ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Frappe: Secure Malicious Identifier in Face Book Application

Ch. Ramesh Kumar
Associate Professor & HoD
Department of CSE,
Malla Reddy Engineering College & Management Sciences,
Kistapur, Medchal, Hyderabad.

P Radhika
Assistant Professor,
Department of CSE,
Malla Reddy Engineering College & Management Sciences,
Kistapur, Medchal, Hyderabad.

Thummala Pranay Kumar
M.Tech (CSE)
Department of CSE,
Malla Reddy Engineering College & Management Sciences,
Kistapur, Medchal, Hyderabad.

Abstract:

Online Social Networks (OSNs) witness a rise in user activity whenever an event takes place. Malicious entities exploit this spur in user-engagement levels to spread malicious content that compromises system reputation and degrades user experience. It also generates revenue from advertisements, clicks, etc. for the malicious entities. Facebook, the world's biggest social network, is no exception and has recently been reported to face much abuse through scams and other type of malicious content, especially during news making events. Recent studies have reported that spammers earn $200 million just by posting malicious links on Facebook. In this paper, we characterize malicious content posted on Facebook during 17 events, and discover that existing efforts to counter malicious content by Facebook are not able to stop all malicious content from entering the social graph. Our findings revealed that malicious entities tend to post content through web and third party applications while legitimate entities prefer mobile platforms to post content. In addition, we discovered a substantial amount of malicious content generated by Facebook pages. Through our observations, we propose an extensive feature set based on entity profile, textual content, metadata, and URL features to identify malicious content on Facebook in real time and at zero-hour. This feature set was used to train multiple machine learning models and achieved an accuracy of 86.9%. The intent is to catch malicious content that is currently evading Facebook's detection techniques.

Our machine learning model was able to detect more than double the number of malicious posts as compared to existing malicious content detection techniques. Finally, we built a real world solution in the form of a REST based API and a browser plug-in to identify malicious Facebook posts in real time.

INTRODUCTION

Social network activity rises considerably during events that make the news, like sports, natural calamities, etc. Facebook, world's biggest social network, is no exception. Being the most preferred OSN for users to get news, Facebook is potentially one of the most lucrative OSNs for malicious entities. Recently, a group of malicious users exploited the famous biting incident during the World Cup,.The petition required a user to sign in with details such as name, country of residence, mobile phone number and email address. The petitioner could potentially end up on a spam mailing list, on the receiving end of a malicious attachment or even subjected to a targeted attack. In another recent incident of Malaysian Airline MH17 flight crash, scammers placed dozens of socalled 'community pages' on Facebook, dedicated to victims of the tragedy. On the page, Facebook users

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

were tricked into clicking links showing extra or unseen footage of the crash. Instead of seeing a video, they were led to various pop-up ads for porn sites or online casinos. 3 Such activity not only violates Facebook's terms of service, but also degrades user experience. It has been claimed that Facebook spammers make $200 million just by posting links. 4 Facebook has confirmed spam as a serious issue, and taken steps to reduce spam and malicious content in users' newsfeed recently (Owens and Turitzin 2014).

The problem of identifying malicious content is not specific to Facebook and has been widely studied on other OSNs in the past. Researchers have used feature based machine learning models to detect spam and other types of malicious content on OSNs like Twitter, and achieved good results (Benevenuto et al. 2010; Grier et al. 2010). However, existing approaches to detect malicious content in other OSNs like Twitter, cannot be directly ported to Facebook because they heavily rely on features that aren't publicly available from Facebook. These include profile, and network information, age of the account, total number of messages posted, number of social connections, etc. In this paper, we highlight that existing techniques used by Facebook for countering malicious content do not eliminate all malicious posts completely. Although Facebook's immune system (Stein, Chen, and Mangla 2011) seems to perform well at protecting its users from malicious content, our focus is on detecting the fraction of content which evades this system. We identify some key characteristics of malicious content spread on Facebook, which distinguishes it from legitimate content. Our dataset consists of 4.4 million public posts generated by 3.3 million unique entities during 17 events, across a 16 month time frame (April 2013 - July 2014).

