isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 3 Mar,2017,ISSN_NO: 2321-3337

DETECTING MALICIOUS APPLICATIONS IN FACEBOOK

Prem Kumar .R , Avinash .M , Sri Gokul Krishnan .R

D.Lavanya (Asst. Professor), Department of Computer Science,

Loyola Institute of Technology Chennai, India.

ABSTRACT — *With 20 million installs a day, third-party apps area 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 less permission than be nign 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*

Keywords — Facebook apps, malicious, online social networks, spam.

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 [2] 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 [1]. Furthermore, many apps have acquired and maintain a really large user base. For instance, FarmVille and City Ville apps have 26.5Mand 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:

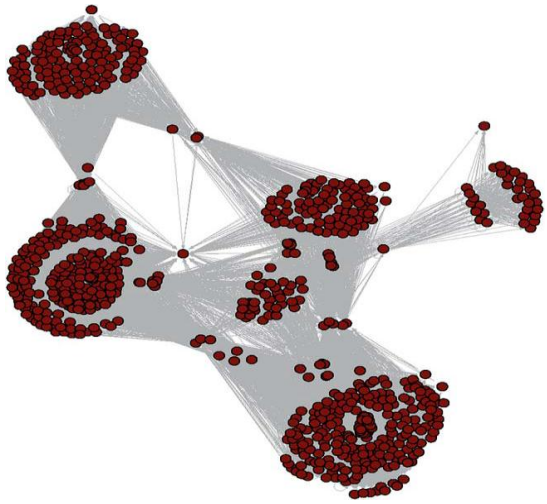
1) the app can reach large numbers of users and their friends to spread spam.

2) the app can obtain users personal information such as e-mail address, home town.

3) 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 [8]. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day [9].Despite the above worrisome trends, today a user has very limited information 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 .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 made 91 million posts over 9 months. 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. Our work makes the following key contributions



13% of observed apps are malicious. We show that malicious apps are prevalent in Facebook and each a large number of users. We find that 13% of apps in our dataset of111K 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 being an 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 than10 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. Furthermore, these apps form large and highly dense connected

components, as shown in Fig. 1.Furthermore, hackers use fast-changing indirection: Application posts have URLs that point to a Web site, and the Web site dynamically redirects to many different apps; we find 103 such URLs that point to 4676 different malicious apps over the course of a month. These observed behaviors 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*. 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%).

EXISTING SYSTEM:

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. and Rahman et al. develop efficient techniques for online spam filtering on OSNs such as Facebook. While Gao et al. relyon having the whole social graph as input, and so is usable only by the OSN provider, Rahman et al. Develop a third-party application for spam detection on Facebook. Others present mechanisms for detection of spam URLs on Twitter. 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: Yang et al. and Benevenu to et al. developed techniques to identify accounts of spammers on Twitter. Others have proposed a honey-pot-based approach to detect spam account son OSNs. Yard et al. analyzed behavioral patterns among spam accounts in Twitter. Instead of focusing on account s created by spammers, our work

enables detection of malicious apps that propagate spam and malware by luring normal users to install them. App Permission Exploitation: Chia et al. 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 apps tend to request more permission. To address privacy risks for using Facebook apps, some studies propose a new application policy and authentication dialog. Makridakiset al. use a real application named "Photo of the Day" to demonstrate how malicious app son Facebook can launch distributed denial-of-service (DDoS) attacks using the Facebook platform. King et al. conducted a survey to understand users interaction with Facebook apps. Similarly, Gjokaetal. study the user reach of popular Facebook applications. 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.

PROPOSED SYSTEM:

Our work makes the following key contributions.

• 13% of observed apps are malicious. We show that malicious apps are prevalent in Facebook and reach a large number of users. We find that 13% of apps in our dataset of111K 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.

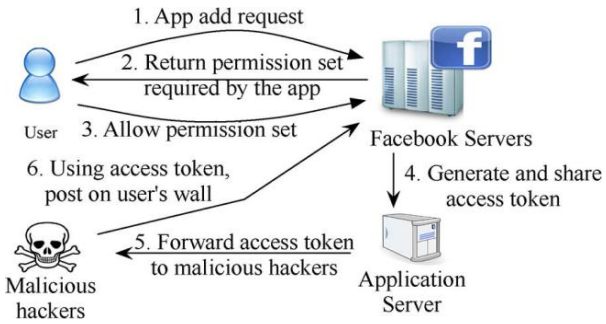
• Malicious and benign app profiles significantly differ. We systematically profile apps and show that malicious app profiles are significantly different than those of benign apps. A striking observation is the "laziness" of hackers; many malicious apps have the same name, as 8%of unique names of malicious apps are each used by more than10 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 apps co system 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.

• 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%).

ARCHITECTURE DIAGRAM:



MODULES

1. Users
2. Admin

1. User

Registration:

In this module if a user wants to access the data which is register Apps to Database and play apps/ games, he/she should register their details first. These details are maintained in a Database

User Login:

In this module, any of the above mentioned person have to login, they should login by giving their username and password.

Users

In this module a user s has register apps after admin updates the Apps Status and App License ID. Then User want to view Apps update details and view Apps center. Finally play apps /games. These details are maintained in a database. These details are maintained in a database.

2.Admin

Admin to check all register Apps and to update Apps Status and Apps license ID .Admin to detected Malicious and blocked Apps site also .These details are maintained in a database. These details are maintained in a database.

VIII. CONCULSION AND FUTUREWORK

- 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.

REFERENCES

- C.Pring, "100 social media statistics for 2012," 2012 [Online]. Available:http://thesocialskinny.com/100-social-media-statistics-for-2012/
- Facebook, Palo Alto, CA, USA, "Facebook Open graph API," [Online].Available: http://developers.facebook.com/docs/reference/api/
- "Wiki: Facebook platform," 2014 [Online]. Available: http://en.wikipedia.org/wiki/Facebook Platform
- "Pr0file stalker: Rogue Facebook application," 2012 [Online]. Available:https://apps.facebook.com/mypagekeeper/?status=scam_report-_fb_survey_scam_pr0file_viewer_2012_4_4
- "Which cartoon character are you—Facebook surveyscam," 2012 [Online]. Available:
- G. Cluley, "The Pink Facebook rogue application and survey scam,"2012 [Online]. Available: http://nakedsecurity.sophos.com/2012/02/27/pink-facebook-survey-scam
- D. Goldman, "Facebook tops 900 million users," 2012 [Online].Available: http://money.cnn.com/2012/04/23/technology/facebookq1/index.htm
- R. Naraine, "Hackers selling $25 toolkit to create malicious Facebookapps," 2011 [Online]. Available: http://zd.net/g28HxI
- HackTrix, "Stay away from malicious Facebook apps," 2013 [Online].Available: http://bit.ly/b6gWn5
- 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.