ONLINE PROFILE COMMUNITY BEHAVIOURS FOR DISPENSATION REPORT DETECTION

N ASHWINI[1], S VISHWANATH REDDY[2]

1PG Scholar, Dept of CSE, Mallareddy College Of Engineering And Technology, Hyderabad, TS, India.

2Assistant Professor, Dept of CSE, Mallareddy College Of Engineering And Technology, TS, India.

***Abstract*—** A novel approach to discover social networks committed by the user, which we apply to social networking sites, Twitter and Face book. Our approach uses a set of statistical models and anomaly detection to identify accounts that experience a sudden change in behavior. Because changes in behavior can also be for benign reasons (for example, a user can change the preferred client application or implement updates at an unusual time), it is necessary to devise a way to distinguish between deleterious and legislative changes. To this end, we are looking for groups of accounts that face similar changes in a short period of time, assuming that these changes are the result of a malicious campaign. We are studying a large anonymous collection of asynchronous "wall" messages among Face book users. We analyze all the messages received by almost 3.5 million Face book users (more than 187 million messages in total) and use a set of automated techniques to discover and characterize coordinated spam campaigns. We demonstrate the practicality and effectiveness of our approach to using full Face book exploratory data: we have successfully discovered several attacking strategies (false, risky and complicit with Face book identities) without prior classification and low error rates. Finally, we apply our approach to detect spam in Face book ads, and find that a surprisingly large portion of clicks comes from anomalous users.

***Keywords*—** *Online social networks, Spam, Spam Campaigns.*

I. INTRODUCTION

Online social networks like Face book and Twitter have become more popular in recent years. People use social networks to stay in touch with family, chat with friends and share news. Over time, social network users create connections with their friends, colleagues and, in general, with those they consider fun or reliable. These contacts form a social framework that controls how information is disseminated in the social network. Users typically receive messages posted by connected users, such as wall posts, tweets, or status updates. The large user base of these social networks has attracted the attention of cybercriminals. According to a 2008 study, 83% of social network users received at least one unwanted message on those networks in that year [1]. In addition, large malware campaigns have been implemented on social networks [2]. Previous work has shown that spam, phishing and malware are real threats to social networking sites [3, 4]. Of course, a message that violates the user profile does not necessarily indicate that this account has been hacked. The message may be strange or simply reflect a natural change in behavior. For this reason, as in previous works, our approach seeks other similar messages recently published in the social network that also violate the user behavior profiles. This means that we can not detect cases in which an attacker publishes a single malicious message through a pirated account. We believe that this is reasonable because the attackers generally try to distribute their messages to more victims. In addition, our experiments show that we can detect pirated accounts even in the case of small campaigns (in our Twitter experiments, for example, we request at least 10 similar messages per hour). We present the first study of this type to measure and analyze attempts to disseminate malicious content in OSN networks. Our work is based on a wide range of Face book "wall" messages. Publications on the wall are the basic form of communication on Face book, where a user can leave messages on a friend's public profile. Wall messages remain in the user profile unless explicitly deleted by the owner. As such, the wall messages are an easy place to look for attempts to publish malicious content on Face book because the messages are static and general, which is likely to be shown by the target user and perhaps by the recipient friends. By tracking many regional Face book networks conducted in 2009, we obtained a large set of anonymous data for Face book users, their friendships and a 1.5 year history of wall-based posts per user [5]. In total, our data collection contains more than 187 million wall publications received by 3.5 million users. Our study of the publications in Face book Wall has two basic phases. First, we analyze all messages on the wall and use a series of complementary techniques to identify attempts to publish malicious content. We focus our analysis on messages that contain URLs or web addresses in text format. From these messages, we produce interconnected subsets of wall publications. We represent each publication as a node, and create edges that link two nodes that point to the same URL, or two nodes that share text content similar to that specified by a raw text footprint. This process creates a series of related subdivisions that divide all suspicious wall messages into mutually subscribed groups, where the messages are likely to be in a linked group. Using dual behavioral suggestions for explosive activities and distributed communications, we can identify subsets of messages that show the characteristics of malicious spam campaigns. We use many complementary mechanisms to verify the effectiveness of our technique and to demonstrate that our approach is very effective in detecting the spread of harmful content. In summary, we present the first attempt to determine the prevalence of malicious accounts and the propagation of malicious content in OSN. We use multiple techniques to detect the link between wall messages and to determine the prevalence of potentially harmful content. Our results are confirmed by a series of verification mechanisms. Our subsequent analysis provides information on the functioning of malicious accounts and has important implications for designing future mechanisms to detect malicious behavior in OSN networks.

