Scientific Journal Impact Factor (SJIF) : 3.518

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

Review On
Social Networking Application Evaluator: Detecting Malicious Social Networking Applications

Mr. Sumit R. Notawale and Prof. Juned A Khan

Student of Master of Engineering in CSE, G.H. Raisoni college of Engineering &Management, Amravati, India

Assistant professor Department of CSE,G.H. Raisoni college of Engineering & Management, Amravati, India

Abstract- With the large number of users installed, third-party apps are a major reason for the popularity and habitual of using the Facebook application. Recently, hackers have started misusing of this third-party apps platform and deploying malicious applications, spreading Malicious application and extracting the user's personal profile information data from the application because Malicious apps can provide a good business for hackers. This is the major issue, as we find that numbers of applications in our dataset are malicious. So that, Our purpose is creating a Facebook application, through which we understand it is malicious or not? Our goal is to develop a FRAppE - Facebook's Rigorous Application Evaluator which will help in detecting malicious applications on Facebook.

Keywords: *Facebook Apps, Malicious Apps, Profiling Apps, Online Social Networks.*

I. INTRODUCTION

We develop Social Networking Application Evaluator Detecting Malicious Social Networking Application, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build Social Networking Application Evaluator Detecting Malicious Social Networking Application, For example we use data from MyPageKeeper, a security app in Social networks that monitors the Social networks profiles of 2.2 million users. We analyze 111K apps that made 91 million posts over nine months. This is arguably the first comprehensive study focusing on malicious Social networks apps that focuses on quantifying, profiling, and understanding malicious apps, and synthesizes this information into an effective detection approach.

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 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).

II. RELATED WORK

Detecting and characterizing social spam campaigns. Gao et al. [1] 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. Towards online spam filtering in social networks. Rahman et al. [2] develop efficient techniques for online spam filtering on Social networking applications such as Facebook, Twitter, and Instagram. In other work, Towards online spam filtering in social networks. Gao et al. [2] and Efficient and Scalable Socware Detection in Online Social Networks. Rahman et al. [3] develop efficient techniques for online spam filtering on Online Social Networking sites such as Facebook In this paper, we describe our work to provide online spam filtering for social networks. We use text shingling and URL comparison to incrementally reconstruct spam messages into campaigns, which are then identified by a trained classifier. We evaluate the system on two large datasets composed of over 187 million Facebook wall messages and 17 million tweets, respectively. The experimental results demonstrate that the system achieves high accuracy.

Detecting suspicious urls in twitter stream. S. Lee and J. Kim. [4] And Design and Evaluation of a Real-Time URL Spam Filtering Service. K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song. [5] Presents the 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. Die free or live hard? Empirical evaluation and new design for fighting evolving twitter spammers. Yang et al. [6] and Detecting spammers on Twitter. Benevenuto et al. [7] developed techniques to identify accounts of spammers on Twitter. Recommend that apps should not be allowed to promote other apps. This is the reason that malicious apps seem to gain strength by self-propagation. Others have proposed a honey-pot based approach [8, 9] to detect spam accounts on Social Networking Applications.

Detecting spam in a twitter network. Yardi et al. [10] In this paper analyzed behavioral patterns among spam accounts in Twitter. 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. Is this app safe? A large scale study on application permissions and risk signals. Chia et al. [11] investigated the privacy intrusiveness of Facebook apps and concluded that currently available signals such as community ratings, popularity, and external ratings such as Web of Trust as well as signals from app developers 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. They also found that 'Lookalike' applications that have names similar to popular applications request more permissions than is typical. Based on a measurement study across 200 Facebook users.

Analyzing facebook privacy settings: user expectations vs. reality. Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. [12] In this paper showed that privacy settings
in Facebook rarely match users' expectations. In this paper only represent how the application can protect the malicious message or malicious post. So from this paper we are unable to protect the malicious applications in this paper they are failed to protect the application from the malicious applications. Characterization Of Osn applications Gjoka et al. [13] 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

III. PROBLEM DEFINITION

In social networking sites they having their own malicious detecting apps for example in facebook they designed My Page Keeper app to protect the malicious posts on the wall of facebook, but they don't have a application which will detect the third party malicious applications so that they can protect the user's personal information, and same things also happen with the twitters message systems(twits), they fails to protect from a malicious third party applications so that to overcome this problems and to get maximum accuracy of the solutions we are trying to design Social Networking Application Evaluator Detecting Malicious Social Networking Application.

Also, malicious applications that are forcing the users to fill their personal information and complete that form provided by third party applications due to with this process the users spend a lot of time in that durations the hackers are taking the advantage of this opportunity to hack personal information's of the users. Social Networking Application Evaluator Detecting Malicious Social Networking Application will restrict them and won't allow the user to fill up their personal information so that users can be protected from this malicious kind of the third party applications.

