Journal of Engineering Sciences
Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

PRO GUARD DETECTING MALICIOUS ACCOUNTS IN SOCIAL-NETWORK-BASED ONLINE PROMOTIONS

[1]V. SAI KRISHNA, [2]G. PRASAD
[1]MCA Student, [2]Assistant Professor
DEPARTMENT OF MCA
SREE CHAITANYA COLLEGE OF ENGINEERING, KARIMNAGAR

Abstract : Online social networks (OSNs) usage as been increased widely and also coordinate money related abilities by empowering the utilization of genuine and virtual cash. They fill in as new stages to have an assortment of business exercises, for example, online promotion event, where clients can get virtual cash as prizes by taking an interest in such occasions. Both OSNs and business accomplices are essentially concerned when aggressors instrument an arrangement of records to gather virtual cash from these occasions, which make these occasions insufficient and result in noteworthy money related misfortune. It happens to extraordinary significance to proactively recognizing these noxious records previously the online advancement exercises and consequently diminishes their need to be remunerated. In this paper, we propose a novel framework, in particular ProGuard, to achieve this target by efficiently incorporating highlights that describe accounts from three points of view including their general practices, their reviving examples, and the use of their money. Experimental results have demonstrated that our system can accomplish a high detection rate of 96.67% at a very low false positive rate of 0.3%.

Keywords: Online social networks, virtual currency, malicious accounts, intrusion detection, network security.

I. INTRODUCTION

Online social networks (OSNs) that integrate virtual currency serve as an appealing platform for various business activities, where online, interactive promotion is among the most active ones. Specifically, a user, who is commonly represented by her OSN account, can possibly get reward in the form of virtual currency by participating online promotion activities organized by business entities. She can then use such reward in various ways such as online shopping, transferring it to others, and even exchanging it for real currency [1]. Such virtual currency-enabled online promotion model enables enormous outreach, offers direct financial stimuli to end users, and meanwhile minimizes the interactions between business entities and financial institutions. As a result, this model has shown great promise and gained huge prevalence rapidly. However, it faces a significant threat: attackers can control a large number of accounts, either by registering new accounts or compromising existing accounts, to participate in the online promotion events for virtual currency. Such malicious activities will fundamentally undermine the effectiveness of the promotion activities, immediately voiding the effectiveness of the promotion investment from business entities and meanwhile damaging ONSs' reputation. Moreover, a large volume of virtual currency, when controlled by attackers, could also become a potential challenge against virtual currency regulation [2].

It therefore becomes of essential importance to detect accounts controlled by attackers in online promotion activities. In the following discussions, we refer to such accounts as malicious accounts. The effective detection of malicious accounts enables both OSNs and business entities to take mitigation actions such as banning these accounts or decreasing the possibility to reward these accounts. However, designing an effective detection method is faced with a few significant challenges. First, attackers do not need to generate malicious content (e.g., phishing

URLs and malicious executables) to launch successful attacks. Comparatively, attackers can effectively perform attacks by simply clicking links offered by business entities or sharing the benign content that is originally distributed by business partners. These actions themselves do not perceivably differentiate from benign accounts. Second, successful attacks do not need to depend on social structures (e.g., ''following'' or ''friend'' relationship in popular social networks). To be more specific, maintaining active social structures does not benefit to attackers, which is fundamentally different from popular attacks such as spammers in online social networks. These two challenges make the detection of such malicious OSN accounts fundamentally different from the detection of traditional attacks such as spamming and phishing. As a consequence, it is extremely hard to adopt existing methods to detect spamming and phishing accounts.

In order to effectively detect malicious accounts in online promotion activities by overcoming the aforementioned challenges, we have designed a novel system, namely ProGuard. ProGuard employs a collection of behavioral features to profile an account that participates in an online promotion event. These features aim to characterize an account from three aspects including i) its general usage profile, ii) how an account collects virtual currency, and iii) how the virtual currency is spent. ProGuard further integrates these features using a statistical classifier so that they can be collectively used to discriminate between those accounts controlled by attackers and benign ones. To the best of our knowledge, this work represents the first effort to systematically detect malicious accounts used for online promotion activity participation.

II. RELATED WORK

Since online social networks play an increasing important role in both cyber and business world, detecting malicious users in OSNs becomes of great importance. Many detection methods have been consequently proposed [3]–[10]. Considering the popularity of spammers in OSNs, these methods almost exclusively focus on detecting accounts that send malicious content. A spamming attack can be considered as an information flow initiated from an attacker, through a series of malicious accounts, and finally to a victim account.

