IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 7, July 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007088 |

Twitter Based Insider Threat Detection Using Machine Learning Algorithms

AKILAN A, G.KAMATCHI

Assistant Professor, Department of CSE, MRK Institute of Technology, Kattumannarkoil, India

Department of CSE, MRK Institute of Technology, Kattumannarkoil, India

ABSTRACT: This paper provide high security against suspicious uniform resource location in social networks. Twitter is a social network and it can be used by more number of peoples. While open the normal browser many number of pages are opened .In that number of pages suspicious pages and malicious pages are occur. It detect the unwanted pages based on the redirect chain and correlation of redirection chain features are extracted from the suspicious URL.Twitter is prone to malicious tweets containing URLs for spam, phishing, and malware distribution. Twitter spam detection schemes utilize account features such as the ratio of tweets containing URLs and the account creation date, or relation features in the Twitter graph. These detection schemes are ineffective against feature fabrications. Since it consume much time and more resources. Conventional suspicious URL detection schemes utilize several features including lexical features of URLs, URL redirection, HTML content, and dynamic behavior. This system investigates correlations of URL redirect chains extracted from several tweets. Because attackers have limited resources and usually reuse them, their URL redirect chains frequently share the same URLs. It develops methods to discover correlated URL redirect chains using the frequently shared URLs and to determine their suspiciousness. Evaluation results show that the classifier accurately and efficiently detects suspicious URLs.

KEYWORDS: Suspicious URL, twitter, Spammer, Online Social Network, anomaly detection

I.INTRODUCTION

Twitter is an online social networking and micro blogging service that enables users to send and read "tweets", which are text messages limited to 140 characters. Registered users can read and post tweets, but unregistered users can only read them. Users access Twitter through the website interface, SMS, or mobile device app. Many social networking Web sites have lots of bells and whistles. Sites like MySpace and Facebook let users build profiles, upload pictures, incorporate multimedia, keep a blog and integrate useful or bizarre programs into homepages. But one Web company with a very simple service is rapidly becoming one of the most talked-about social networking service providers:

Twitter.

So what does Twitter do? When we sign up with Twitter, we can use the service to post and receive messages to a network of contacts. Instead of sending a dozen e-mails or text messages, we send one message to our Twitter account, and the service distributes it to all our friends. Members use Twitter to organize impromptu gatherings, carry on a group conversation or just send a quick update to let the user know what's going on.

The idea behind twitter is that you broadcast to anyone who chooses to follow you, simple messages also known as "tweets". It could be as simple as what you are doing right now or you could ask a question to your followers. Likewise we can choose to follow people and receive their messages.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007088 |

II.DETECTING SPAMMERS

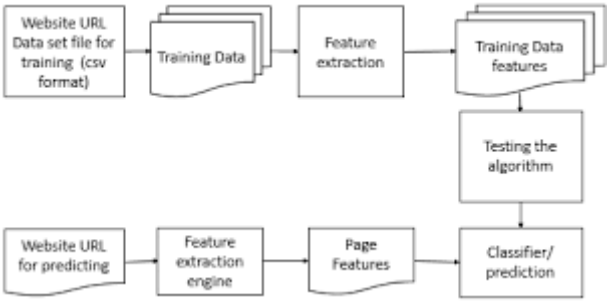

Fig 1.Block diagram for detecting suspicious URL

Understanding the link farming in the twitter- Twitter has emerged as a popular platform for discovering real-time information on the Web, such as news stories and people's reaction to them. Like the Web, Twitter has become a target for link farming, where users, especially spammers, try to acquire large numbers of follower links in the social network. Acquiring followers not only increases the size of a user's direct audience, but also contributes to the perceived influence of the user, which in turn impacts the ranking of the user's tweets by search engine. In twitter stream, it first investigates link farming in the Twitter network and then explores mechanisms to discourage the activity. The twitter stream find that link farming is wide spread and that a majority of spammers' links are farmed from a small fraction of Twitter users, the social capitalists, who are themselves seeking to amass social capital and links by following back anyone who follows them.

Online spam filtering in social networks- Online social networks are extremely popular collaboration and communication tools that have attracted millions of Internet users. Unfortunately, recent evidence shows that they can also be effective mechanisms for spreading attacks. Popular OSNs are increasingly becoming the target of phishing attacks launched from large botnets. Furthermore, the click through rate of OSN spam is orders of magnitude higher than its email counterpart indicating that users are more prone to trust spam messages from their friends in OSNs. The OSN spam problem has already received attention from researchers. Meanwhile, email spam, a seemingly very similar problem, has been extensively studied for years. Unfortunately, the bulk of the existing solutions are not directly applicable, because of a series of distinct characteristics pertaining to the OSN spam. 1. In any OSN, all messages, including spam, originate from accounts registered at the same site. In contrast, email spam is not necessarily sent from accounts registered at legitimate service providers. The widely used email server reputation based detection approaches rely on the assumption that the spamming SMTP servers run on bot machines, and are thus inapplicable in OSNs. Realizing that this assumption is not always true, researchers have proposed to identify accounts signed up by spammers from legitimate email service providers 2. Spamming account identification is also the focus of the existing OSN spam detection work However, the second characteristic of OSN spam is that the majority of spam messages come from compromised rather than accounts created and exclusively controlled by spammers. It essentially means that spammers and legitimate users are sharing accounts. Thus, identifying spamming accounts is not sufficient to fight OSN spam. 3. Messages in OSNs spam or not, are generally short. The perception that legitimate emails have variable size while spam tends to be small. It proposes to use spam campaigns, instead of individual spam messages, as the objects for spam classification. It solve the challenge of reconstructing campaigns in real-time by adopting incremental clustering and parallelization. It identify six features that distinguish spam campaigns from legitimate message clusters in OSNs.The warningbird system develop and evaluate an accurate and efficient system that can be easily deployed at the OSN server side to provide online spam filtering.

