacy Settings: User Expectations vs. Reality

Y. L. Krishna, P. G. Balachander, Krishnamurthy Alan Mislove focused on calculating the discrepancy between the desired and exact privacy settings, quantifying the magnitude of the problem of managing privacy.

2.8 LIBSVM: A library for support Vector machines. Analysing Facebook Privacy Settings: User Expectations vs. Reality

C.-C. Chang and C.-J. Lin - LIBSVM is a library for Support Vector Machines (SVMs). This paper helps users to easily spread SVM to their applications. The article presents all implementation details of LIBSVM. Problems such as clarifying SVM optimization problems, multi-class classification, probability estimates, and parameter selection are discussed in detail.

2.9 Trust evaluation on Facebook using multiple contexts.

Tomá, Jan Samek applied the term trust from the point of view of artificial intelligence to social network analysis methods. It evaluates current available interactions for a model of trust considering various social networks. A mathematical model of trust for Facebook is designed. This model is implemented in Python programming language. Experiments are conducted on a sample amount of Facebook users and furthermore analysed from the perspective of both artificial intelligence and social psychology.

ISBN: 978-81-936820-0-5
Proceedings DOI: 10.21467/proceedings.1

Series: AIJR Proceedings

FIGURES TAKEN FROM THE SURVEY NEWS AND MAGAZINES

3 BACKGROUND

To expose malignant posts, MyPage-Keeper is used, a security app which was introduced by Facebook.It observes the Facebook profiles of 2.2 million users. It crawls user's wall post and news feed continuously and uncovers malicious posts and notifies the infected users. This review paper presents a extensive analysis focusing on malignant Facebook applications that focuses on measuring, marking, and understanding malignant applications and incorporates this useful information into an effective identification approach. MyPageKeeper mainly identifies malignant posts in Facebook and notify victims. The Sample dataset contains apps for which the ground truth is, they are malicious or not. For collecting sample malicious apps, we use a heuristic: if a post is flagged by MyPageKeeper as malicious which is posted by an app, they app is malicious. Then same amount of benign apps are collected to make the comparison fair.

The major problem statement is to detect a malicious Facebook app given its app ID?

Facebook enables third-party developers to offer functionalities to its users by means of Facebook applications. Unlike typical desktop and smart phone applications, installation of a Facebook application by a user does not involve the user downloading and executing an application binary. Instead, when a user adds a Facebook application to her profile, theuser grants the application server:

1) the leveraging permissions in order to access a subset of the information listed on the user's Facebook profile (e.g., the user's e-mail ad-dress), wherein the user's private data will be targeted for
2) permissions in order to perform certain actions on behalf of the user, such as the ability to post on the user's wall by faking or luring promises to the users.

This paper makes the following key contributions.

Malicious Facebook apps are prevalent

13% of observed apps are malicious. The malicious apps are common-place in Facebook and spread to a huge number of users.13% of apps in the dataset of 111K distinct apps are malicious. Also, 60% of malicious apps imperil more than 100K users each by convincing them to follow the links on the posts made by these apps, and
40% of malicious apps have over 1000 monthly active users each.

Malicious and benign app profiles significantly differ.

A striking observation is the "laziness" of hackers; many malicious apps have the same name, as 8% of uniquenames of malicious apps are each used by more than 10 different apps (as defined by their app IDs). Overall, theapps can be profiled based on two classes of features:

1) Those that can be obtained based on the 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
2) Others being based on that require a cross-user view to aggregate information across time and across apps (e.g., the posting behaviour of the app and the similarity of its name to other apps).

