International Journal of Research
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

Analysing and Detecting Money Laundering Accounts in Online Social Networks

V. Jyothi
Associate Professor,
Department of Computer Science and Engineering, Anurag Group of Institutions
vjyothicse@cvsr.ac.in
Kavya Reddy Kavadapu
Department of Computer Science and Engineering, Anurag Group of Institutions
kavyareddy2801@gmail.com
Sadiya Afshan
Department of Computer Science and Engineering, Anurag Group of Institutions
sadiyaafshan1998@gmail.com
Shaik Babar Basha
Department of Computer Science and Engineering, Anurag Group of Institutions
Shaikbabar7@gmail.com

Abstract

Virtual currency in OSNs 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 behaviour 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: account viability, transaction sequences, and spatial correlation among accounts.

Keywords: virtual currency, malicious account, attacker, spatial features.

1. 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 Credits, and Amazon Coin. Usually, users purchase virtual money using real currency at a regulated rate; one user can also transfer it to another user via various methods such as recharging their account and sending gifts. 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, they can compromise

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

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, they can instrument accounts under their 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 . to attract potential buyers.

We call OSN accounts that are used by attackers for the collection and transfer of virtual currency 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. The goal of our work is to design an effective method capable of detecting money-laundering accounts. As a means toward this end, we perform an extensive study of behaviours of money-laundering accounts based on data collected. We have devised multi-faceted features that characterize accounts from three aspects: account viability, transaction sequences, and spatial correlation among accounts.

Behaviour Analysis:

Figure 1 shows a typical process of virtual currency laundering. The first step is to collect virtual currency with zero or extremely low cost. For example, attackers can hack users' accounts (and thus control their virtual currency), exploit the system vulnerabilities, or participate in online promotion activities to win virtual currency for free or at significantly discounted rates [2]. Next, attackers attract potential buyers with considerable discounts, through various ways such as spreading spams and posting advertisements, and then sell the virtual currency in popular e-commerce websites such as eBay or Taobao. Once a buyer commits the purchase (i.e., paid real money to an attacker through the e-commerce

The first step is to collect virtual currency with zero or extremely low cost. For example, attackers can hack users' accounts, exploit the system vulnerabilities, or participate in online promotion activities to win virtual currency for free or at significantly discounted rates. Next, attackers attract potential buyers with considerable discounts, through various ways such as spreading spams and posting advertisements, and then sell the virtual currency in popular e-commerce websites such as eBay. Once a buyer commits the purchase, their account will receive virtual currency from one or multiple malicious accounts controlled by an attacker. Since OSNs may investigate an account if it has initiated a large number of transactions in a short period of time, an attacker usually distributes their virtual currency across multiple accounts and uses them alternatively to transfer virtual currency to buyers.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

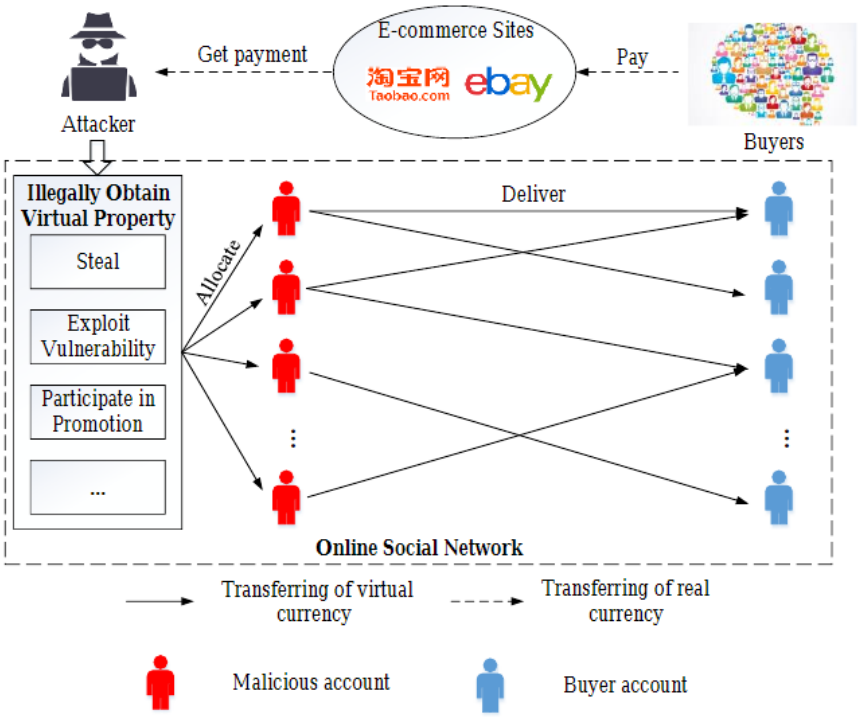

Fig 1 : Process of Virtual Currency Laundering

2. PROPOSED WORK

To keep away from the detection, attackers usually disguise the anomaly behaviors of the malicious accounts. However, some typical behavior patterns are unavoidable to achieve the goal of laundering. We can still design several effective vitality features to distinguish the malicious and benign accoun

