Research Paper

Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

An Improved Technique for Detecting Suspicious Urls in Twitter Stream

Engineering

KEYWORDS :

Adithya.N.P. PG Scholar, Department of Computer Science, Vedavyasa Institute of Technology, University of Calicut, Kerala, India.

Ginnu George Assistant Professor, Department of Computer Science, Vedavyasa Institute of Technology, University of Calicut, Kerala, India.

ABSTRACT

Social networking sites have become very popular in recent years. Among these sites, Twitter is the fastest growing site. Because of its popularity, Twitter is prone to malicious tweets containing URLs for spam, phishing, and malware distribution. Conventional 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 or consume much time and resources. Conventional suspicious URL detection schemes utilize several features including lexical features of URLs, URL redirection, HTML content, and dynamic behavior. However, evading techniques such as time-based evasion and crawler evasion exist. This paper proposes an improved technique for detecting suspicious URLs in Twitter stream. 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. In order to discover correlated URL redirect chains using the frequently shared URLs and to determine their suspiciousness some methods are developed. Numerous tweets from the Twitter public timeline are collected and build a statistical classifier using them. Using these classifier phishing URLs are detected. Evaluation results show that this classifier accurately and efficiently detects suspicious URLs.

I. INTRODUCTION

Nowadays online social networking sites have an unavoidable role in our day to day life. Facebook, Twitter, Orkut are some of them. Among these sites Twitter is the fastest growing one than any other sites. Twitter [1] is a famous social networking and information sharing service that allows users to exchange tweets with their friends. Tweets are messages carrying 140 characters or less. When a user John, sends a tweet, it will be distributed to all of his followers who have registered John as one of their friends. Instead of distributing a tweet to all of his followers, John can also send a tweet to a specific twitter user Tom by mentioning this user by including @Tom in the tweet. Unlike status updates, mentions can be sent to users who do not follow John.

Twitter users share URLs with their friends usually by using URL shortening services [2]. In order to reduce the URL length since tweets can contain only a restricted number of characters. Some of the URL shortening services includes "bit.ly" and "tinyurl.com". "t.co" is the URL shortening service provided by twitter. Ease of information dissemination on Twitter and a large audience, makes it a popular medium to spread external content like articles, videos, and photographs by embedding URLs in tweets. However, these URLs may link to low quality content like malware, phishing websites or spam websites. Malware, short for malicious software, is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising. Recent statistics show that on an average, 8% tweets contain spam and other malicious content.

The popularity of Twitter also increases day by day. So the hackers also make use of this popularity in order to spread their malicious tweets. Tweets contain texts and http links. Earlier detection mechanisms were not efficient, but time consuming. The features used for the purpose of detection could be fabricated easily by an attacker. Therefore the problem is to provide security to twitter users by identifying malicious URLs from benign ones in real time.

So many techniques for detecting spam [3], [4], [5], [6] and suspicious URLs were introduced. Most of them are time and resource consuming. Warning bird[13] proposed by Sangho Lee and Jong Kim is a robust method compared to other existing systems which concerned with detection of suspiciousness in URLs. But it cannot detect phishing URLs. It works as an analytical tool rather than a detection system.

Instead of investigating the landing pages of individual URLs in each tweet, which may not be successfully fetched, correlations of URL redirect chains extracted from a number of tweets has to be considered. Because attacker's resources are generally limited and need to be reused, their URL redirect chains usually share the same URLs. The system is developed in such a way that it should rely on correlated URL redirect chains. Because correlated URL redirect chains use the frequently shared URLs which determines their suspiciousness and can be done in almost real time.

This paper mainly focuses on detecting phishing URLs in twitter stream. For this detection the technique makes use of a classifier which shows suspicious features values of URLs.

Major contributions of this research work are:

- Automatic realtime phishing detection mechanism for Twitter: There have been studies on phishing detection in emails and spam detection on Twitter, but, to the best of our knowledge, this is the only system which study on realtime detection and protection of phishing on Twitter.
- More efficient than plain blacklisting method: Our technique proves to be better than plain blacklist lookup which is the most common technique used for phishing detection.
- Develop a browser for real time detection system
- Provide a distributed architecture for detection of urls

II LITERATURE SURVEY

H.Kwak, C.Lee, H.Park, and S.Moon proposed a work in 2010 [1] which mainly focuses on Twitter, a microblogging service less than three years old, commands more than 41 million users as of July 2009 and is growing fast. Twitter users tweet about any topic within the 140-character limit and follow others to receive their tweets. Twitter offers an Application Programming Interface (API) that is easy to crawl and collect data. Twitter tracks phrases, words, and hashtags that are most often mentioned and posts them under the title of "trending topics" regularly. A hashtag is a convention among Twitter users to create and follow a thread of discussion by prefixing a word with a '#' character. Inorder to identify influentials on Twitter, the authors have ranked users by the number of followers and by PageRank and found two rankings to be similar.

