Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-4, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Detecting Malicious Facebook Application

Prof. S. A. Aher (Project guide), Mr. Ketan N. Vaidya, Mr. Rakesh R. Hingmire, Mr. Tejas R. Borade & Mr. Rohit V. Patanpallu
SVIT, Chincholi, Nashik.

Abstract: *First, we identify a set of features that help us distinguish malicious apps from benign ones. For example, we find that malicious apps often share names with other apps, and they typically request fewer permissions than benign apps. Second, leveraging these distinguishing features, we show that FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and a high true positive rate (95.9%). Finally, we explore the ecosystem of malicious Facebook 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 1584 apps enabling the viral propagation of 3723 other apps through their posts. Long term, we see FRAppE as a step toward creating an independent watchdog for app assessment and ranking, so as to warn Facebook users before installing apps.*

1. Introduction

Online social networks (OSNs) enable and encourage third-party applications (apps) to enhance the user experience 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. For example, Facebook provides developers an API that facilitates app integration into the Facebook user experience. There are 500K apps available on Facebook, and on average, 20M apps are installed every day Furthermore, many apps have acquired and maintain really large user base. For instance, Farm Ville and City Ville apps have 26.5M and 42.8M users to date.

Recently, hackers have 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: 1) the app can reach large numbers of users and their friends to spread spam; 2) the app can obtain users' personal information such as mailaddress,hometown,andgender;and3)the app can "reproduce" by making other malicious apps popular. To make matters worse, the deployment of malicious apps is simplified by ready-to-use toolkits starting at $25. In other words, the motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day.

Despite the above worrisome trends, today a user has very limited in formation at the time of installing an app on Facebook. In other words, the problem is the following: Given an app's identity number (the unique identifier assigned to the app by Facebook), can we detect if the app is malicious? Currently, there is no commercial service, publicly available information, or research-based tool to advise a user about the risks of an app. As we show in Section III, malicious apps are widespread and they easily spread, as an infected user jeopardizes the safety of all its friends.

So far, the research community has paid little attention to OSN apps specifically. Most research related to spam and malware on Facebook has focused on detecting malicious posts and social spam campaigns. At the same time, in a seemingly backwards step, Facebook has dismantled its app rating functionality recently. 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 What App? though these could be very powerful in the future, so far they have received little adoption. We discuss previous work in more detail in Section VIII. In this paper, we develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from My Page Keeper, a security app in Facebook that monitors the Facebook profiles of 2.2 million users. We analyze 111K apps that made91million posts over 9 months.

2. Methodology

13% of observed apps are malicious. We show that malicious apps are prevalent in Facebook and reach a large numberofusers.Wefindthat13%ofappsinourdatasetof 111K distinct apps are malicious. Also, 60% of malicious apps endanger 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. 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%ofunique 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: 1) 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 2) others that require a cross-user view to aggregate information across time and across apps (e.g., the posting behavior of the app and the similarity of its name to other apps). The emergence of app-nets: Apps collude at massive scale. We conduct a forensics investigation on the malicious app ecosystem to identify and quantify the techniques used to promote malicious apps. We find that apps collude and collaborate at a massive scale. Apps promote other apps via posts that point to the "promoted" apps. If we describe the collusion relationship of promoting–promoted apps as a graph, we find 1584 promoter apps that promote 3723 other apps. 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. We were surprised to find popular good apps, such as Farm Ville and Facebook for iPhone, posting malicious posts. On further investigation, we found a lax authentication rule in Facebook that enabled hackers to make malicious posts appear as though they came from these apps.

FRAppE can detect malicious apps with 99% accuracy. We develop FRAppE (Facebook's Rigorous Application Evaluator) to identify malicious apps using 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 available on-demand, can identify malicious apps with 99.0% accuracy, with low false positives (0.1%) and high true positives (95.6%). By adding aggregation-based information, FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and higher true positives (95.9%). Our recommendations to Facebook. The most important message of the work is that there seems to be a parasitic Eco-system of malicious apps within Facebook that needs to be understood and stopped. However, even this initial work leads to the following recommendations for Facebook that could potentially also be useful to other social platforms. 1) Breaking the cycle of app propagation. We recommend that apps should not be allowed to promote other apps. This is there as on that malicious apps seem to gain strength by self-propagation. Note that we only suggested against a special kind of app promotion where the user clicks the app A installation icon, app A redirects the user to the intermediate installation page of app B, and the user cannot see the difference unless she examines the landing URL very carefully where client ID is different. At the end, the user ends up installing app B although she intended to install app A. Moreover, cross promotion among apps is forbidden as per Facebook's platform policy [16]. 2) Enforcing stricter app authentication before posting. We recommend a stronger authentication of the identity of an app before a post by that app is accepted. As we saw, hackers fake the true identify of an app in order to evade detection and appear more credible to the end user.