Despite the diversity of these methods, they generally leverage partial or all of three sources for detection including i) the content of the spam message, ii) the network infrastructure that hosts the malicious information (e.g., phishing content or exploits), and iii) the social structure among malicious accounts and victim accounts. For example, Gao et al. [11] designed a method to reveal campaigns of malicious accounts by clustering accounts that send messages with similar content. Lee and Kim [12] devised a method to first track HTTP redirection chains initiated from URLs embedded in an OSN message, then grouped messages that led to webpages hosted in the same server, and finally used the server reputation to identify malicious accounts. Yang et al. [13] extracted a graph from the ''following'' relationship of twitter accounts and then propagated maliciousness score using the derived graph; Wu et al. [9] proposed a social spammer and spam message co-detection method based on the posting relations between users and messages, and utilized the relationship among user and message to improve the performance of both social spammer detection.

Compared to existing methods on detecting spamming accounts in OSNs, it is faced with new challenges to detect malicious accounts that participate in online promotion activities. First, different from spamming accounts, these accounts neither rely on spamming messages nor need malicious network infrastructures to launch attacks. Second, social structures are not necessary. Therefore, none of existing methods is applicable to detecting malicious accounts in online promotion activities. To solve the new challenges, our method detects malicious accounts by investigating both regular activities of an account and its financial activities.

III. SYSTEM MODEL

Our objective is to design a detection system capable of identifying malicious accounts that participate in

online promotion events for virtual currency collection (at the collection phase) before rewards are committed.

Detecting malicious accounts at this specific time point (i.e., before the commitment of rewards and at the

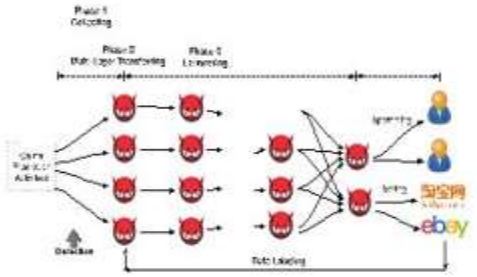


Figure .1. Virtual currency flow for malicious OSN accounts.

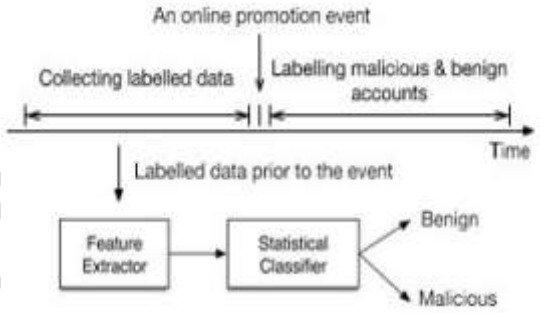
collection phase) results in unique advantages. First, as a simple heuristic to prevent freshly registered accounts that are likely to be bots, business entities usually require the participating accounts to be registered for a certain amount of time (e.g., a few weeks). Therefore, the detected and mitigated malicious accounts cannot be immediately replaced by the newly registered accounts, thereby drastically limiting attackers' capabilities. In contrast, no constraint is applied for accounts used for virtual currency transferring and laundering. This implies such accounts can be easily replaced by attackers if detected, resulting negligible impact to attackers' capabilities. Second, our detection system will label whether an account is malicious when it participates in an online promotion event; this enables business entities to make actionable decisions such as de-prioritize this account from being rewarded in this event. Therefore, it can proactively mitigate the financial loss faced by business entities.

PROPOSED SYSTEM

- ❖ In the proposed system, the system proposes a novel system, namely ProGuard, to accomplish this objective by systematically integrating features that characterize accounts from three perspectives including their general behaviors, their recharging patterns, and the usage of their currency.
- ❖ The system has performed extensive experiments based on data collected from the Tencent QQ, a global leading OSN with built-in financial management activities.

SYSTEM ARCHITECTURE

Figure 2 presents the temporal relationship among the data collection process, online promotion events, and the account labeling process. Therefore, it is worth noting that an account may not have any historical financial activities (even for virtual currency collection activities) since it participates in the online promotion for the first time.



The architectural overview of the system

Although the aforementioned ''trace-back'' method is effective in manually labeling malicious accounts, using it as a detection method is impractical. First, it requires a tremendous amount of manual efforts for forensic analysis such as identifying suspicious virtual-currency dealers in external e-commerce websites, correlating spamming content with user accounts, and correlating sellers' profiles with user accounts. In addition, evidence for such forensic analysis will be only available after malicious accounts participate in online promotion events. Therefore, this data labeling process, if used as detection method, cannot guide business entities to mitigate their financial loss proactively. In contrast, our method is designed to detect malicious accounts prior to the reward commitment. For each account, we collect a variety of information including 1) login activities, 2) a list of anonymized accounts that this account has sent instant messages to, 3) service purchase activities, 4) the recharging activities, and

5) the expenditure activities. ProGuard is composed of two phases, namely the training phase and the detection phase. In the training phase, a statistical classifier is learnt from a set of prelabelled malicious and benign accounts. In the detection phase, an unknown account will first be converted to a feature vector and then analyzed by the statistical classifier to assess its maliciousness. The bottom of Figure 3 presents the architectural overview of ProGuard. As a variety of statistical classifiers have been developed and widely used, designing features capable of discriminating between malicious accounts and benign accounts becomes of central focus. In this section, we will introduce various features and demonstrate their effectiveness on differentiating malicious accounts from benign ones. We propose three general guidelines to steer the feature design.

