Analyzing And Detecting Money-Laundering Accounts In Online Social Networks

Kankatala Sri Manikanteswari, Sri.S.K.Alisha, Sri.V.Bhaskara Murthy
Mca Student, Senior Assistant Professor, Associate Professor
Dept Of Mca
B.V.Raju College, Bhimavaram

ABSTRACT

Virtual currency in online social networks (OSN) plays an increasingly important role in supporting various financial activities such as currency exchange, online shopping, and paid games. Users usually purchase virtual currency using real currency. This fact motivates attackers to instrument an army of accounts to collect virtual currency unethically or illegally with no or very low cost and then launder the collected virtual money for massive profit. Such attacks not only introduce significant financial loss of victim users, but also harm the viability of the ecosystem. It is therefore of central importance to detect malicious OSN accounts that engage in laundering virtual currency. To this end, we extensively study the behaviors of both malicious and benign accounts based on operation data collected from Tencent QQ, one of the largest OSNs in the world. Then, we devise multi-faceted features that characterize accounts from three aspects including account viability, transaction sequences, and spatial correlation among accounts. Finally, we propose a detection method by integrating these features using a statistical classifier, which can achieve a high detection rate of 94.2% at a very low false positive rate of 0.97%.

I. INTRODUCTION

Online social networks (OSNs) have started to leverage virtual currency as an effective means to glue financial activities across various platforms such as online shopping, paid online games, and paid online reading. Examples of virtual currency in such OSNs include but are not limited to Tencent Q Coin, Facebook Credits1, and Amazon Coin. Usually, users purchase virtual money using real currency at a regulated rate; a user can also transfer it to another via various ways such as recharging her account and sending out gifts [1]. These facts enable attackers to gain potentially massive profits through the following steps. First, an attacker can collect virtual currency with zero or low cost. For example, she can compromise and subsequently control a legitimate account or register a huge number of accounts to win gifts (in the form of virtual currency) in online promotion activities. Next, she can instrument accounts under her control to transfer virtual currency to other accounts in return for real currency, with rates that are usually much lower compared to the regulated rate. Attackers usually post advertisements in popular e-commerce websites [2] to attract potential buyers. We term OSN accounts that are used by attackers for the collection and transfer of virtual currency as money-laundering accounts. Money-laundering accounts have caused a tremendous financial loss for compromised accounts, fundamentally undermined the effectiveness of online promotion activities, and possibly introduced potential conflicts against currency regulations. Detecting money-laundering accounts in OSNs therefore becomes of essential importance, which, however, is faced with new, significant

challenges. First, committing money-laundering activities does not require the usage of traditional malicious content such as spam, malicious URLs, or malicious executables. Although spamming might be used by attackers for advertisement, neither methods nor the accounts used for spamming are necessarily associated with the money-laundering accounts. Second, money-laundering activities do not rely on social behaviors and structures (e.g., "following" or "friend" relationship in popular social networks) to operate. These challenges make existing methods immediately ineffective, since they focus on detecting OSN-based spamming, phishing, and scamming attacks, whose proper operation necessitates malicious content [3, 4], social structures [5], or social behaviors [6]. Detecting money laundering activities in traditional financial transactions has attracted significant research efforts [7]. For example,

Dreżewski et al. [8] designed a system to detect money laundering activities from billings and bank account transactions.

Paula et al. [9] used the AutoEncoder to classify exporters and detect money laundering activities in exports of goods and products in Brazil. Colladon et al. [10] presented predictive models to quantify risk factors of clients involved in the factoring business and proposed a visual analysis method to detect the potential clusters of criminals and prevent money laundering. Different from traditional money laundering detection problems in bank-related activities, account behaviors of laundering virtual currency in OSNs involve bank-related financial activities, online social network, and virtual recharging and expenditure activities.

The goal of our work is to design an effective method capable of detecting money-laundering accounts. As a means towards this end, we perform an extensive study of behaviors of money-laundering accounts based on data collected from Tencent QQ, one of the largest OSNs in the world with a giant body of reportedly 861 million active users. We have devised multi-faceted features that characterize accounts from three aspects including account viability, transaction sequences, and spatial correlation among accounts. Experimental results have demonstrated that our method can achieve a high detection rate of 94.2% with a very low false positive rate of 0.97%. To the best of our knowledge, this work represents the first effort to analyze and detect money-laundering accounts in OSNs integrating virtual currency at this large scale.

II. EXISTING SYSTEM

- In the existing system, an approach to sort and map relational data and present predictive models – based on network metrics – to assess risk profiles of clients involved in the factoring business. The system finds that risk profiles can be predicted by using social network metrics.

- In the system dataset, the most dangerous social actors deal with bigger or more frequent financial operations; they are more peripheral in the transactions network; they mediate transactions across different economic sectors and operate in riskier countries or Italian regions.

- Finally, to spot potential clusters of criminals, we propose a visual analysis of the tacit links existing among different companies who share the same owner or representative. The system findings show the importance of using a network-based approach when looking for suspicious financial operations and potential criminals.

Disadvantages

- It is not based on Behavior Analysis and Feature Extraction.
- There is no Vitality Features to detect malicious attackers.

