International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 10 | Oct 2020 www.irjet.net p-ISSN: 2395-0072

Evaluating and Finding Out the Money Laundering Accounts in Online Social Networks

Shaik Shajahan[1], C.H. Phani Krishna[2], P. Jyothi[3]

[1]*M. Tech, Student, Department of CS&E, Teegala Krishna Reddy Engineering College, Hyderabad, India*
[2]*Head of Department, Department of CS&E, Teegala Krishna Reddy Engineering College, Hyderabad, India*

Abstract - *Virtual money shows a most important role in supporting various economic actions on online social network for example currency exchange, online shopping and paid games. Users usually buy virtual currency with real currency. This motivates the attackers to instrument an army of accounts to gather virtual currency in an unethical or illegal way with less low cost and then recycle the virtual money collected for huge profits. Such attacks not only entail significant financial losses for victims' users, but also damage the ecosystem's profitability. Therefore, it's about crucial to find out malicious OSN accounts dedicated to virtual currency laundering. To this end, we broadly study the behaviour of malicious and benign accounts based on operational data collected by Tencent, one of the huge OSNs in the world. Thus, we design multi-faceted features that can be representing the report from ternary aspects, including account profitability, transaction sequences and spatial correlation between accounts. Finally, we propose a detection method integrating these features using a statistical classifier, which can reach a large detection rate of 94.2% at a very low false positive rate of 0.97%.*

Key Words: Money Laundering, Social Network, Ecommerce, Vulnerability, Random Forest Algorithm.

1. INTRODUCTION

Online social networks (OSNs) have begun to exploit virtual currency as an effective means of pasting financial assets on various platforms, such as online shopping, paid online games and paid online reading. Examples of virtual currency in such OSNs include, among others, Tencent Q Coin, Facebook Credits1 and Amazon Coin. Typically, users buy virtual money using real currency at a regulated rate; a user can also transfer it to another in several ways, such as topping up their account and sending gifts. These facts allow attackers to obtain potentially huge gains through the following steps. First, an attacker can collect virtual currency at zero or low cost. For example, you can commit and then verify a legitimate account or register a large number of accounts to win gifts (in the form of virtual currency) in online promotional activities. Subsequently, you can implement the accounts under your control to transfer the virtual currency to other accounts in exchange for the real currency, with rates that are generally much lower than the regulated rate. Attackers usually advertise on popular e-commerce websites to attract potential buyers. We define the OSN accounts that attackers use to collect and transfer virtual currency as money laundering accounts. Money laundering accounts caused a huge financial loss for compromised accounts, fundamentally undermined the effectiveness of online promotional activities and possibly introduced potential conflicts against monetary regulations. The identification of accounts related to money laundering in NGOs is therefore of fundamental importance, but must face new and significant challenges. First, performing recycling activities does not require the use of traditional malicious content, such as spam, malicious URLs or malicious executable files. While perpetrators of advertising attacks cannot use spam, the methods or accounts used for spam are necessarily associated with anti-money laundering accounts. Second, money laundering activities are not based on social behaviors and structures to operate. These challenges make existing methods ineffective immediately, as they focus on detecting attacks of spam, phishing and OSN-based scams, whose proper functioning requires harmful content, social structures or social behavior.

2. LITERATURE SURVEY

Money Laundering is relatively a fresh topic from the perspective of research, at least in the Indian context. Hence, there is a scope for discovering new trends based on experiences of jurisdictions which have implemented their own anti money laundering framework. This is important both from the legislative point of view and from the perspective of financial sector in general and securities markets, in particular.

3. EXISTING SYSTEM

An approach to classify and map relational data and present predictive models, based on network metrics, to assess the risk profiles of customers involved in the factoring business. The system detects that risk profiles can be predicted using social media metrics. In the data set of the system, the most dangerous social actors deal with larger or more frequent financial transactions; they are more peripheral in the transaction network; they mediate transactions in different economic sectors and operate in riskier Italian countries or regions. Finally, to detect possible groups of criminals, we propose a visual analysis of the tacit connections between different companies that share the same owner or representative. The results of the system show the importance of using a network-based approach when looking for suspicious financial transactions and potential criminals.

4. PROPOSED SYSTEM

The proposed system is designed and is an effective method capable of detecting money laundering accounts. As a means to this end, we conducted an in-depth study of the behavior of money laundering accounts based on data collected by Tencent QQ, one of the largest NSOs in the world with a gigantic body of 861 million active users. The system has designed multi-faceted features that characterize accounts from three aspects, including account profitability, transaction sequences and spatial correlation between accounts. Experimental results have shown that our method can reach a high detection rate of 94.2% with a very low false positive rate of 0.97%. As far as we know, this work represents the first effort to analyze and detect OSN money laundering accounts that integrate the virtual currency on this large scale.

Algorithm:

First, start with the selection of random samples from a given dataset.

Next, this algorithm will construct a decision tree for every sample. Then it will get the prediction result from every decision tree.

In this step, voting will be performed for every predicted result.

At last, select the most voted prediction result as the final prediction result.

