ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Detecting Compromised Accounts in Online Social Networks by Analysing Social Behavior

Mursidha Nasreen[1], Jaseela Jasmin TK[2]

M.Tech. Student, Dept. of CSE, Cochin College of Engineering, Valanchery, Malappuram, Kerala, India[1]

Asst. Professor, Dept. of CSE, Cochin College of Engineering, Valanchery, Malappuram, Kerala, India[2]

ABSTRACT: Account Compromization is a serious threat to users of online social networks. Relentless spammers exploit the established trust relationships between account owners and their friends. To better serve users various social communication needs, OSNs provideagreatvarietyofonlinefeaturesfortheiruserstoengagein,suchasbuilding connections, sending messages, uploading photos, browsing friends latest updates, etc. Validate the system by collecting and analyzing the social behavior. Based on this social behavior the system checks the account is compromised or not. We study the social behaviors of OSN users, i.e., their usage of OSN services, and the application of which in detecting the compromised accounts.

KEYWORDS: Online Social Behavior, Privacy, Data analysis, Compromised account detection

I. INTRODUCTION

Compromised accounts in Online Social Networks (OSNs) are more favourable than sybil accounts to spammers and other malicious OSN attackers. Malicious parties exploit well established connections and trust relationships between the legitimate account owners and their friends, and efficiently distribute spam ads, phishing links, or malware, while avoiding being blocked by the service providers. Offline analyses of tweets and Facebook posts reveal that most spam are distributed via compromised accounts, instead of dedicated spam accounts. Recent large-scale account hacking incidents in popular OSNs further evidence this trend. Unlike dedicated spam or sybil accounts, which are created solely to serve malicious purposes, compromised accounts are originally possessed by benign users, While dedicated malicious accounts can be simply banned or removed upon detection, compromised accounts cannot be handled likewise due to potential negative impact to normal user experience (e.g., those accounts may still be actively used by their legitimate benign owners). Major OSNs today employ IP geolocation logging to battle against account compromization. However, this approach is known to suffer from low detection granularity and high false positive rate. Previous research on spamming account detection mostly cannot distinguish compromised accounts from sybil accounts, with only one recent study by Egeleet al[1]. features compromised accounts detection.

OSNs provide a great variety of online features for their users to engage in, such asbuildingconnections,sendingmessages,uploadingphotos,browsingfriend'slatest updates, etc. We first conduct a study on online user social behavior of comments bycollecting and analysing user comments of wellknown OSN website. The comments of every individual user is different. It may be positive comments or negative comments. Thenegativecommentscontainsmanyspamwords,theseshorttextspam words are listed. The list of short text spam words are stored in database. Here we using the MySQL database as server. To detect the compromised accounts, using collaborative filtering algorithm. Filtering the spam words from the social activity commenting by comparison with the database. In this paper results show the social behavioral profiles can accurately differentiate individual OSN users and detect compromised accounts.

II. RELATED WORK

The core idea underlying our approach is that it is possible to model the regular activities of individual users. If, at any point, a user account gets compromised, it is likely that there will be a noticeable change in the accounts

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

behaviours. Online social networks, such as Facebook and Twitter, have become increasingly popular over the last few years. People use social networks to stay in touch with family, chat with friends, and share news. The users of a social network build, over time, connection switch their friends, colleagues, and, in general, people they consider interesting or trust worthy. Typically, users receive messages published by the users they are connected to, in the form of wall posts, tweets, or status updates.

In our system, filter the compromised accounts from all user accounts by the basis of social behavior of social activity comment. Every OSNs has an area for writing comments. The users can upload their images and photos. The users are try to upload better photos and images. A and B are two authorized users, both are friends by accepting friend request. A and B can view all data of each other, i.e. personal information, shares, uploads etc. When user A upload an image, the user B can find it and can write comment about that image. Normally the user B will write the good comments. In some cases bad comments will present, that may be by an unauthorized user. In proposed system, we construct a model of OSNs with all social activities. Users and admin has a login id and password for the security purpose. Here we using the MySQL database as server. To detect the compromised accounts there are mainly two steps, measurement study and differentiating users.

