International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

TRACING AND FILTERING INORGANIC TWEETS URLs IN TWITTER

[1]Mahalakshmi A, and [2]Padma M

University College of Engineering (BIT CAMPUS), Tiruchirappalli

[1]Mahalakshmiwin25@gmail.com

[2]emamurugan@gmail.com.

***Abstract*- Twitter enables us community - based opportunities to engage, share and interact short text messages through online social networking .The community value oriented and related services like tweets that contain context information about 140 characters and URL links by using URL shortening service that are threatened by spammers, content polluters, malware disseminators. It is an effort made for preserving community value and long term success lead to propose the technique "supervised learning based classifier" for detecting suspicious URLs in Twitter. In this proposed approach two key components are utilized to detect suspicious URLs. They are, tracing the suspicious URLs by discovering correlated URL redirected chains using the frequently shared URLs and filtering out the malicious URLs by building a statistical classifier using numerous tweets collected from the Twitter public timeline. More precisely and effectively this approach focuses on the detection of suspicious URLs in Twitter than that of already prevailing detecting system.**

Keywords: Suspicious URL, twitter, URL redirection, conditional redirection, classification

I. INTRODUCTION

Being a social animal no human being can live in isolate, everyone gets satisfied if he/she is socially recognized. Social recognition can be achieved through sharing of ideas, knowledge, and messages like news, trending topics, jokes and other information by means of communicative modes available for us. Now we are in the computerized world, online social networking made sharing in the easiest possible way. Among available online social networking services Twitter is popularly known online social networking and micro-blogging service that permits users to post and share their information all the way they need[1]. The information shared by the users in Twitter consists of short text messages (140 characters) denoted as tweets. While sharing, if a user 'A' post the tweets in the Twitter public timeline, it will be reflected to his/her followers and sends the tweets to the specific Twitter user 'B' too, by indicating @b in the tweet, unlike status updates of tweets can also be delivered to users those who are not the follower of user A. when user need to share the URLs via tweets, can use URL shortening services to reduce URL length, because tweets contain limited number of characters only. TinyURL.com and bit.ly are commonly used services and a shortening service t.co. is also provided by Twitter [2].

The unauthorized users have chances of using Twitter as a tool to spread malicious links for advertising to generate sales, virus, disseminate pornography, phishing, unsophisticated users to legitimate users and hijacking or simple just to compromise system reputation .All because of short in length of tweets and usage of shortened malicious URLs that redirect the Twitter user to external servers. Attackers are not only pollute real time search but can interfere on statistics presented by tweets mining tools and consume more extra resources from users and systems too.

For malicious links, inevitable Twitter spam detection schemes have been proposed and still continuing [3]. These schemes are classified as,

1) Account feature based: use the distinguished features of spam accounts such as date of account creation, the number of followers and friends and the ratio of tweets having URLs.

2) Relation feature based: rely upon more robust features like the distance and connectivity apparent in the Twitter graph.

3) The message feature based: focused on the lexical of messages.

In the recent scenario tremendous efforts are made for detecting suspicious URLs and number of detecting schemes has also been introduced. They may be executed in virtual machine honey spots such as honey monkey and wepawet by using static and dynamic crawlers. Here classification are in accordance of several features and including lexical features of URLs, URL redirections, DNS information and the HTML contents of the landing pages.

A. Concepts and goal

Our goal is to develop the suspicious URLs detection against conditional redirection .Because an attackers can use the mechanism of conditional redirections, to redirect the normal users into malicious landing pages. In which an attacker creates a long URL redirect chains that can be reduced by using URL shortening service, such as bit.ly and

t.co as well as the attackers own private redirection servers. By using the redirection server, the attackers redirect the normal visitors into malicious landing pages. The attackers then upload the tweets with the initial URL of the redirect chains to Twitter. Later, when a user or crawler visits the initial URL, they will be redirected to an entry point of the intermediate URLs that are associated with private redirection severs. These redirection server check the current user is the normal browsers or crawlers. If the current visitors seem to be a normal, the server visitors to a malicious landing page. If not, they will redirect the visitors to a benign landing page. Therefore, the attackers can selectively attack normal users while deceiving investigators.

B. Proposed system

To develop suspicious URL detection system for Twitter. As investigators, cannot fetch the content of malicious landing URLs, because attackers do not reveal them to users. Attackers cannot rely on the initial URLs, as they can generate a large number of different initial URLs by abusing URL shortening services. The attacker may reuse some of their redirection servers when creating their redirect chains because they do not have infinite redirection servers. While analyzing several correlated URL redirect chains including individual redirect chains, can find the entry point of the intermediate URLs , the chains and the tweet context information for discovering and creating several features and this can be utilized suspicious URLs classification .

