Journal of Peace, Development and Communication

PEACE AND DEVELOPMENT

Volume 08, Issue 02, April-June 2024
pISSN: 2663-7898, eISSN: 2663-7901
Article DOI: https://doi.org/10.36968/JPDC-V08-I02-21
Homepage: https://pdfpk.net/pdf/
Email: se.jpdc@pdfpk.net

Article:	**A Review of COMPA Systems for Detection of Compromised Accounts on Social Media Networks**
Author(s):	Ahmed Faraz Senior Assistant Professor, Department of Computer Engineering, School of Engineering and Applied Sciences, Bahria University Karachi Campus
Published:	23rd June 2024
Publisher Information:	Journal of Peace, Development and Communication (JPDC)
To Cite this Article:	Faraz, A. (2024). A Review of COMPA Systems for Detection of Compromised Accounts on Social Media Networks. *Journal of Peace, Development and Communication*, *08*(02), 279-285. https://doi.org/10.36968/JPDC-V08-I02-21
Author(s) Note:	Ahmed Faraz is servig as a Senior Assistant Professor at Department of Computer Engineering, School of Engineering and Applied Sciences, Bahria University Karachi Campus Email: ahmed.faraz2004@gmail.com, ahmedfaraz.bukc@bahria.edu.pk

ABSTRACT

The high profile social media networks are vulnerable and require more security measures and systems to prevent financial losses to the industries and high level businesses because of the involvement and compromise of digital systems and cellular devices interconnecting the users to the social media networks. In this research paper, we review the COMPA system which efficiently detects the compromised high profile social media accounts in order to prevent the infiltration of cyber criminals into high profile social media networks.

Key Words: High Profile Social Media Networks, Malware, Phishing Attacks, Compromised Accounts

1. Introduction

Since nowadays social media networks and websites have changed the way of communication between people and the rest of the world. People have become closer and closer by using social media networks and websites like Facebook, Twitter etc. People have become very used to with the use of social media websites as studied by (Egele et al., 2013, p. 85). Those people who work in offices usually start their day by logging on into the Facebook and they check their messages sent by their relatives, friends and their coworkers. Or it is a common practice of the people that they log on into their Facebook or Twitter accounts during their lunch break and they check their messages sent by their relatives, friends and their coworkers. It has been observed that users of Facebook or Twitter accounts develop their habits through prolonged use of Facebook or Twitter accounts over long time and they develop "trust" among themselves as studied by (Egele et al., 2015, p. 450). The trust is developed among users of Facebook or Twitter account's users as well as between users and the owner of the Facebook or Twitter account. Also it is a common practice of big multinational companies, firms, news agencies that they use social media networks for the purpose of the advertisement of their products, bidding of the shares, prolific profits of businesses. In this report I discuss the cybercrimes which are conducted through the social media networks like Facebook, Twitter etc. Also we will discuss a software based solution for the detection of cybercrimes conducted through social media networks. This software based solution is named as COMPA which has been proposed and designed at the University of California Santa Barabara as referred in (Velayudhan & Somasundaram, 2019).

2. Literature Review

The cyber criminals have been adopted a new successful course of action which is compromising social network accounts. The cyber criminals search for those accounts which belong to the owners of big multinational companies or news agencies or firms and they hack these accounts by taking the ownership of these accounts of big multinational companies, news agencies and firms. In other words the accounts authorized by the owners of big multinational companies and news agencies would be under control of the cyber criminals as studied by (Trång et al., 2015, p.80). It has been observed from the market of US that big multinational companies have born the big financial losses because of compromising accounts by the cyber criminals. Also the news agencies and firms in USA have suffered reputational loss as well because of the compromised accounts on social media networks and websites. It is a very common misconception about the term "Compromised Accounts" among people. People and laymen have the concept that Compromised Accounts are those accounts which are held by certain users and they remain unused by the owners of the accounts for a long time as studied by (VanDam et al., 2019, p.28). This concept is wrong. The most correct definition of the Compromised Accounts is that compromised accounts are those accounts which are held by the legitimate owners of the account but they are compromised by the cyber criminals. Cyber criminals usually identify and target those accounts which belong to high profile brands, news agencies and companies. For example when we talk about the high profile brands in Pakistan we can consider examples of PTCL, PTA, KELECTRIC, UFONE, ZONG, TELENOR etc. Cyber criminals compromise the accounts of the high profile brands and companies and by compromising these accounts cyber criminals can propagate fake messages, spam emails, fake news alerts, fake product prices. In this way cyber criminals may tarnish the reputation of high

profile companies and may devastate the business and financial assets of high profile companies as referred by (Velayudhan & Somasundaram, 2019).