III. MEASUREMENT STUDY

We conduct a measurement study of Facebook users to understand their online social behaviors. In order to observe the social activity commenting. And the database contains the comments may be positive or negative based on the contents of shares. From negative comments the short text spam words are collected and stored in the database. To detect the compromised accounts, want to differentiate the users. Using the content based collaborative filtration algorithm. And list of compromised accounts are displays in server module.

IV. EXPERIMENTAL RESULTS

Here the spam words are filtered from user comments. First analyse the user comments, then the comment split to word by word. Each words are compared with the short text spam words which set by admin. If there is matching occur, then the account considered as compromised accounts. Figure 1 shows example of list of compromised accounts. The list contains all details about the account user and the list viewed by admin.

ALL SPAM ACCOUNT USERS

User Image	User name	Account Type	Command	View Reason
	Aravind	Spam Account	bad image and i hate	Using Spam Word and Maleware Document
	Psalmgajey	Spam Account	i hate this	Using Spam Word and Maleware Document

Fig1. Example of list of compromised account users

V. CONCLUSION

We proposed an approach to detect the compromised accounts in operating system networks. Our method identifies the spam words present in the comment of individual OS Nusers by using the content based collaborative filtering algorithm. Hereweused adatabasetostorethesocialactivitiesofusers. Basedonthefilteringofspamwords, admin is able to distinguish the account user is authorized or not.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

REFERENCES

[1] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "COMPA: Detecting compromised accounts on social networks," in Proc. Symp. Netw. Distrib. Syst. Secur. (NDSS), San Diego, CA, USA, 2013.
[2] Y. Bachrach, M. Kosinski, T. Graepel, P. Kohli, and D. Stillwell. Personality and patterns of facebook usage. In Proceedings of the3rd Annual ACM Web Science Conference, WebSci 12, pages 2432, Evanston, Illinois, USA, 2012. ACM
[3] F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida .Characterizing user behavior in online social networks. In Proceedings of the 9th ACMSIGCOMMconferenceonInternetmeasurementconference,IMC09,pages4962, Chicago, Illinois, USA, 2009. ACM.
[4] Q. Cao, M. Sirivianos, X. Yang and T. Pregueiro, Aiding the detection of fake accounts in large scale social online service. In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, NSDI12, San Jose, CA, USA, 2012. USENIX Association.
[5] M. Egele, G. Stringhini, C. Kruegel and G. Vigna. Compa: Detecting compromised accounts on social networks. In Symposium on Netowrk and Distributed System Security, NDSS 13, San Diego, CA USA. Internet Society.
[6] H. Gao, Y. Chen and K. Lee, . Towards online spam filtering in social networks. In Symposium on Netowrk and Distributed System Security, NDSS 12, San Diego, CA USA.Internet Society.
[7] XinRuan,ZhenyuWu,HainingWangandSushilJajodia,Profiling Online SocialBehaviorsforCompromisedAccountDetection.In IEEETransactions on Information Forensics and Security, pp. 176 - 187.
[8] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen and B. Y. Zhao, Detecting and characterizing social spam campaigns, in Proc. 10th ACM SIGCOMM Conf. Internet Meas. (IMC), Melbourne, VIC, Australia, 2010, pp. 3547.
[9] K.-I.GohandA.-L.Barabsi, Burstiness and memory in complex systems, in Europhys. Lett., 81, no. 4, p. 48002, 2008.
[10] K. Lee, J. Caverlee and S. Webb, Uncovering social spammers: Social honeypots+machine learning, in Proc. 33rd Int. ACM SIGIR Conf. Res. Develop. Inf. Retr. (SIGIR), Geneva, Switzerland, 2010, pp. 435442.
[11] C.Ross,E.S.Orr,M.Sisic,J.M.Arseneault,M.G.Simmering and R.R. Orr, Personality and motivations associated with Facebook use, in Comput. Human Behavior, vol. 25, no. 2, pp. 578586, 2009.