2.1 Vitality features

To avoid detection, attackers usually disguise the anomaly behaviour of the malicious accounts. However, some typical behaviour patterns are unavoidable to achieve the goal of laundering. We can still design several effective vitality features to distinguish the malicious and benign accounts. Regular users usually actively use their OSN accounts for various daily activities such as chatting, photo sharing, and finance. In contrast, malicious accounts are mostly driven by transactions for money laundering, which are much less active compared to benign accounts.

2.2 Sequential features of financial activities

The sequences of financial activities are likely to differ between benign accounts and money-laundering accounts. In order to model the sequential behavior, we use the discrete-time Markov Chain model. Specifically, we record the sequence of three basic financial activities: virtual-currency recharge, self-expenditures, and expenditures as gifts. Each state in the Markov Chain corresponds to one activity and the transition between two states represents a pair of two consecutive financial activities. Hence, the Markov Chain has three states and

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

nine total transitions. Each transition is associated with the probability of this transition among all observed transitions.

2.3 Spatial features of currency transfer

The developed graph can effectively profile the behavior of coordinated laundering accounts. Specifically, an attacker usually distributes their virtual currency across multiple money-laundering laundering accounts to reduce the risk of being detected and subsequently banned. As a result, when a buyer purchases virtual currency from the attacker, they usually need to instrument a set of money-laundering accounts to transfer currency to the buyer's account. As this process repeats for a large number of buyers, these money-laundering accounts will share a giant set of destination accounts, forming a fully-connected graph with high weight values for edges. A group of benign accounts may also transfer virtual currency to one or a few accounts (e.g., as birthday gifts) and thus form a fully connected graph, whose edges, however, are likely to have small weights. Since an account may receive gifts from both benign accounts (e.g., friend accounts) and money-laundering accounts, edges that connect benign and money-laundering accounts will also exist.

2.4 Detection and evaluation

We leverage machine learning techniques to integrate all these features to perform effective detection. Specifically, feature values extracted from labelled malicious and benign users have been employed to train a statistical classifier. After an unknown user is represented by a vector of feature values, the classifier can automatically evaluate the maliciousness of this user. A variety of statistical classifiers could be employed in our system to perform detection.

3. CONCLUSION

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

REFERENCES

[1] Y. Wang and S. D. Mainwaring, "Human-Currency Interaction: Learning from Virtual Currency use in China," Proc. SIGCHI Conf. Human Factors in Computing Systems, ACM, 2008, pp. 25–28.

[2] Y. Zhou et al., "ProGuard: Detecting Malicious Accounts in Social-Network-Based Online Promotions," IEEE Access, vol. 5, 2017, pp. 1990–99.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 07 Issue 05
May 2020

[3] F. Wu et al., "Social Spammer and Spam Message Co-Detection in Microblogging with Social Context Regularization," Proc. 24th ACM Int'l. Conf. Information and Knowledge Management, ACM, 2015, pp. 1601–10.

[4] L. Wu et al., "Adaptive Spammer Detection with Sparse Group Modeling," Proc. 11th Int'l. AAAI Conf. Web and Social Media, AAAI, 2017, pp. 319–26.

[5] S. Fakhraei et al., "Collective Spammer Detection in Evolving Multi-Relational Social Networks," Proc. 21st ACM SIGKDD Int'l. Conf. Knowledge Discovery and Data Mining, ACM, 2015, pp. 1769–78.

[6] F. Hao et al., "Robust Spammer Detection in Microblogs: Leveraging User Carefulness," ACM Trans. Intelligent Systems and Technology, vol. 8, no. 6, 2017, pp. 83:1–31.

[7] G. K. Palshikar, "Detecting Frauds and Money Laundering: A Tutorial," Proc. Int'l. Conf. Big Data Analytics, Springer, 2014, pp. 145–60.

[8] R. Dreewski, 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 et al., "Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering," 2016 15th IEEE Int'l. Conf. Machine Learning and Applications (ICMLA), Anaheim, CA, 2016, pp. 954–60.

[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 et al., "Mining Sequential Patterns by Pattern-Growth: The PrefixSpan Approach," IEEE Trans. Knowledge and Data Engineering, vol. 16, no. 11, 2004, pp. 1424–40.

[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 et al., "Finding Influential Communities in Massive Networks," The VLDB Journal, 2017.

[14] S. Rogers, and 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.