A REVIEW OF DETECTION OF MALICIOUS URLs IN TWITTER STREAM USING A NEAR REAL TIME SYSTEM

1NUPUR S. GAWELE, 2NITIN N. PATIL

1PG Student, Department of Computer Engineering, North Maharashtra University
SES's R. C. Patel Institute of Technology, Shirpur, MS, India
2H.O.D. and Associate professor, Department of Computer Engineering, North Maharashtra University
SES's R. C. Patel Institute of Technology, Shirpur, MS, India
Email: nupurgawale14@gmail.com, er_nitinpatil@rediffmail.com

Abstract—This paper presents a survey of twitter stream which is vital for finding twitter attacks. Online social networking has become a very popular way for users to meet and interact online. Users spend a large amount of time on popular social network platforms such as Facebook, MySpace, or Twitter, storing and sharing a wealth of personal information. This information, as well as the possibility of contacting billions of users, also attracts the interest of cybercriminals. Millions of users tweeting around the world, real time systems and different types of mining tools are emerging to allow people tracking the events and post on Twitter. Twitter allows users to discuss events and post their status, these services open opportunities for new forms of spam. Trending topics, the most talked about trending topics on Twitter at a given point in time, have been seen as an opportunity to generate traffic and revenue. Spammers post tweets containing typical words of a trending topic and URLs, usually obfuscated by URL that lead users to completely unrelated websites. This kind of spam can contribute to devalue real time search services unless mechanisms to fight and stop spammers can be found. Online social networks are extremely popular among Internet users. Unfortunately, in the wrong hands they are also effective tools for executing spam campaigns. So to avoid that presenting an online spam filtering system that can be deployed as a component of the online social networks platform to inspect messages generated by users in real-time. And that reconstructs spam messages into campaigns for classification rather than determine them individually. Although campaign identification has been used for offline spam filtering, apply this technique to aid the online spam detection problem with low overhead. Accordingly, system adopts a set of features that effectively distinguish and determine spam campaigns. It drops messages classified as “spam” before they reach the intended destination, thus protecting them from various kinds of malicious aspects. Firstly collecting a large dataset of Twitter. From that construct a large labeled collection of users, manually classified into spammers and non-spammers. Then identify a number of characteristics related to tweet content and user social behavior, which could potentially be used to detect spammers. Used these characteristics as attributes of machine learning process for classifying users as either spammers or nonspammers. This strategy succeeds at detecting much of the spammers while only a small percentage of non-spammers are misclassified. In this system investigates correlations of URL redirect chains extracted from several tweets and forms frequently shared url. Because attackers have limited resources and usually they reuse them. Develop methods to discover correlated URL redirect chains using the frequently shared URLs and to determine their suspiciousness. Collect numerous tweets from the Twitter public timeline and build a statistcal classifier using them. Evaluation results show that classifier accurately and efficiently detects suspicious URLs.

Keywords: Twitter Stream, Malicious URL, URL redirection, conditional redirection, classification

I. INTRODUCTION

The online social networking sites are there to communicate with millions peoples. Through this site people are come together or closer still they are far away from each other. Just because of this online social networking site. This is the very big advantages of these sites and aim of the developer. In this online social networking site the online service providers are there. They are connected with the user through some interface. So, there are very famous social networking sites are there like Facebook, Twitter, Myspace etc. Through this site the billion people are connected continuously at the same time. They can share their views, ideas, emotion and also they can see to each other also can share the online audio, video chatting. So these sites are working for user. Facebook is born in 2000 through which all people they can meet there new, old friend on that window. The Facebook this site was also gives the all facility to user. Then after the world is growing as fast the twitter newly social networking site is born in 2004. Twitter is microblogging service and site. That gives all the features and facilities to the twitter user like Facebook and all. Twitter is very famous and social networking site among all the networking sites. In twitter user tweet the text. It means supposes two people are talking or connected to each other than both are sending some update to each other about itself or either on some current trending topic. So, at that time they post there text.
That text we can say it is tweet. Twitter this online social networking site having its own rules and regulation. The text to be tweeted has limit of 140 characters. In twitter user can send the tweet to any other one in only 140 characters. In this way user can communicate. Also along with user can share their picture, videos, URLs etc. When one or more webpages want send one user to another then at that time URL link is used.