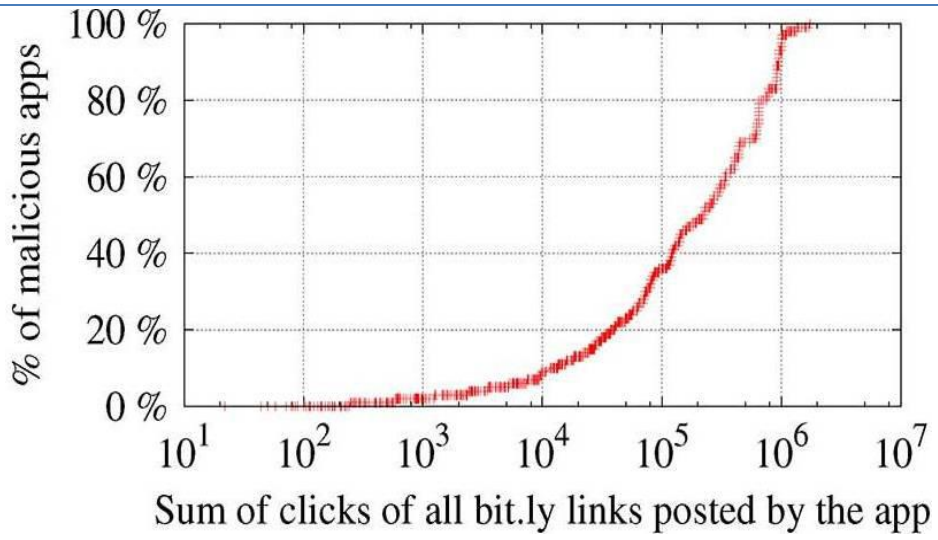
Furthermore, cyber ccriminals use fast-changing indirection: Applications posts have URLs that point to a Web site, and the Web site dynamically redirects to many different apps. These observed behaviours indicate well-organized crime: One hacker controls many malicious apps, which we will call an app net, since they seem a parallel concept to botnets.

Malicious hackers impersonate applications.

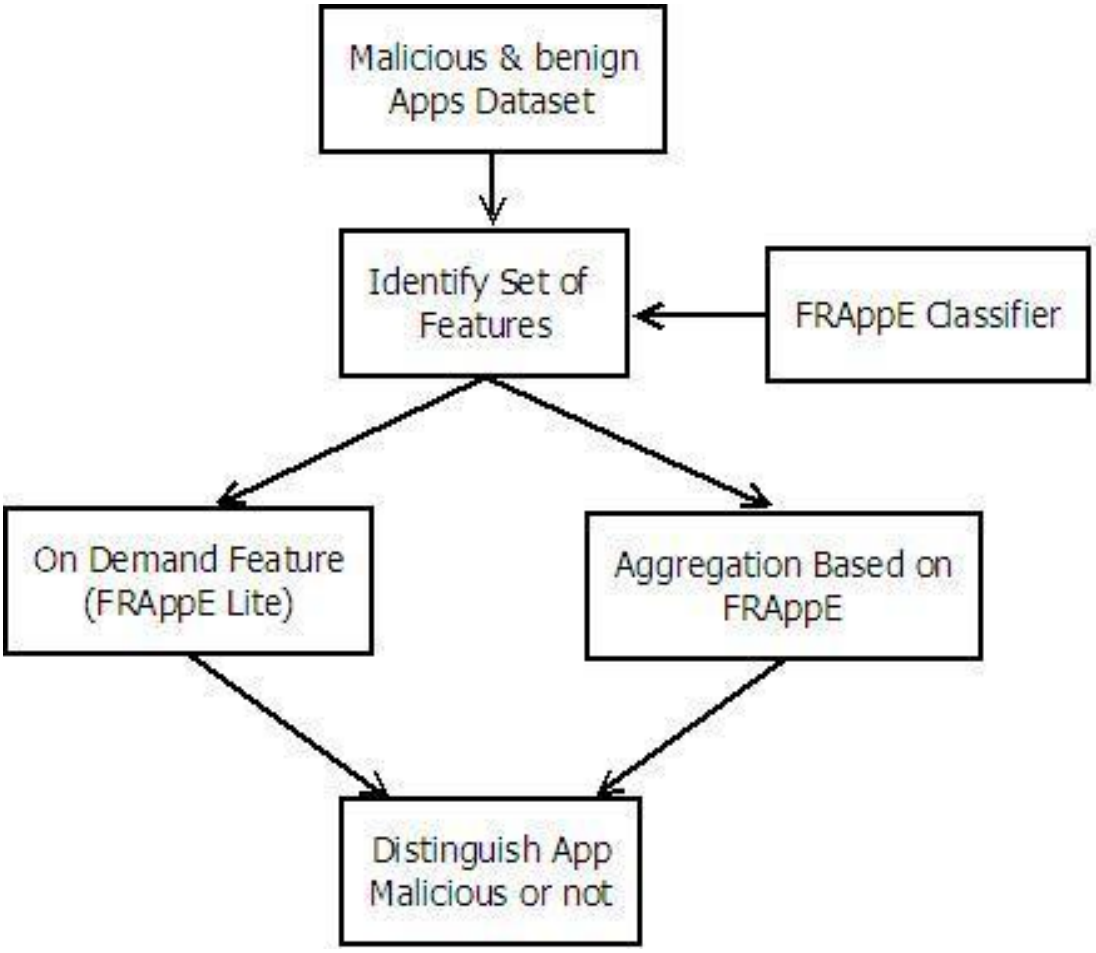
It is surprised to find popular good apps, such as FarmVille and Facebook for iPhone, posting malicious posts. On further observations, a lax authentication and authorization rule in Facebook that enabled hackers to make malicious posts appear as though they came from these apps.