We then propose an extensive set of 42 features which can be used to distinguish malicious content from legitimate content in real time and at zero-hour. We emphasize on zerohour detection because content on OSNs spreads like wild- fire, and can reach thousands of users within seconds. Such velocity and reach of OSN content makes it hard to control the spread of malicious content, if not detected instantly. We apply machine learning techniques to identify malicious posts on Facebook using this feature set and achieve a maximum accuracy of 86.9% using the Random Forest classifier. We also compare our technique with past research and find that our machine learning model is able to detect more than twice the number of malicious posts as compared to clustering based campaign detection techniques used in the past.

LITERATURE SURVEY

a) A technique for computer detection and correction of spelling errors:

The method described assumes that a word which cannot be found in a dictionary has at most one error, which might be a wrong, missing or extra letter or a single transposition. The unidentified input word is compared to the dictionary again, testing each time to see if the words match—assuming one of these errors occurred. During a test run on garbled text, correct identifications were made for over 95 percent of these error types.

b) LIBSVM: A library for support vector machines:

LIBSVM is a library for Support Vector Machines (SVMs). We have been actively developing this package since the year 2000. The goal is to help users to easily apply SVM to their applications. LIBSVM has gained wide popularity in machine learning and many other areas. In this article, we present all implementation details of LIBSVM. Issues such as solving SVM optimization problems theoretical convergence multiclass classification probability estimates and parameter selection are discussed in detail.

c) Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs

Malicious Web sites are a cornerstone of Internet criminal activities. As a result, there has been broad

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

interest in developing systems to prevent the end user from visiting such sites. In this paper, we describe an approach to this problem based on automated URL classification, using statistical methods to discover the tell-tale lexical and host-based properties of malicious Web site URLs. These methods are able to learn highly predictive models by extracting and automatically analyzing tens of thousands of features potentially indicative of suspicious URLs.

d) Design and evaluation of a real-time URL spam filtering service

On the heels of the widespread adoption of web services such as social networks and URL shorteners, scams, phishing, and malware have become regular threats. Despite extensive research, email-based spam filtering techniques generally fall short for protecting other web services. To better address this need, we present Monarch, a real-time system that crawls URLs as they are submitted to web services and determines whether the URLs direct to spam. We evaluate the viability of Monarch and the fundamental challenges that arise due to the diversity of web service spam. We show that Monarch can provide accurate, real-time protection, but that the underlying characteristics of spam do not generalize across web services. In particular, we find that spam targeting email qualitatively differs in significant ways from spam campaigns targeting Twitter. We explore the distinctions between email and Twitter spam, including the abuse of public web hosting and redirector services. Finally, we demonstrate Monarch's scalability, showing our system could protect a service such as Twitter--which needs to process 15 million URLs/day--for a bit under $800/day.

e) Detecting spammers on social networks

Social networking has become a popular way for users to meet and interact online. Users spend a significant amount of time on popular social network platforms (such as Facebook, MySpace, or Twitter), storing and sharing a wealth of personal information. This information, as well as the possibility of contacting thousands of users, also attracts the interest of cybercriminals. For example, cybercriminals might exploit the implicit trust relationships between users in order to lure victims to malicious websites. As another example, cybercriminals might find personal information valuable for identity theft or to drive targeted spam campaigns.

In this paper, we analyze to which extent spam has entered social networks. More precisely, we analyze how spammers who target social networking sites operate. To collect the data about spamming activity, we created a large and diverse set of "honey-profiles" on three large social networking sites, and logged the kind of contacts and messages that they received. We then analyzed the collected data and identified anomalous behavior of users who contacted our profiles.

EXISTING SYSTEM

Recently, hackers have started taking advantage of the recognition of this third-party apps platform and deploying malicious applications. Malicious apps will give a profitable business for hackers, given the recognition of OSNs, with Facebook leading the manner with 900M active users.