Analyzing spammer's social networks- Twitter stream perform an empirical analysis of the cyber criminal ecosystem on Twitter. Essentially, through analyzing inner social relationships in the criminal account community, it finds that criminal accounts tend to be socially connected, forming a small-world network. It also finds that criminal hubs, sitting in the center of the social graph, are more inclined to follow criminal accounts. Through analyzing outer social relationships between criminal accounts and their social friends outside the criminal account community, it reveals three categories of accounts that have close friendships with criminal accounts. Through these analyses, it provides a

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007088 |

novel and effective criminal account inference algorithm by exploiting criminal accounts' social relationships and semantic coordination.

Although it is difficult to accurately trace how these connections are generated, this observation still reflects the high probability that criminal accounts in the same criminal organization are artificially/intentionally connected. In fact, no matter whether these connections are built using random selection or intentional construction, criminal accounts could benefit from such strong social connections in the criminal community. Essentially, this structure provides "support" followers to criminal accounts, which are very important for criminal accounts to either break the Following Limits Policy or evade detection features that are built based on the metric of follower number. It presents an empirical analysis of the cyber criminal ecosystem on Twitter. It provides in-depth investigation on inner and outer social relationships. It observes two findings in the cyber criminal community and reveals the characteristics of three representative categories of criminal supporters. Spurred by defense insights originating from these analyses, we design an effective algorithm to infer more criminal accounts by starting from a seed set of known criminal accounts and exploiting the properties of their social relationships and semantic correlations. It analyzed dataset may contain some bias.

Also, the number of analyzed criminal accounts is most likely only a lower bound of the actual number in the dataset, because the only target on one specific type of criminal accounts due to their severity and prevalence on Twitter.

III.METHOD

Spam and non-spam accounts and extract the features that can effectively distinguish spam from non-spam accounts. To detect spam accounts, some schemes manually analyze the collected data some use honey profiles to lure spammers. In existing spam detection scheme strong relationship with their neighbors .It will lead to many possibility can send suspicious message. Attacker can lure the normal user based on their interesting advertisment.There is no correlated relationship with their neighbours. It need more time to did their process. There is no specific keyword for detecting the attacker messages. Spam nodes usually cannot establish robust relationships with their victim nodes. However, the extractions of these features involve a large consumption of time and resources.

Many possibilities for misidentification of legitimate user. In previous approach only some of the attributes are used for detecting spammers' accounts. Instead of that attributes some misbehavior possible. Twitter public timeline to detect accounts that post tweets with blacklisted URLs and yet others monitor Twitter's official account for spam reporting. Previous works have proved that language model disagreement techniques are very efficient in tasks such as blocking blog spam and detecting nepotistic links and Web spam. For this reason, it want to apply these techniques to improve classification in a spam Twitter labeled dataset of around 34 K trending topics, 21 million tweets and 6 million URLs.Twitter stream apply Kullback–Leibler Divergence between their respective language models. KLD is an asymmetric divergence measure originating in information theory.

To cope with malicious tweets, several Twitter spam detection schemes , have been proposed. These schemes can be classified into account feature-based relation feature-based and message feature-based schemes. Account feature-based schemes use the distinguishing features of spam accounts such as the ratio of tweets containing URLs, the account creation date, and the number of followers and friends. However, malicious users can easily fabricate these account features. The relation feature-based schemes rely on more robust features that malicious users cannot easily fabricate such as the distance and connectivity apparent in the Twitter graph. Extracting these relation features from a Twitter graph, however, requires a significant amount of time and resources as a Twitter graph is tremendous in size.

The message feature-based scheme focused on the lexical features of messages. However, spammers can easily change the shape of their messages. A number of suspicious URL detection schemes[2] have also been introduced. They use static or dynamic crawlers, and they may be executed in virtual machine honey pots, such as Capture-HPC, HoneyMonkey, and Wepawet, to investigate newly observed URLs. These schemes classify URLs according to several features including lexical features of URLs, DNS information, URL redirections, and the HTML content of the landing pages.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007088 |

IV.RESULT

The collection of tweets with URLs and crawling for URL redirections. Detect misbehavior URLs .The classification component executes our classifier using input feature vectors to classify suspicious URLs. The proposed system can used for dynamic environment.This concept can detect the attacker URL with dynamic behaviour.The attacker could not use the normal web page.Based on the correlation of all the features about the attacker can extracted before the training and classification phase. The features are extracted based on the domain and HTTP address and many features are considered. Based on the all the feature the attackers. The advantage of this approach is time consumption and used in dynamic user account creation not only static user creation.This concept is based on the analysis of the language used in each tweet, to identify those messages whose purpose is to divert traffic from legitimate users to spam websites. The proposed system using **supervised learning algorithm** to detect the attackers. This system quickly detects the attackers and it consuming very less time compared to the existing system.