3. Implementation

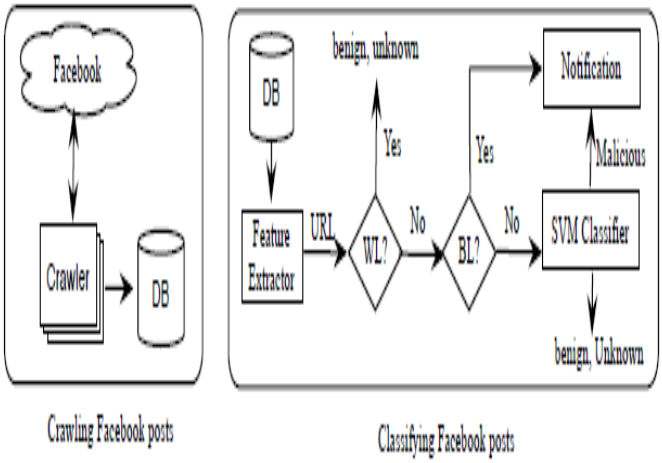

Figure 1 System Architecture

With 20 million installs a day, third-party apps are a major reason for the popularity and addictiveness of Facebook. 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 Facebook 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 Facebook. To develop FRAppE, we use information gathered by observing the posting behavior of 111K Facebook apps seen across 2.2 million users on Facebook.

First, we identify a set of features that help us distinguish malicious apps from benign ones. For example, we find that malicious apps often share names with other apps, and they typically request

fewer permissions than benign apps. Second, leveraging these distinguishing features, we show that FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and a high true positive rate (95.9%). Finally, we explore the ecosystem of malicious Facebook 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 1584 apps enabling the viral propagation of 3723 other apps through their posts. Long term, we see FRAppE as a step toward creating an independent watchdog for app assessment and ranking, so as to warn Facebook users before installing apps.

4. Conclusion

Applications present convenient means for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of malicious apps and how they operate. In this paper, using a large corpus of malicious Facebook apps observed over a 9-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 benign apps. Leveraging our observations, we developed FRAppE, an accurate classifier for detecting malicious Facebook applications. Most interestingly, we highlighted the emergence of app-nets—large groups of tightly connected applications that promote each other. We will continue to dig deeper into this ecosystem of malicious apps on Facebook, and we hope that Facebook will benefit from our recommendations for reducing the menace of hackers on their platform. In this survey, we explored various research attempts towards exploring the Facebook network, analyzing malicious content on it, and analyzing events on online social media in general. The aim of this survey was to look at relevant literature, which could aid in studying and combating malicious user generated content spread on Facebook during events. In order to keep this survey focused, we did not cover a variety of possibly relevant research areas including detection of compromised / fake accounts, and sybil nodes in the Facebook network, detection of spam on other social networks like Twitter, credibility / trustworthiness of information of user generated content, and event detection in online social media. We also looked at the various challenges and limitations posed by Facebook (as discussed in Section 3). Apart from technical limitations, there exist various research gaps in existing literature, which are yet to be addressed and explored.

5. Acknowledgements

We take this opportunity to express heartily thanks to all those who helped us in the completion of the project Phase-1 on "**Detecting Malicious Facebook Applications"**
We express deep sense of gratitude to our Project Guide Prof. S. A. Aher and H.O.D. Prof. P.V.Waje, Asst. Prof., INFORMATION TECHNOLOGY DEPARTMENT, Sir Visvesvaraya Institute of Technology, Chincholi for their guidance and continuous motivation. We gratefully acknowledge the help provided by our Project Guide Prof S. A. Aher on many occasions for improvement of this project with great interest. We would like to extend our sincere thanks to our family members. It is our privilege to acknowledge their cooperation during the course of this Project. We express heartiest thanks to my known and unknown well-wishers for their unreserved cooperation, encouragement and suggestions during the course of this Project. Last but not the least, We would like to thanks to my all teachers, and all my friends who helped us with the ever daunting task of gathering information for the Project.

6. References

[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] "Whiich 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.htm

[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.

[11] H. Gao*et al.*, "Detecting and characterizing social spam campaigns," in *Proc. IMC*, 2010, pp. 35–47.

[12] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards online spam filtering in social networks," in *Proc. NDSS*, 2012.