II. BASIC TERMS

A. Keypoints of Twitter

In twitter suppose two people Alice and Bob is communicated then Alice is tweeting his text in the form of tweet. As Bob is friend of Alice because of that Bob getting all the post of Alice on his window. It means Bob is follower of Alice. He can see all the post of Alice. Again instead of sending to all the post there is also post can be sending to only one particular person. In this way the twitter is working. Now, on this social site have some advantages also their some disadvantage. Because of this online social networking sites. As we know network is huge part through this network the world is so closed and connected. Without network support these sites are not working properly. So, in the network their so many people are there to sharing data among that some kind of people are want to get the data or it means they hacked the user personal and confidential data and those people we can say that attacker. So, in the network common forms of web attacks are there. Also we can say viruses who want to destroyed user data. Alice and Bob are connected , and if the Alice send account number to Bob then at that time the third party person get that information then very huge loss of the both Alice and Bob have to survived. So, that in the network security is very important for confidential data. This main dangerous and serious problem is in the network. Still the researchers are working on them. They also survived from this situation. Because as the world is growing facilities are provided by the service providers is also growing but simultaneously the attacker also growing there ways are continuously changed for attacking. So there is very big challenged for the researchers to detect them and drown out from the bottom. This attacker loss the user data, continuously irritating the user they also make the slow speed of user’s system. Up till now we understand the attacker which creates unwanted interrupt into the user work. Now how they interrupt in users work. So there are various ways of attacking spam, phishing and malware etc.

B. Keypoints of Attacks on twitter

Spam is flooding the Internet with many copies of the same message. And spam is force the user who would not attempt or receives the message. Spam is nothing but the commercial advertising, get rich and quick schemes. This spam also has types. The first one is Cancellable Usenet spam and Email spam. The cancellable Usenet spam is a single message sent to 20 or more Usenet newsgroups. The aim of this Usenet spam is the people or user who read the newsgroups but not posting the text or not clicking on any link. So to finding the address of those people for that Usenet spam is used. And the second one that is Email spams which targets individual user with direct mail message. Email spam aim is that usually cost users money out of pocket to receive. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses. Then another second web attack is phishing. Phishing means to catch the user into our net like that attacker give the interesting advertisement, rich schemes it means attacker feel that user is attempting to that and gives the details of itself. The attacker mainly wants only the user details through that he may want attack. Phishing is the act of attempting to acquire information such as usernames, password, and credit card details. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. And the third attack is malware attack. Malware short for malicious software is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of intrusive software. Malware includes computer viruses, horses, rootkits, key loggers, dialers, spyware, adware, malicious, rogue security software and other malicious programs the majority of active malware threats are usually worms or Trojans rather than viruses. Malware is sometimes known as a computer contaminant. Malware is different from defective software, which is legitimate software but contains harmful bugs that were not corrected before release. However, some malware is disguised as genuine software, and may come from an official company website in the form of a useful or attractive program which has the harmful malware embedded in it along with additional tracking software that gathers marketing statistics. In this way there are many major forms of web attacks are there to disturbed the user system. So this attacks gives very big challenged to researchers to work on them. So many researchers are working on from long time to avoid these attacks.