ISBN: 978-81-936820-0-5
Proceedings DOI: 10.21467/proceedings.1

Series: AIJR Proceedings



SYSTEM OVERVIEW



While being given the benign (the safe) dataset and the malicious dataset, the FRAppE classifier will classify it and identify the set of features that the tool must identify and give as the output to the user. The features as told before, will be classified in two variants FRAppE lite - being the On-Demand feature and FRAppE- Aggregation Based feature. Using all the above classifications and the features, we shall determine whether a application being used by the users are malignant or not.

4 CONCLUSION

This paper is written as a survey of the base paper "Detecting Malicious Facebook Applications" bySazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos. Applications present convenient means for cyber criminals in order to spread malicious content on Facebook. However, little is understood about the characteristics of malicious apps and how they operate. In this paper, an analysis of a large amount of malignant Facebook apps is observed and it is found 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 benign apps. Leveraging our observations, FRAppE is developed, an accurate classifier for detecting malicious Facebook applications. We hope that Facebook will benefit from our recommendations for reducing the menace of cyber criminals on their platform.

5 REFERENCES

[1] C. Pring, "100 social media statistics for 2012," 2012 [Online].
[2] Facebook,PaloAlto,CA,USA, "Facebook Opengraph API," [Online].
[3] "Wiki: Facebook platform," 2014 [Online]. Available: http://en. wikipedia.org/wiki/Facebook_Platform
[4] "Pr0file stalker: Rogue Facebook application," 2012 [Online].
[5] "Which cartoon character are you—Facebook survey scam," 2012 [Online].
[6] G. Cluley, "The Pink Facebook rogue application and survey scam," 2012 [Online].
[7] D. Goldman, "Facebook tops 900 million users," 2012 [Online].
[8] HackTrix, "Stay away from malicious Facebook apps," 2013 [Online].
[9] 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.
[10] H. Gaoet al., "Detecting and characterizing social spam campaigns," in Proc. IMC, 2010, pp. 35–47.
[11] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in Proc. NDSS, 2012.
[12] "WhatApp? (beta)—A Stanford Center for Internet and Society Website with support from the Rose Foundation," [Online].
[13] "MyPageKeeper," [Online]. Available: https://www.facebook.com/ apps/application.php?id=167087893342260
[14] Facebook, Palo Alto, CA, USA, "Application authentication flow using OAuth 2.0," [Online].

ISBN: 978-81-936820-0-5

Series: AIJR Proceedings
Proceedings DOI: 10.21467/proceedings.1