- There square measure many ways that hackers will like a malicious app:
- The app will reach giant numbers of users and their friends to unfold spam,
- The app will get users' personal data like email address, home town, and gender.
- The app will "re-produce" by creating different malicious apps widespread.

As a results of the on top of issues, there square measure several malicious apps spreading on Facebook on a daily basis. As a result of user has terribly restricted data at the time of putting in AN app on his Facebook profile as user doesn't acknowledge the projected app is malicious or not solely the identity variety.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

LIMITATIONS

- Hackers spreading malwares exploitation app.
- Many malicious apps spreading on Facebook

PROPOSED SYSTEM

During this project, we have a tendency to develop FRAppE, a collection of economical classification techniques for distinguishing whether or not Associate in Nursing app is malicious or not. To create FRAppE, we have a tendency to use information from MyPageKeeper. To create FRAppE, we have a tendency to use information from MyPageKeeper, a security app in Facebook that monitors the Facebook profiles of two.2 million users. We have a tendency to analyse 111K apps that created close to regarding ninety one million posts over 9 months. This is often definitely the primary comprehensive study specializing in malicious Facebook apps that focuses on quantifying, profiling, and understanding malicious apps, and synthesizes this info into an efficient detection approach. We've got introduced 2 options i.e. classifiers to discover the malicious apps FRAppE fat-free and FRAppE. In 1st classifier it discover the initial level detection e.g. apps identity variety, name and supply etc. and in second level detection the particular detection of malicious app has been done.

ADVANTAGES:

- Facebook Rigorous Application Evaluator is the tool to detect malicious apps.
- It provides security to users profiles from malicious apps on any social networking sites.
- It is more accurate classifier than the any other classifiers like SVM.

METHODOLOGY

There exists a wide range of malicious content on OSNs today. These include phishing URLs, spreading malware, advertising campaigns, content originating from compromised profiles, artificial reputation gained through fake likes, etc. We do not intend to address all such attacks. We focus our analysis on identifying posts containing one or more malicious URLs and creating automated means to detect such posts in real time, without looking at the landing pages of the URLs. We emphasize on not visiting the landing pages of URLs since this process induces time lag and increases the time taken by real time systems to make a judgment on a post. Existing methods involve detection of such malicious posts by grouping them into campaigns (Gao et al. 2010), or by looking up public blacklists like PhishTank, Google Safebrowsing, etc. to identify malicious URLs. However, as previously discussed, both campaign detection techniques and URL blacklists prove ineffective while the attack is new. For the scope of this work, we refer to a post as malicious if it contains one or more malicious URLs.

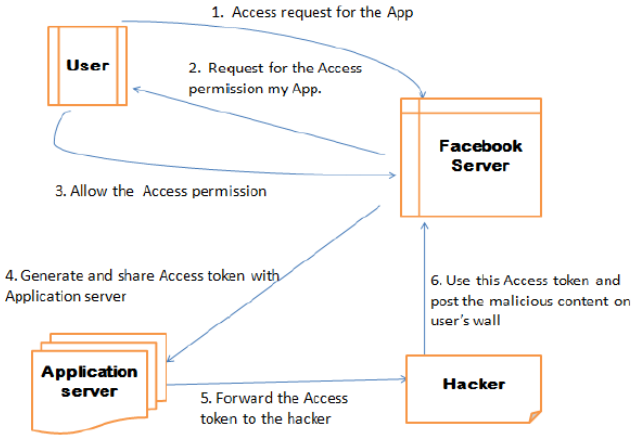

Fig:- Operation of Facebook Malicious Application

IMPLEMENTATION

a) 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 than 10 different apps (as defined by their app IDs). Overall, we profile apps based on two classes of features: (a) 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 (b) others that

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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).