To collect large number of tweets from Twitter public timeline and trained the statistical classifier using discovered features .This trained classifier demonstrates the efficacy of the detection of suspicious URLs the contribution of paper follows:

1) A new suspicious URL detection system for Twitter to detect the suspiciousness based on URL redirect chains correlations that are difficult to fabricate. The system uses the frequently shared URLs to find correlated URL redirect chains and to determine their suspiciousness in almost real time.

2) Among new features of detecting suspicious URLs, some have recently discovered and while others are variations of previously discovered features.

C. Anatomy of the system:

Data allocation:

The data allocation component has three subcomponents: the collecting tweets with URLs, crawling URL Redirections and Tweet queue. To collect tweets with URLs and their context information from the Twitter public timeline, this component uses Twitter Streaming APIs. Whenever this component obtains a tweet with a URL, it executes a crawling thread that follows all redirections of the URL and looks up the corresponding IP addresses. The crawling thread appends these retrieved URL and IP chains to the tweet information and pushes it into a tweet queue. Already seen, our crawler cannot reach malicious landing URLs when they use conditional redirections to evade crawlers. However, because our detection system does not rely on the features of landing URLs, it works independently of such crawler evasions.

Feature extraction:

The feature extraction component has three subcomponents: grouping of identical domains, finding entry point URLs, and extracting feature vectors. This component monitors the tweet queue to determine whether a sufficient number of tweets have been collected. Specifically, our system uses a tweet window instead of individual tweets. When more than w tweets are collected, it pops w tweets from the tweet queue. First, for all URLs in the w tweets, this component checks whether they share the same IP addresses. If several URLs share at least one IP address, it replaces their domain names with a list of domains with which they are grouped. For instance, when http://123.com/hello.html and http://xyz.com/hi.html share the same IP address, this component replaces these URLs with http://[‘123.com’,‘xyz.com’]/hello.html and http://[‘123.com’,‘xyz.com’]/hi.html, respectively. This grouping process enables the detection of suspicious URLs that use several domain names to bypass the blacklisting. Next, this component tries to find the entry point URL for each of the w tweets. First, it measures the frequency with which each URL appears in these tweets. It then discovers the most frequent URL in each URL redirect chain in the w tweets. The discovered URLs thus become the entry points for their redirect chains. If two or more URLs share the highest frequency in a URL chain, this component selects the URL nearest to the beginning of the chain as the entry point URL.

Finally, for each entry point URL, the component finds URL redirect chains that contain the entry point URL, and extracts various features from these URL redirect chains along with the related tweet information. These feature values are then turned into real-valued feature vectors.

When group domain names or find entry point URLs, ignore whitelisted domains to reduce false positive rates. Whitelisted domains are not grouped with other domains and are not selected as entry point URLs

Training:

The training component has two subcomponents: retrieval of account statuses and training of the classifier. Because of using an offline supervised learning algorithm, the feature vectors for training are relatively older than feature vectors for classification. To label the training vectors using the Twitter account status; URLs from suspended accounts are considered malicious whereas URLs from active accounts are considered

benign. Then periodically update our classifier using labeled training vectors.

Classification:

The classification component executes our classifier using input feature vectors to classify suspicious URLs. When the classifier returns a number of malicious feature vectors, this component flags the corresponding URLs and their tweet information as suspicious. These URLs, detected as suspicious, will be delivered to security experts or more sophisticated dynamic analysis environments for an in-depth investigation.

.

II. Related Works

D. K. Mc Grath and M. Gupta [4] says that Internet users billions of dollars a year of phishing. Utilizing various sources data sets that are collected in real-time and analyzing various aspects of phishers. The authors examined the anatomy and domains, registration of phishing domains and activation time, and machine used for hosting phishing sites. In this paper, it is well cleared that findings were used as heuristics infiltration of email of phishing-related and in the identifying suspicious domain registrations.

Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia[5] says that The online social networking a new web accesors plays dual role one is social networking and micro-blogging. Users normally communicate among themselves through publishing text-based messages and posts. Twitter has its own popularity it opens structures lead attracted a huge number of automated programs, like bots, which appear to be a double-edged sword. Huge amount of benign –tweets generated by legitimate bots delivering news and updating tweets, in the case malicious bots spread spam or malicious contents. More interestingly, in the middle between human and bot, there has emerged cyborg referred to either bot-assisted human or human-assisted bot. To assist the users, the interactor within, this paper rely on the classifying of human, bot and cyborg accounts on Twitter. They first conduct a set of large-scale measurements with a collection of over 500,000 accounts. They found difference among human, bot and cyborg in terms of tweeting behavior, tweet content, and account properties. Based on the measurement results, we propose a classification system that includes the following four parts: (1) an entropy-based component, (2) a machine-learning-based component, (3) an account properties component, and (4) a decision maker. It uses the combination of features extracted from an unknown user to determine the likelihood of being a human, bot or cyborg. Here the experimental evaluation demonstrates the efficacy of the proposed classification system.

S. Chhabra, A. Aggarwal, F. Benevento, and P. Kumara guru [6] says that the rapid growth rate of social media, accessibility and minimal in size attracted the cybercrime .Day by day the crime has gradually increasing is phishing. The ultimate aim of the phishers to steal the valuable personal and wealth information from users that can be misused for any type of fraudulent purposes. Even now efforts are made by the researchers and the industry has in the process of developing inevitable technique to identify the attack through instant messaging and with email, very few researchers have undergone for better understanding of phishing on online social media. Conveniently phisher use the application of URLs shortened services like Twitter .This review gives an outlook of phishing attack in this scenario. This related literature implies that URL shortness are used not only for space reducing purpose but also to hide identity too. Facebook, habbo, orkut are the social media that are competing e- commerce such as e-bay, pay ball in terms of focus and traffic of phishers. This study reveals to understand deeply in phishing strategy .According to the authors this is the first study that concludes phishing landscape using blacklisted phishing URL from phish tank, URLs strategy, bit.ly and cues from Twitter to track and identifying the effect of phishing in online social network.

In recent days, URL shortened have occupied and important position in the field of social media networking. Mostly the user used Twitters or Facebook to disseminate information by means of online social media such as Twitter or Facebook. Exchanges of large URLs provided by typical URLs. The shorter URLs are shared and misused by users via online social media, e-mail or other forms of electronic communication. If the user clicks on the shortened URL, this will automatically redirected to the underlying long URL. Shortened URLs can provide legitimate purposes, has many as possible like click tracking, that this can also serve illicit behavior such as fraud, deceit and spam. Although usage of URL shortened services today is ubiquitous, our research community knows little about how exactly these services are used. The authors provide the first insights into the planetary-scale of this problem. The results revealed the relevant for researchers and engineers have the thirst in better understanding of coming up phenomenon and dangers of spamming via URL shortened services [7].

III. Conclusion

A suspicious URL detection system for Twitter considers correlations of URL redirect chains extracted from number of tweets collected from Twitter public timeline and trained a statistical classifier using the discovered features. Because attackers use limited resources, their URL redirect chains usually share the same URLs. To discover several features that can be used to classify suspicious URLs by analyzing their tweet context information and the correlated URL redirect chains. The trained classifier is shown to be accurate.

IV. REFERENCES

[1] H. KwaK, C. Lee, H. Park, and S. Moon, "What is Twitter, a social network or a news media?" inProc. WWW, 2010

[2] D. Antoniades, I. Polakis, G. Kontaxis, E. Athanasopoulos, S. Ioannidis, E. 4.P. Markatos, and T. Karagiannis, "we.b: The web of short URLs," inProc. WWW, 2011.

[3] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," inProc. ACSAC, 2010.

[4] D. K. McGrath and M. Gupta, "Behind phishing: An examination of phisher modi operandi," inProc. USENIX LEET, 2008

[5] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Who is tweeting on Twitter: Human, bot, or cyborg?" inProc. ACSAC, 2010.

[6] S. Chhabra, A. Aggarwal, F. Benevento, and P. Kumara guru, "Phi.sh/$social: the phishing landscape through short URLs," in Proc. CEAS, 2011.

[7] F. Benevento, G. Magno, T. Rodrigues, and V. Almeida, "Detecting spammers on Twitter," in Proc. CEAS, 2010.

[8] J. Song, S. Lee, and J. Kim, "Spam filtering in Twitter using sender receiver relationship," inProc. RAID, 2011.

[9] Yang, R. Harkreader, and G. GU, "Die free or live hard? Empirical evaluation and new design for fighting evolving Twitter spammers," inProc. RAID, 2011.