A Study On Social Networking Malicious Activities and Prevention Techniques

Palash Pramod Patil
BE Computer Engineering
NBN Sinhgad School Of Engineering, Pune

Sanket Narayan Mane
BE Computer Engineering
NBN Sinhgad School Of Engineering, Pune

Ajinkya Santosh Patil
BE Computer Engineering
NBN Sinhgad School Of Engineering, Pune

Shailesh Marutirao Rathod
BE Computer Engineering
NBN Sinhgad School Of Engineering, Pune

***Abstract*— With the increasing use of social networking site, there are increments in the malicious, fake, and viruses. Daily approximately 20 million users will register in one day on different social networking site. Unfortunately, hackers have realized the potential of using apps for spreading malware and spam. And now days this problem is more critical, as our survey find that at least 13% of apps in our dataset are malicious. And due to this the research community has focused on detecting malicious posts and campaigns. In this paper, we took the survey of some social networking sites and application and malicious activity relates to it. Also we mention the different techniques to control malicious activities for different social networking sites like Twitter, Facebook.**

***Keywords*— Facebook Apps, Malicious Apps, Profiling Apps, Online Social Networks, Social Network Security, Spam profiles**

I. INTRODUCTION

A web threat is any threat that uses the World Wide Web to facilitate cybercrime. Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web. They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets. Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking.

Online social networks (OSN) 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 a large user base. For instance, Farmville and CityVille apps have 26.5M user data.

The online social networking websites like Facebook, twitter, Myspace etc. are used by millions of people to communicate with each other though they're so much away from one another. Simply because of this on-line social networking site people can send their information, video, audio or even web pages also. This can be the terribly huge advantages of those sites and aim of the developer. In this on-line social networking website the net service providers are important component. They are connected with the user through some interface. Many papers have been published on the detection of spam profiles in OSNs. But so far very few review paper has been published in this field which consolidated the current research. Our paper aims to provide a review of the academic research and work done in this field by various researchers and highlight the future research direction.

II. PREVIOUS WORK DONE

In paper [1] they mentioned Facebook applications are one of the reasons for Facebook attractiveness. Unfortunately, numerous users are not aware of the fact that many malicious Facebook applications exist. To educate users, to raise user's awareness and to improve Facebook user's security and privacy, they developed a Firefox add-on that alerts users to the number of installed applications on their Facebook profiles. In this study, they present the temporal analysis of the Facebook applications installation and removal dataset collected by our add-on. This dataset consists of information from 2,945 users, collected during a period of over a year. They used linear regression to analyse our dataset and discovered the linear connection between the average percentage change of newly installed Facebook applications and the number of days passed since the user initially installed our add-on. Additionally, They found out that users who used our Firefox add-on become more aware of their security and privacy installing on average fewer new applications. Finally, they discovered that on average 86.4% of Facebook users install an additional application every 4.2 days.

In paper [2] they focus on another application called twitter. Twitter spam detection is a recent area of research in which most previous works had focused on the identification of malicious user accounts and honeypot-based approaches. However, in this paper they present a methodology based on two new aspects: the detection of spam tweets in isolation and without previous information of the user; and the application of a statistical analysis of language to detect spam in trending topics. Trending topics capture the emerging Internet trends and topics of discussion that are in everybody's lips. This growing microblogging phenomenon therefore allows spammers to disseminate malicious tweets quickly and massively. In this paper we present the first work that tries to detect spam tweets in real time using language as the primary tool. They first collected and labeled a large dataset with 34 K trending topics and 20 million tweets. Then, they have proposed a reduced set of features hardly manipulated by

spammers. In addition, they have developed a machine learning system with some orthogonal features that can be combined with other sets of features with the aim of analysing emergent characteristics of spam in social networks. They have also conducted an extensive evaluation process that has allowed us to show how our system is able to obtain an F-measure at the same level as the best state-of the- art systems based on the detection of spam accounts. Thus, our system can be applied to Twitter spam detection in trending topics in real time due mainly to the analysis of tweets instead of user accounts.