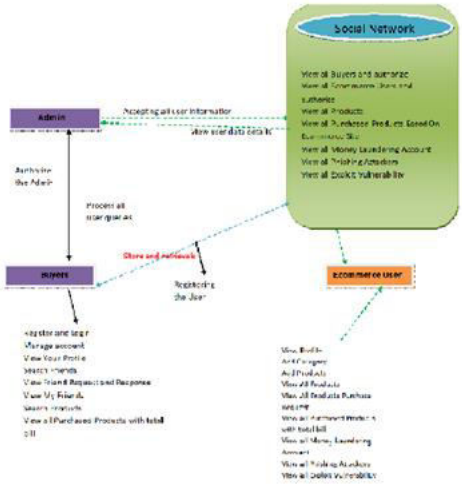
III. PROPOSED SYSTEM

- The proposed system is designed which is an effective method capable of detecting money-laundering accounts. As a means towards this end, we perform an extensive study of behaviors of money-laundering accounts based on data collected from Tencent QQ, one of the largest OSNs in the world with a giant body of reportedly 861 million active users.
- The system has devised multi-faceted features that characterize accounts from three aspects including account viability, transaction sequences, and spatial correlation among accounts.
- Experimental results have demonstrated that our method can achieve a high detection rate of 94.2% with a very low false positive rate of 0.97%. To the best of our knowledge, this work represents the first effort to analyze and detect money-laundering accounts in OSNs integrating virtual currency at this large scale.

Advantages

- Login activities, which include the account ID, the login date, the login IP address, and the account level.
- The expenditure activities, which include the expenditure account ID, the expenditure date, the expenditure amount, the purchased service, the payment way, and the account ID to receive the service.
- The recharging activities, which include the recharging account ID, the recharging date, the recharging amount, the payment way.

IV. ARCHITECTURE DIAGRAM



V. MODULES

Social Network

In this module, the Social Network has to login by using valid user name and password. After login successful he can do some operations such as

View all Buyers and authorize,
View all Ecommerce Users and authorize,
View all Products,
View all Purchased Products Based On Ecommerce Site,
View all Money Laundering Account,
View all Phishing Attackers,
View all Exploit Vulnerability

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Ecommerce User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration

successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like View Profile, Add Category, Add Products, View All Products, View All Products Purchase Request, View all Purchased Products with total bill, View all Money Laundering Account, View all Phishing Attackers, View all Exploit Vulnerability.

Buyers

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like Manage account,View Your Profile,Search Friends ,View Friend Request and Response,View My Friends,Search Products ,View all Purchased Products with total bill.

VI. CONCLUSION

This article presents the analysis and detection method of money-laundering accounts in OSNs. We analyzed and compared the behaviors of both malicious and benign accounts from three perspectives including 1) the account viability, 2) the transaction sequences, and 3) spatial correlation among accounts. We designed a collection of 54 features to systematically characterize the behaviors of benign accounts and malicious accounts. Experimental results based on labeled data collected from Tencent QQ, a global leading OSN, demonstrated that the proposed method achieved high detection rates and very low false positive rates.

REFERENCE

[1] Y. Wang and S. D. Mainwaring, “Human-currency interaction: learning from virtual currency use in China,” in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2008, pp. 25–28.

[2] Y. Zhou, D. Kim, J. Zhang, et al., “ProGuard: Detecting Malicious Accounts in Social-Network-Based Online Promotions,” IEEE Access, vol. 5, 2017, pp. 1990-1999.

[3] F. Wu, J. Shu, Y. Huang, and Z. Yuan, “Social spammer and spam message co-detection in microblogging with social context regularization,” in Proceedings of the 24th ACM International on Conference on Information and Knowledge Management. ACM, 2015, pp. 1601–1610.

[4] L. Wu, X. Hu, F. Morstatter, et al., “Adaptive Spammer Detection with Sparse Group Modeling,” in Proceedings of the 11th International AAAI Conference on Web and Social Media. AAAI, 2017, pp. 319-326.

[5] S. Fakhraei, J. Foulds, M. Shashanka, and L. Getoor, “Collective spammer detection in evolving multi-relational social networks,” in Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2015, pp. 1769–1778.

[6] F. Hao, X. Xing, R. Yong, et al., “Robust Spammer Detection in Microblogs: Leveraging User Carefulness,” ACM Transactions on Intelligent Systems and Technology, vol. 8, no. 6, 2017, pp. 83:1-83:31.

[7] G. K. Palshikar, “Detecting Frauds and Money Laundering: A Tutorial,” in Proceedings of the International Conference on Big Data Analytics. Springer, 2014, pp. 145-160.

[8] R. Dreżewski, J. Sepielak and W. Filipkowski, “The application of social network analysis algorithms in a system supporting money laundering detection,” Information Sciences, vol. 295, 2015, pp. 18-32.

[9] E. L. Paula, M. Ladeira, R. N. Carvalho and T. Marzagão, “Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering,” 2016 15th IEEE International Conference on

Machine Learning and Applications (ICMLA), Anaheim, CA, 2016, pp. 954-960.
10] A. F. Colladon and E. Remondi, "Using social network analysis to prevent money laundering," Expert Systems with Applications, vol. 67, 2017, pp. 49-58.
[11] J. Pei, J. Han, B. Mortazavi-Asl, et al., "Mining sequential patterns by pattern-growth: The prefixspan approach", IEEE Transactions on knowledge and data engineering, vol. 16, no. 11, 2004, pp. 1424-1440. [12] M. E. J. Newman, "Communities, modules and large-scale structure in networks ," Nature Physics , vol. 8, no. 1, 2012, pp. 25-31.
[13] R. Li, L. Qin, J. X. Yu, et al., "Finding influential communities in massive networks," The VLDB Journal, 2017.
[14] S. Rogers, M. Girolami, A first course in machine learning. CRC Press, 2016. [15] J. Han, M. Kamber, and J. Pei, Data mining: concepts and techniques. Elsevier, 2011.
[15] J. Han, M. Kamber, and J. Pei, Data mining: concepts and techniques. Elsevier, 2011.