When cyber criminals compromise social network accounts of news agencies or newspapers, it may harm the financial assets of companies. In 2013, false news spread on Associated Press (AP) news agencies caused significant financial loss to the Standard and Poor's 500 indexes. The news was about the bomb explosion in White House in 2013 and it caused US $130B loss to the Standard and Poor's Index as studied by (Wang et al., 2020, p.406). The detection of the compromised accounts is still not automated and it is done manually. Therefore immediate detection of compromised accounts is still a challenging problem to the researchers in the field of Information Security. When the malicious event is done, it is detected after the occurrence of malicious event and after using compromised accounts. For example the false news about the explosion of bomb in the white house was detected after it has been spread about to 300 users. After spreading to 3000 users it was blocked. Similarly Skype Twitter account was hacked during a national holiday and a message was sent by the hacker who was not the owner of the Skype Twitter account. The message was remained accessible during the whole day as studied by (Cui et al., 2021, p.405).

These events show that it is very difficult to detect the accounts which are compromised and not owned by the account's legitimate owner. Also detection of the compromised accounts is still manual and it takes time to detect that account has been hacked and compromised. Since the detection period usually prolongs up to certain hours or days or weeks depending upon the type of compromise, we cannot block the messages sent by the illegitimate owner of the social media account as referred in (Phad & Chavan , 2018) .

A wealth of research has been proposed for detection of fake accounts which spread fake messages among the users of social networks but very lesser research has been proposed on the detection of legitimate and compromised accounts. Since ordinary people have the concept that fake accounts are as similar as the legitimate and compromised accounts, which is absolutely wrong. Fake accounts are those accounts which spread fake news, messages through social networks whereas the compromised accounts are those accounts which are held by the legitimate owners but they are compromised by the cyber criminals as studied by (Karimi et al., 2018, p. 318).

3. Research Methodology

When we discuss the steps of research methodology we have to implement "Mitigation techniques" for the proposed secure system. The Mitigation Techniques are of two types:

- We can detect malicious accounts which are spreading messages. The detection of malicious accounts can be done by grouping together the similar messages.
- We can look for the suspicious URLs which are included in the messages sent by the cyber criminals.

These systems can detect messages sent by the compromised social network accounts or the messages sent by the cyber criminals advertising the websites pointing towards malware or phishing or these systems may detect the messages sent by the cyber criminals may use multiple accounts to send the same message on social networks.

When the proposed system was tested to detect the compromised accounts, it was found that the proposed system only detected one message at a time sent by the cyber criminals from the compromised accounts. Also the system detected only such message which does not contain

URL pointing to malware or phishing web site. This implies that the systems proposed for detection of compromised accounts has limitations and it is unable to detect more than one message sent by the cybercriminal from multiple social networking websites and it is suspicious that whether the proposed system may detect URLs included in the message sent by the cybercriminal pointing to malware or phishing websites.

COMPA system is a system which was proposed for detection of compromised social network accounts. The design of COMPA is based on a very simple behavior of social network user. A typical social network user usually checks the accounts activities and messages at the time of breakfast from the mobile phone at morning time, or a social network user may check the accounts activities and messages at the lunch break or he/she may check the accounts activities and messages at the end of the office hours during relaxation time. The friends of social network account user which remain in contact become more limited after passage of certain time although the user has a number of friends on social networking website. The habits of a social network user develop over time and at the attainment of certain time period the habits become stable. If a cybercriminal attacks a social network account and compromise it, the messages sent by the cybercriminal exhibit very apparent anomaly from the messages sent or received by the social network account user. The COMPA system has the following features:

- COMPA is the first system designed to detect compromised social network accounts.
- COMPA can detect compromises of the high profile social network accounts. Since the behavior of these high profile accounts are very consistent, false positives are minimal.
- To detect large scale compromises, we group similar messages together and apply COMPA to them, in this way we detect those messages whose behavior deviates with the behavior of high account profiles. There are two types of social network accounts, the first one is regular social network accounts and the second one is the high profile social network accounts. The behavior of regular social network accounts is very different from the behavior of high profile social network accounts. The behavior of regular social network accounts is more variable than the behavior of high profile social network accounts. Therefore the false positives are very low.
- We have applied COMPA system to two popular social network accounts, Facebook and Twitter.

We have detected hundreds of thousands of compromised social network accounts using COMPA. Our system COMPA was able to detect four high profile compromises that affected popular Twitter accounts. The COMPA system was also able to flag as legitimate a fake compromise, a high profile compromise made by US fast food Chain Company that affected its popular Twitter account.

Extensive research has been done on detecting large scale compromises that affected thousands of social network accounts and on detecting isolated compromises of high profile social network accounts. There is an essential fact that the high profile social network accounts compromises exhibit or show very consistent behavior as studied by (VanDam, et al., 2018, p. 474). Our system COMPA can easily detect isolated compromises of high profile social network accounts.