IV. PROPOSED SYSTEM

In this work, we develop Social Networking Application Evaluator Detecting Malicious Social Networking, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build Social Networking Application Evaluator Detecting Malicious Social Networking, we use data from My Page Keeper, a security app in Social networking application that monitors the Social networking application profiles of millions users. We analyze lots of apps that made millions posts over nine months. This is arguably the first comprehensive study focusing on malicious Social networking application apps that focuses on quantifying, profiling, and understanding malicious apps, and synthesizes this information into an effective detection approach.

Detecting spam on OSNs:

We analyzed posts on the walls of million Social networking app users and showed that 10% of links posted on Social networking app walls are spam. They also presented techniques to identify compromised accounts and spam campaigns. In other work, we develop efficient techniques for online spam filtering on OSNs such as Social networking app. While rely on having the whole social graph as input, and so, is usable only by the OSN provider, develop a third-party application for spam detection on Social networking app. Others present mechanisms for detection of spam URLs on Social networking app. 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 Social networking app.

In the proposed methodology diagram clearly showing that when the user inserting the post, then system methodology will checking out the post at two check post that is black listed keywords and the URL contains. If the post is text shingling then it would be verified with the blacklisted key words or else if it is url links then it will check out url contains with the help of web mining technology, then system will calculating the post percentage and if the percentage is more than 67.33% then it won't be published, and it will goes to the waiting queue and it will get blocked the post by the system administrative.

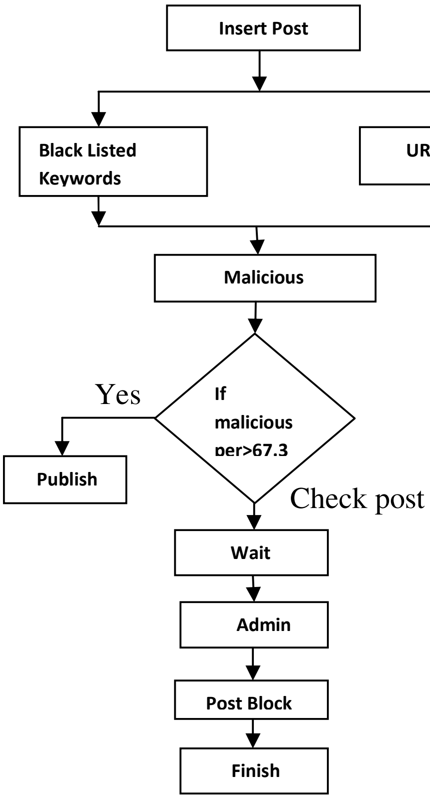

Fig: Proposed Methodology

V. CONCLUSION

Applications present a convenient means for hackers to spread malicious content on Social networks. However, little is understood about the characteristics of malicious apps and how they operate. In this work, using a large corpus of malicious Social networks app observed over a nine 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 less permission than benign apps. Leveraging our observations, we developed Social Networking Application Evaluator: Detecting Malicious Social Networking Applications, an accurate classifier for detecting malicious Social networks applications. Most interestingly, we highlighted the emergence of AppNets— large groups of tightly connected applications that promote each other. We will continue to dig deeper into this ecosystem of malicious apps on Social networks, and we hope that Social networks application will benefit.

REFERENCES

[1] H. Gao, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," In IMC, 2010.

[2] J. Ma, L. K. Saul, S. Savage, and G. M. Volker, "Beyond blacklists: learning to detect malicious web sites from suspicious urls," In KDD, 2009.

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

[4] S. Lee and J. Kim, "Warningbird: Detecting suspicious urls in twitter stream," In NDSS, 2012.

[5] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, "Design and Evaluation of a Real-Time URL Spam Filtering Service," In Proceedings of the IEEE Symposium on Security and Privacy, 2011.

[6] C. Yang, R. Harkreader, "Die free or live hard? Empirical evaluation and new design for fighting evolving twitter spammers," In RAID, 2011.

[7] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida, "Detecting spammers on Twitter," In CEAS, 2010.

[8] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: social honeypots + machine learning," In SIGIR, 2010.

[9] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," In ACSAC, 2010.

[10] S. Yardi, D. Romero, G. Schoenebeck et al, "Detecting spam in a twitter network," First Monday, 2009.

[11] P. Chia, Y. Yamamoto, and N. Asokan. Is this app safe? A large scale study on application permissions and risk signals," In WWW, 2012.

[12] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," In IMC, 2011.

[13] M. Gjoka, M. Sirivianos, A. Markopoulou, and X. Yang, "Characterization Of Osn applications," In Proceedings of the first workshop on Online social networks, WOSN, 2008.

[14] T. Stein, E. Chen, and K. Mangla, "Facebook immune system," In Proceedings of the 4th Workshop on Social Network Systems, 2011.

[15] GAO, H., HU, J., WILSON, C., LI, Z., CHEN, Y., AND ZHAO, B. Y. "Detecting and characterizing social spam campaigns," In *Proceedings of the 10th annual conference on Internet measurement* (New York, NY, USA, 2010), IMC '10, ACM.