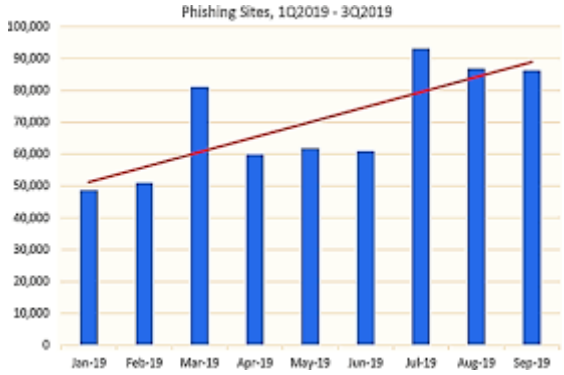

Fig2: Result Analysis

Two tools that are available to spammers are the 140 characters in a tweet and the linked pages. In addition, because of growing micro blogging phenomenon and trending topics, spammers can disseminate malicious tweets quickly and massively. The system introduced new features on the basis of these correlations, implemented a near real-time classification system using these features, and evaluated the system's accuracy and performance. The evaluation results show that our system is highly accurate and can be deployed as a near real-time system to classify large samples of tweets from the Twitter public timeline. The operators can also extract other features from e-mail context information such as the number of senders and receivers, the number of mail servers and relay servers, and similarities in e-mail messages. Web forum services are also similar; as their operators can collect all posts and comments of users containing URLs and can extract based features as well as other features including user IDs, IP addresses, and message similarities.

V.CONCLUSION

Thus it concluded that comparing the existing methods of suspicious URL detection utilizes much resources and it consuming more time to detect the suspicious URL. . It used account feature-based, relation feature-based and message feature-based schemes. However, malicious users can easily fabricate these account and message features. The relation feature-based schemes rely on more robust features that malicious users cannot easily fabricate such as the distance and connectivity apparent in the Twitter graph .So, in proposed system a new suspicious URL detection method was used. It used supervised learning algorithm to detect and classify suspicious URL.It extracts feature vectors such as URL redirect chain length, IP address, and domain name. It also addresses dynamic and multiple redirections. The final goal of the proposed method is it introduced some new features on the basis of these correlations, and the system's accuracy and performance was increased.

REFERENCES

[1] S. Lee and J. Kim, "WarningBird: Detecting Suspicious URLs in Twitter Stream," Proc. 19th Network and Distributed System Security Symp. (NDSS), 2012.

[2] C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: The Underground on 140 Characters or Les," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), 2010.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165

|| Volume 10, Issue 7, July 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1007088 |

[3] C. Yang, R. Harkreader, and G. Gu, "Die Free or Live Hard? Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers," Proc. 14th Int'l Symp. Recent Advances in Intrusion Detection (RAID), 2011.

[4] C.Y.R. Harkreader, J. Zhang, S. Shin, and G. Gu, "Analyzing Spammers' Social Networks for Fun and Profit—a Case Study of Cyber Criminal Ecosystem on Twitter," Proc. 21st Int'l World Wide Web Conf. (WWW), 2012.

[5] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida,"Detecting Spammers on Twitter," Proc. Seventh Collaboration,Electronic Messaging, Anti-Abuse and Spam Conf. (CEAS), 2010.

[6] G. Stringhini,C. Kruegel, and G. Vigna, "Detecting Spammers on Social Networks," Proc. 26th Ann. Computer Security Applications Conf. (ACSAC), 2010.

[7] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, "Towards Online Spam Filtering in Social Networks," Proc. 19th Network and Distributed System Security Symp. (NDSS), 2012.

[8] J. Ma, L.K. Saul, S. Savage, and G.M. Voelker, "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs," Proc. 15th ACM SIGKDD Conf. Knowledge Discovery and Data Mining (KDD), 2009

[9] J. Ma, L.K. Saul, S. Savage, and G.M. Voelker, "Identifying Suspicious URLs: An Application of Large-Scale Online Learning,"Proc. 26th Int'l Conf. Machine Learning (ICML), 2009.

[10] J. Song, S. Lee, and J. Kim, "Spam Filtering in Twitter Using Sender-Receiver Relationship," Proc. 14th Int'l Symp. Recent Advances in Intrusion Detection (RAID), 2011

[11] M. Cova, C. Kruegel, and G. Vigna, "Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code,"Proc. 19th Int'l World Wide Web Conf. (WWW), 2010

[12] S. Ghosh, B. Viswanath, F. Kooti, N.K. Sharma, G. Korlam, F.Benevenuto, N. Ganguly, and K.P. Gummadi, "Understanding and Combating Link Farming in the Twitter Social Network,"Proc. 21st Int'l World Wide Web Conf. (WWW), 2012.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details