b)The emergence of AppNets: 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. The most interesting result is 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 1,584 promoter apps that promote 3,723 other apps. Furthermore, these apps form large and highly-dense connected components, Furthermore, hackers use fast-changing indirection: applications posts have URLs that point to a website, and the website dynamically redirects to many different apps; we find 103 such URLs that point to 4,676 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 AppNet, since they seem a parallel concept to botnets.

c) Malicious hackers impersonate applications:

We were surprised to find popular good apps, such as 'FarmVille' 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.

d) FRAppE can detect malicious apps with 99% accuracy:

We develop FRAppE (Facebook's Rigorous Application Evaluator) to identify malicious apps 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 false negatives(4.4%). By adding aggregation-based information, FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and lower false negatives (4.1%).

RELATED WORK

Facebook has its own immune system (Stein, Chen, and Mangla 2011) to safeguard its users from unwanted malicious content. Researchers at Facebook built and deployed a coherent, scalable, and extensible real time system to protect their users and the social graph. This system performs real time checks and classifications on every read and write action.

Designers of this complex system used an exhaustive set of components and techniques to differentiate between legitimate actions and spam. These components were standard classifiers like Random Forest, Support Vector Machines, Logistic Regression, a feature extraction language, dynamic model loading, a policy engine, and feature loops. Interestingly, despite this complex immune system deployed by Facebook, unwanted spam, phishing, and other malicious content continues to exist and thrive on Facebook. Although the immune system deployed by Facebook utilizes a variety of techniques to safeguard its users, authors did not present an evaluation of the system to suggest how accurately and efficiently the system is able to capture malicious content.

CONCLUSION

OSNs witness large volumes of content during real world events, providing malicious entities a lucrative environment to spread scams, and other types of malicious content. We studied content generated during 17 such events on Facebook, and found substantial presence of malicious content which evaded Facebook's existing immune system and made it to the social graph. We observed characteristic differences between malicious and legitimate posts and used them to train machine learning models for automatic detection of malicious posts. Our extensive feature set was completely derived from public information available at zero-hour, and was able to

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

detect more than double the number of malicious posts as compared to existing spam campaign detection techniques. Finally, we deployed a real world solution in the form of a REST based API and a browser plug-in to identify malicious Facebook posts in real time.

During this work, employing a great amount of malicious Facebook applications we tend to shows that malicious applications area unit considerably take issue from mild apps with the many options. For instance, malicious apps area unit possible to share names with different applications, and that they usually request fewer permissions than mild apps.

Investment our observations, we tend to developed FRAppE, associate correct classifier for sleuthing malicious Facebook applications. Most apparently, we tend to highlight the emergence of AppNets massive teams of tightly connected applications that promote one another. We are going to still dig deeper into this scheme of malicious apps on Facebook, and that we hope that Facebook can benefit from our recommendations for reducing the menace of hackers on their platform.

FUTURE ENHANCEMENT

we would like to test the performance and usability of our browser plug-in. We would also like to investigate Facebook pages spreading malicious content in further detail. Further, we intend to study malicious Facebook posts which do not contain URLs.

Already FACEBOOK Application is Existed in real time, but in this project we have enhanced with more reliable in detecting.Implement this project in Facebook for Real time.While the user is blocked, the Alert Message should exist on Email, So that user knows that he/she was Blocked.

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. Gao et 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.

Author Details

Thummala Pranay Kumar completed his B.E degree in vasavi college of engineering in 2014. He is

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

pursuing M.Tech. in Computer Science & Engineering from Department of Computer Science & Engineering in Malla Reddy Engineering College & Management sciences, Kistapur, Medchal, Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA, India. His research interest includes cloud, data mining, Big Data and networking.

P Radhika, working as Assistant Professor, department of computer science and engineering, in Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal ,Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA., India. Her research interests include data mining, computer networks.

Ch. Ramesh Kumar, working as Assoc. Prof & Head of the Department of Computer Science and Engineering in Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal, Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA., India. he has several international publications to his credit. His research interests include Software reuse, Software performance, Software testing ,Data Mining and cloud computing.