In [3] they took survey on different technique to detect spammers. Impersonators, phishers, scammers and spammers crop up all the time in Online Social Networks (OSNs), and are harder to identify. Spammers are the users who send unsolicited messages to a large audience with the intention of advertising some product or to lure victims to click on malicious links or infecting user's system just for the purpose of making money. A lot of research has been done to detect spam profiles in OSNs. In this paper we have reviewed the existing techniques for detecting spam users in Twitter social network. Features for the detection of spammers could be user based or content based or both. Current study provides an overview of the methods, features used, detection rate and their limitations (if any) for detecting spam profiles mainly in Twitter. Spammers are the malicious users who contaminate the information presented by legitimate users and in turn pose a risk to the security and privacy of social networks. Spammers belong to one of the following categories [22]: 1. Phishers: are the users who behave like a normal user to acquire personal data of other genuine users. 2. Fake Users: are the users who impersonate the profiles of genuine users to send spam content to the friends' of that user or other users in the network. 3. Promoters: are the ones who send malicious links of advertisements or other promotional links to others so as to obtain their personal information.

In [4] paper they took survey of detection of suspicious URL on social networking sites. Social networking sites are used by billions of people to share the information with each other. To communicate with each other over the long distance. But it also attracts the attackers in carrying out different attacks or get the information being shared by the social networking sites users. Social networking sites users can send the messages to each other in the form of text, that texts have the size limitation of maximum 140 characters. So to share the web pages URL shorting is used. Attackers send the suspicious URLs in texts and move the users to malicious pages. This paper presents a survey of different methods used to detect the suspicious URL (sites) in twitter stream. This paper also presents a WARNING BIRD APPLICATION. It is a near real time system to detect the suspicious URLs by classifying them.

In [5] this is the main paper on which we going to focus. We are implementing this method by making some enhancement in the system. Their 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, they use information gathered by observing the posting behavior of 111K Facebook apps seen across 2.2 million users on Facebook. First, they identify a set of features that help us distinguish malicious apps from benign ones. For example, they find that malicious apps often share names with other apps, and they typically request less permission than benign apps. Second, leveraging these distinguishing features, they show that FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and a low false negative rate (4.1%). Finally, they explore the ecosystem of malicious Facebook apps and identify mechanisms that these apps use to propagate. Interestingly, they find that many apps collude and support each other; in our dataset, they find 1,584 apps enabling the viral propagation of 3,723 other apps through their posts. Long-term, they see FRAppE as a step towards creating an independent watchdog for app assessment and ranking, so as to warn Facebook users before installing apps.

III. CONCLUSION

Social networking sites and associated technologies can bring significant benefits to the business as well as to people, but as the use of these technologies grows, it will become difficult for organizations to tightly control all of the many forms of activities related to it. Many problems related to these can be control by some of the technique and we summarize these recent techniques to control malicious activities. We try to take the complete survey of all the technique in this paper.

REFERENCES

[1] Facebook Applications Installation and Removal: A Temporal Analysis, Dima Kagan, Michael Fire, Aviad Elyashar, and Yuval Elovici Telekom Innovation Laboratories and Information Systems Engineering Department, Ben-Gurion University of the Negev, Beer-Sheva, Israel Email: fkagandi,mickyfi,aviade, elovicig@bgu.ac.il

[2] Detecting malicious tweets in trending topics using a statistical analysis of language,Juan Martinez-Romo ⇑, Lourdes Araujo,NLP & IR Group, Dpto. Lenguajes y Sistemas Informáticos, Universidad Nacional de Educación a Distancia (UNED), Madrid 28040, Spain.

[3] Techniques to Detect Spammers in Twitter- A Survey,Monika Verma, Divya,Sanjeev Sofat, Ph.D Professor Department of Computer Science PEC University of Technology,

[4] Detection of Suspicious URL in Social Networking Site Twitter: Survey Paper Jyoti
D.Halwar, Sandeep Kadam , Vrushali Desale, D.Y.Patil College Of Engg.

[5] FRAppE: Detecting Malicious Facebook Applications Md Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos Dept. of Computer Science, University of California, Riverside Riverside, CA 92507 rahmanm, huangt, harsha, michalis@cs.ucr.edu

[6] S. Lee and J. Kim, "WarningBird: Detecting suspicious URLs in Twitter stream," in Proc. NDSS, 2012.

[7] Antoniades, I. Polakis, G. Kontaxis, E. Athanasopoulos, S. Ioannidis, E. P. Markatos, and T. Karagiannis, "we.b: The web of short URLs," in Proc. WWW, 2011.

[8] Klien and M. Strohmaier, "Short links under attack: geographical analysis of spam in a URL shortener network," in Proc. ACM HT, 2012.

[9] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbotnetwork: when bots socialize for fame and money," in Proceedings of the 27th Annual Computer Security Applications Conference. ACM,2011, pp. 93–102.

[10] C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. ACM transactions on Intelligent Systems and Technology, 2, 2011.

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