The COMPA system detect compromises of social network accounts on the basis of behavioral profile of social network accounts. The essential characteristic of COMPA system

is that this system builds behavioral profile of social network account users as studied by (Kaur et al., 2019, p.70).

In order to build behavioral profile of social network account users, the COMPA system stores the messages of the social network account users and maintains the history of the messages and activities of social network account users. When the social network account user uses social network account and sends messages to friends or relatives or clients or customers, the COMPA system compares the messages with the history of the messages that is profile of the social network account user as studied by (Egele et al., 2013, p.85).

4. Results and Discussion

On the basis of the type of social network accounts, the results obtained from the COMPA system are different. If the social network account belongs to regular users or ordinary users or customers, the social network account is referred as a regular social network account. If the social network account belongs to high profile companies, news agencies, multinational firms, NGOS, government websites and big private organizations, the profile is referred as high profile social network accounts. It has been observed that the high profile social network accounts show a very consistent behavior whereas the regular social network accounts show inconsistent behavior. On the basis of comparison of activities of social network account users with profiles of social network accounts, the COMPA system detects the compromises of social network account user. Also, it has been observed that the regular social network account user uses the client software features more fluently and with persistence against the user who uses the high profile social network account. Therefore the COMPA system also considers the activities of a user on social network account, and on the basis of the activities it discriminates and distinguishes the regular social network account with the high profile social network account.

5. Conclusion and Future Work

Hence it is concluded that the software based system COMPA successfully detects compromises of social network accounts and using the COMPA system we can detect the compromises of high profile social network accounts, in this way the financial, reputational and other different types of losses not only reduced but can be eliminated through the use of COMPA system.

The use of COMPA system can be more elaborated and extended for detection and identification of malicious users who try to gain Swift Systems implemented in banks as well.

References and Consulted Material

Egele, M., Stringhini, G., Kruegel, C., & Vigna, G. (2013, February). Compa: Detecting compromised Accounts on social networks. *In NDSS* (Vol. 13, pp. 83-91).

Egele, M., Stringhini, G., Kruegel, C., & Vigna, G. (2015). *Towards detecting compromised accounts on social networks. IEEE Transactions on Dependable and Secure Computing*, 14(4), 447-460.

Trång, D., Johansson, F., & Rosell, M. (2015, September). Evaluating algorithms for detection of Compromised social media user accounts. *In 2015 Second European Network Intelligence Conference* (pp. 75-82). IEEE.

VanDam, C., Masrour, F., Tan, P. N., & Wilson, T. (2019, August). You have been caute! early Detection of compromised accounts on social media. *In Proceedings of the 2019 IEEE/ACM International conference on advances in social networks analysis and mining* (pp. 25-32).

Suresh, S., & Joseph, U. M. *Hacking Malicious Users on Social Networks Using COMPA Method.*

P. Velayudhan, S., & Somasundaram, M. S. B. (2019). *Compromised account detection in online Social networks: A survey. Concurrency and Computation: Practice and Experience*, 31(20), e5346.

Wang, X., Tang, H., Zheng, K., & Tao, Y. (2020). Detection of compromised accounts for online social Networks based on a supervised analytical hierarchy process. *IET Information Security*, 14(4), 401-409.

Cui, Y., Wang, K., Hu, J., Zhao, W., Feng, L., & Cui, J. (2021). Compromised Accounts Detection Based on Information Entropy. International Journal of Network Security, 23(3), 401-411.

Phad, P. V., & Chavan, M. K. (2018, July). Detecting compromised high-profile accounts on social Networks. In 2018 9th International Conference on Computing, *Communication and Networking Technologies (ICCCNT) (pp. 1-4). IEEE.*

Karimi, H., VanDam, C., Ye, L., & Tang, J. (2018, August). End-to-end compromised account Detection. In 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis And Mining (ASONAM) (pp. 314-321). *IEEE.*

VanDam, C., Tan, P. N., Tang, J., & Karimi, H. (2018, August). Cadet: A multi-view learning Framework for compromised account detection on twitter. *In 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (ASONAM) (pp. 471-478). IEEE.

Desale, D., & Desai, P. (2017). A Heuristic Approach for Compromised Account Detection through Machine Learning. *IJETT*, 1(2).

Kaur, R., Singh, S., & Kumar, H. (2019). Metacom: Profiling meta data to detect compromised Accounts in online social networks. In Future Network Systems and Security: 5th International Conference, FNSS 2019, Melbourne, VIC, Australia, November 27–29, 2019, Proceedings 5 (pp. 65-80). *Springer International Publishing*.