General Behaviors: Benign accounts are usually used by regular users for variety of activities such as chatting, photo sharing, and financial activities. In contrast, malicious accounts are more likely to be driven by online promotion events. Therefore, the benign accounts tend to be more socially active compared to malicious accounts.

Currency Collection: The malicious accounts under investigation focus on using online promotion activities to collect virtual currency. In contrast, benign users are likely to obtain virtual currency from multiple resources.

Currency Usage: Attackers' ultimate objective is to monetize the virtual currency. In contrast, benign users use their virtual currency in much more diversified ways.

IV. IMPLEMENTATION

Bank Admin

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as View all users and authorize, View all Sellers and authorize, Set Limit Access and view, View all malicious users Based on Product Purchase(user tries to purchase with no balance) and block if they to do same thing more than the access limit,View all malicious users Based on Amount Transfer(user tries to transfer to another user with no balance) and block if they to do same thing more than the access limit, List all Malicious seller with Malware details and mention this account holder as Spam account and block this user, view user and seller un block request and un block, View No.of Malicious Users and Normal Users in chart, View product rank in chart

User

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like --- Register with Location and Login and Request to un block if u blocked View your profiles with Account Type(Malicious or Normal, Create Bank Account, View Account, View Mini Statement, Search Friends and Find Friends, Give Authorization, View Your Friends, Search Products by content keyword and view the details, purchase the product, Transfer the amount to your friend.

Seller

In this module, there are n numbers of users are present. Seller should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like View Profile with account type, Add Product with pcat,pname, manufacturer, pdesc with browse file,filename, pprice,puses,pimage

, View all products with rank and ratings, View all purchased users with total Bill and malicious users(user tries to purchase with no balance)

V. CONCLUSION

Extensive amount of uses of online social networks, the privacy and security issues will occur. To solve this issue this paper brings an approach as ProGuard

Technique. The designing and implementation of this technique can identify accurately and efficiently fake accounts.Many times it is difficult to recognize the original post in facebook groups because more number of persons are sharing the posts daily for the transmission. To discriminate the legal and spam posts proposed technique is used. Functioning of this commencement is committed by receiving the outcomes utilizing this mechanism and this mechanism successfully detects the fake accounts.

REFERENCES

[1] Y. Wang and S. D. Mainwaring, ``Human-currency interaction: Learning from virtual currency use in China," in Proc. SIGCHI Conf. HumanFactors Comput. Syst., 2008, pp. 25_28. [2] J. S. Gans and H. Halaburda, ``Some economics of private digi-tal currency," Rotman School Manage., Toronto, ON, Canada, Tech.Rep. 2297296, 2013.

[3] X. Hu, J. Tang, and H. Liu, ``Online social spammer detection," in Proc.28th AAAI Conf. Artif. Intell., 2014, pp. 59_65.

[4] X. Hu, J. Tang, and H. Liu, ``Leveraging knowledge across media forspammer detection in microblogging," in Proc. 37th Int. ACM SIGIR Conf.Res. Develop. Inf. Retr., 2014, pp. 547_556.

[5] Z. Chu, S. Gianvecchio, H.Wang, and S. Jajodia, ``Detecting automation oftwitter accounts: Are you a human, Bot, or cyborg?" IEEE Trans. Depend.Sec. Comput., vol. 9, no. 6, pp. 811_824, Nov. 2012.

6] Z. Chu, S. Gianvecchio, A. Koehl, H. Wang, and S. Jajodia, ``Blog orblock: Detecting blog bots through behavioral biometrics," Comput. Netw.,vol. 57, no. 3, pp. 634_646, 2013.

[7] S. Fakhraei, J. Foulds, M. Shashanka, and L. Getoor, ``Collective spammerdetection in evolving multirelational social networks," in Proc. 21th ACMSIGKDD Int. Conf. Knowl. Discovery Data Mining, 2015, pp. 1769_1778.

[8] Y.-R. Chen and H.-H. Chen, ``Opinion spammer detection inWeb forum,"in Proc. 38th Int. ACM SIGIR Conf. Res. Develop. Inf. Retr., 2015, pp. 759_762.1998.

[9] F.Wu, J. Shu, Y. Huang, and Z. Yuan, ``Social spammer and spam message co-detection in microblogging with social context regularization," in Proc.24th ACM Int. Conf. Inf. Knowl. Manag., 2015, pp. 1601_1610.

[10] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, ``Twit-ter spammer detection using data stream clustering," Inf. Sci., vol. 260,pp. 64_73, Sep. 2014.

[11] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, ``Detecting andcharacterizing social spam campaigns," in Proc. 10th ACM SIGCOMMConf. Internet Meas., 2010, pp. 35_47.