II. LITERATURE SURVEY

Most of the previous search for unwanted account detection can distinguish between hacked accounts and sybil accounts, with only one recent study. The characteristics expose the risk accounts. Current methods include analyzing the profile of the account and analyzing the content of the message (such as embedded URL analysis and message segmentation). However, analyzing the profile of the account is almost impractical to detect vulnerable accounts, since their profiles are the original common user information that is likely to remain intact by spammers. Harmful parties exploit established contacts and trust relationships between legitimate account holders and their friends, and effectively distribute spam, phishing or malware links while avoiding blocking by service providers. Today, OSN is working to register the location of IP to combat the breakdown of the account. However, it is known that this technique has a low detection accuracy and a high false positive rate. The URL blacklist faces the challenge of timely maintenance and updating, and message aggregation presents a significant burden when exposed to a large number of messages in real time.

III. PROPOSED METHOD

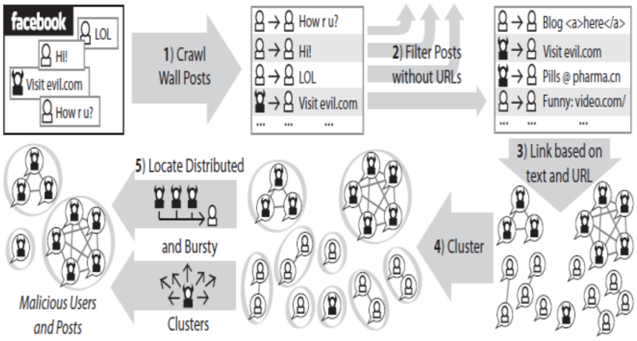
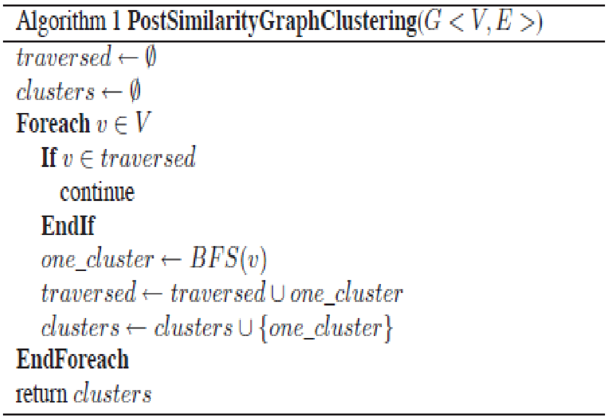


Fig 1: The system Architecture

To identify malicious wall posts from our large data set, we used semantic similarity measures to identify the exclusive groups exchanged within the set of wall posts. Then, we use behavioral cues to identify different collections of walls as benign or potentially harmful. In this section, half of the process is several steps through which we organize, collect and identify potentially harmful publications. We begin by analyzing the whole process, followed by a detailed description of each step.



```
Algorithm 1 PostSimilarityGraphClustering($G < V, E >$)
$traversed \leftarrow \emptyset$
$clusters \leftarrow \emptyset$
Foreach $v \in V$
    If $v \in traversed$
        continue
    EndIf
    $one\_cluster \leftarrow BFS(v)$
    $traversed \leftarrow traversed \cup one\_cluster$
    $clusters \leftarrow clusters \cup \{one\_cluster\}$
EndForeach
return $clusters$
```

The problem of identifying spam campaigns now has less problems identifying the related sub-graphics within the similarity graph. Each connected subscript is equivalent to one component of a potential spam campaign. The identification of sub-graphics is easily solved by selecting repetitive nodes and identifying cases of cross-closure. Summarize the implementation in the algorithm.

VI.CONCLUSION

We suggest creating a social behavior profile for individual OSN users to describe their behavior patterns. Our approach takes into account both controversial and introverted behaviors. Based on social behavior profiles, we can distinguish users from others, which can be easily used to detect pirated accounts. Specifically, we provide eight behavioral features to portray users' social behaviors, which include both publication and navigation activities. The statistical distributions of the users of the values of these characteristics include their behavior profile. Although user behavior profiles vary, it is very likely that the activities of individual users are consistent with their behavior profile. Therefore, this fact is used to detect a piracy account, since the social behavior of the scammers is not compatible with the original behavior of the user. Our evaluation of a sample of Face book users indicates that we can achieve high detection accuracy when behavioral profiles are created in a complete and accurate manner.

VII. REFERENCES

[1]. Harris Interactive Public Relations Research, “A Study of Social Networks Scams,” 2008.

[2]. J. Baltazar, J. Costoya, and R. Flores, “KOOBFACE: The Largest Web 2.0 Botnet Explained,” 2009.

[3]. H. Gao, J. Hu, C.Wilson, Z. Li, Y. Chen, and B. Zhao, “Detecting and Characterizing Social Spam Campaigns,” in Internet Measurement Conference (IMC), 2010.

[4]. C. Grier, K. Thomas, V. Paxson, and M. Zhang, “@spam: the underground on 140 characters or less,” in ACM Conference on Computer and Communications Security (CCS), 2010.

[5]. WILSON, C., BOE, B., SALA, A., PUTTASWAMY, K. P., AND ZHAO, B. Y. User interactions in social networks andtheir implications. In Proceedings of the ACM European conference on Computer systems (2009).