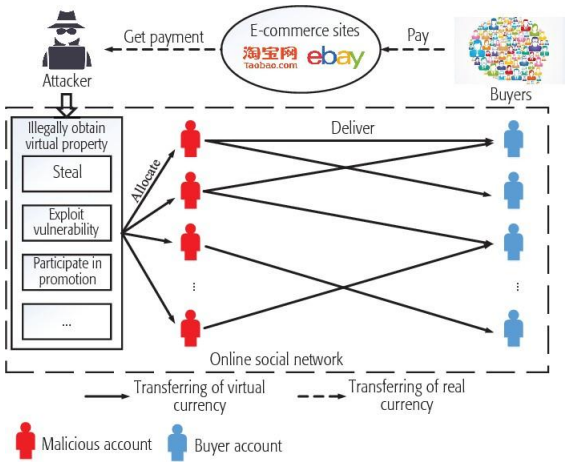

Fig -1: Architecture diagram

Data Collected from different Ecommerce Users, and these data will be stored in huge databases with high security.

User interface –User will search, view, select, and buy the item.
E-commerce interface – Register, Add product, Find Attackers.

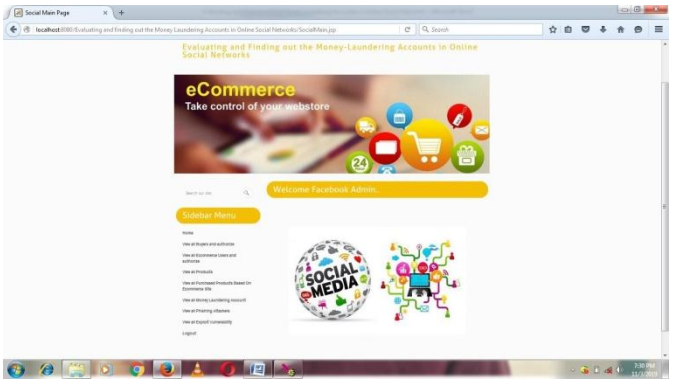

Fig -2: Social Network Page

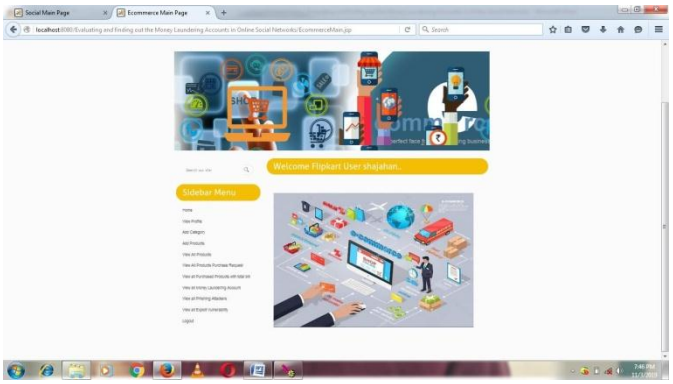

Fig -3: Ecommerce Page

Fig -4: Exploit Vulnerability Page

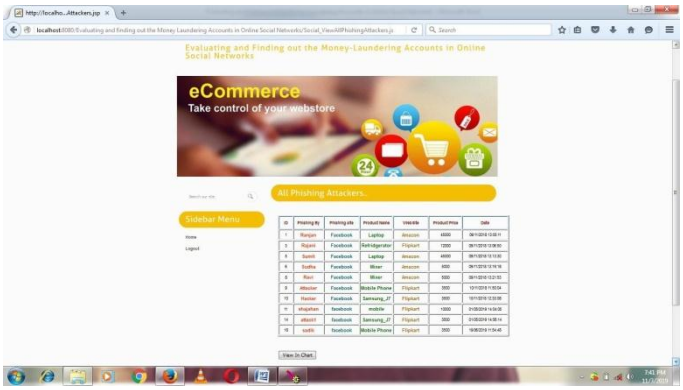

Fig -5: Phishing Attackers Page

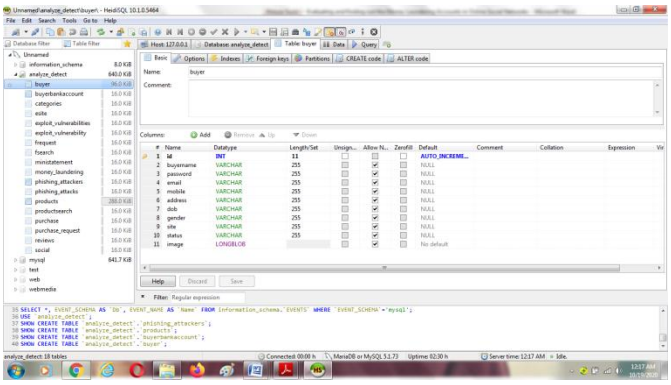

Fig -6: Database

5. FUTURE SCOPE

The system described in this document provides a basic framework for identifying recycling activity. While the results presented in this document indicate that the system can accurately identify suspicious networks, future work is expected to extend and further improve the accuracy of the systems. Future work will also consider uncontrolled approaches to the detection of new types. Future work will take into consideration the evolution of the structure of the community over time and will try to capture the relationships between the structure and the particular attributes of edge and vertex.

6. CONCLUSION

This article presents the method of analysis and detection of money laundering accounts in OSN. We analyze and compare the behavior of malicious and benign accounts from three perspectives, including 1) the profitability of the account, 2) the sequence of transactions and 3) the spatial correlation between the accounts. We have designed a collection of 54 features to systematically characterize the behavior of malicious and harmful accounts. Experimental results based on tagged data collected by Tencent QQ, a world- leading NSO, have shown that the proposed method has achieved high detection rates and very low false positive rates.

REFERENCES

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.

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.

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.

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.

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.

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.