III. OTHER TECHNIQUES FOR DETECTION OF MALICIOUS URLS

A. Study on Collection of Database
Collect all twitter database based on some twitter public timeline. Crawled all tweets, URLs, pictures whatever the user posted that all data is collecting. From that collection we may want to detect the spam, phishing and malware etc. So for that using the PageRank algorithm. Firstly, finding the account details means from how long account is used or working time it means popularity of account or user. Then through that timeline whatever posting is there from that account would be consider. On that basis ranking can be done. Then second ranking is that the how many followers following them so both this table somewhat same ranking. Now, third is the ranking on rewetting it means when any particular user rewetting same post then ranking may differ from previous two columns. Among this whatever user account are highlighted through this ranking all that user account have more doubt. So, all the posting coming from them or going from them is very important as point of view detecting. In this method the trending topic is most consider to finding the defect. So the topic which very well represented, issues are drown carefully and neatly then that topic is consider as trending topic primarily basis. Then after those seven days continuously observing the updates about that then finally that topic is placed in trending topic list. Generally attacker uses this trending topic to attack on user. Because the more users are interested in current affair so many people are clicking URLs, sharing the webpages about that, updating itself. So whatever they get about that they by default use, it shares it. Unfortunately they survived through these attacks.

B. Account details and Content Attribute

Firstly categorized the legitimate user and the spammer, using simply account details and through posting. Any text with URL tweet is their then and that URL is not related with the text so understand that this account is malicious user account and tweet also malicious with link. Then secondly check every tweet and URL redirection. And finding the malicious tweet. Again for clearer searching he collects small 20 tweets cluster then observed that on twitter public timeline. Also uses the feature to detect the malicious attribute in which Google safe browsing and Capture HPC techniques to find phishing and malware attacks. And the feature is very useful to get clue. Like the content based feature, profile based feature, gaining more posts, mixing normal posts, graph based feature, neighbor based feature etc. through this feature like as already said that the content and url is not match with each other then it will be malicious. Then profile based feature means account details like account is public or private then timeline, whole friend and follower list etc. Again one very important point is that spam tweets are small in length compare to legitimate tweet so this also one way to finding the spammer [5].Because the spammer have less resources so in this way also spammer was detected but only one thing that when URL redirection is checked so that we have to click on every page or link so that attacker is easily spared their recourses into the user account and account or data is loosened. So method is effective but after affection.

C. Study of Online spam filtering

Online social networking sites are depending on the network support. So this online social networking site uses online service providers through interface user are connected. In these schemes the online spam filtering is constructed in online service providers. This online spam filtering compares the tweets with previously stored data. Then finding the suspicious attribute[11]. In these schemes the system details past message are compare with the current incremental cluster then again that fed to the trained classifier.

IV. RESEARCH DIRECTION

A. Study on Feature Extraction

Grouping the same domain name, if domain name is same then from that IP address are grouped. Once all tweet of same domain name and same IP address then after that finding the entry point URL. Any one user sending too many URL then initial pages are different but the virus or attacking pages may be the same. One user having different chain length so all that grouped into one URL which having all URL references that main URL is finally checked by the system. Then all the features are applied to that entry point url like frequency of entry point url, chain length of url, initial landing pages of url, time of interval of appearance, content size etc. this features are using means predication is their also the machine leaning algorithm is used that have many list of method that is Bayesian network, Decision tree, Support vector machine etc. algorithms used.

B. Study on Training and Classification

Classification is there and the tweet which are consider as suspicious then that finally goes into the sliding window which gives message do not follow it. And which are not classified then that tweet again going for training. Then training uses the account details and training classifier. Then again feature is extracted. In this way this warningbird system is very effective to finding malicious urls.

CONCLUSIONS AND FUTURE WORK

In this paper, we have discussed the robust result and it protects the user from suspicious URL in twitter. This system protects against conditional redirection and that distinguishes investigators from normal browsers and denied malicious pages. This
correlation is used by the research to implement a near real time classification system and also the system accuracy and performance evaluated. In our future work, we are planning to system to address dynamic and multiple redirections.

ACKNOWLEDGEMENT

We are thankful to all the researchers who helped us throughout this survey. We have done research in this area which gives future research direction for many researchers.

REFERENCES