III. PROPOSED SYSTEM

3.1 Motivation and Basic Idea

The aim of proposed system is to develop a suspicious URL detection system for twitter which is robust enough to protect against conditional redirections, also to detect phishing URLs from the suspicious URLs. Proposed system Collects the suspicious information from the various warningbird tool (various system) to perform the various machine learning mechanism on this collected information to get phishing URLs.

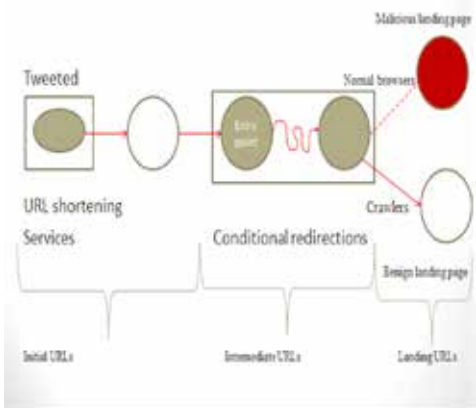

Fig.1 [13]: Conditional redirection

Consider a simple example of conditional redirections(fig.1), in which an attacker creates a long URL redirect chain using a public URL shortening service, such as *bit.ly* and *t.co*, as well as the attacker's own private redirection servers used to redirect visitors to a malicious landing page. The attacker then uploads a tweet including the initial URL of the redirect chain to Twitter. Later, when a user or a crawler visits the initial URL, he or she will be redirected to an entry point of the intermediate URLs that are associated with private redirection servers. Some of these redirection servers check whether the current visitor is a normal browser or a crawler. If the current visitor seems to be a normal browser, the servers redirect the visitor to a malicious landing page. If not, they will redirect the visitor to a benign landing page. Therefore, the attacker can selectively attack normal users while deceiving investigators.

So as investigators, we cannot fetch the content of malicious landing URLs, because attackers do not reveal them to us. We also cannot rely on the initial URLs, as attackers can generate a large number of different initial URLs by abusing URL shortening services. The attackers may reuse some of their redirection servers when creating their redirect chains because they do not have infinite redirection servers. Therefore, if we analyze several correlated redirect chains instead of an individual redirect chain, we can find the entry point of the intermediate URLs in these chains.

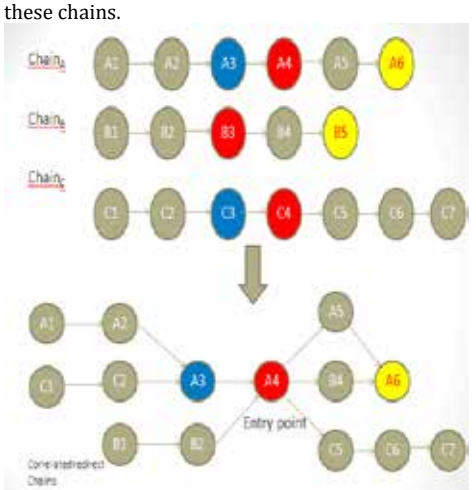

Fig.2[13]:Redirect chains and their correlation

Consider the three redirect chains shown in the top half of Fig.2, which share some URLs: A3 = C3, A4 = B3 = C4, and A6=B5 (similar colors show same URLs in fig.2). By combining the three redirect chains using these shared URLs, we can generate the correlated redirect chains (the bottom half of Fig. 2) that share the same entry point URL, A4 (because A4 is the most frequent URL in these chains). The correlated redirect chains show that the entry point has three different initial URLs and two different landing URLs, and participates in redirect chains that are six to seven URLs long. These are the characteristics of the suspicious URLs. Even the entry point, A4, does not allow our crawler to visit the latter URLs, we could infer that the chains are suspicious because it has many initial URLs for the same landing (entry point in reality) URLs. Therefore, this correlation analysis can help in detecting suspicious URLs even when they perform conditional redirections.

3.2 System Details

This system consists of mainly 4 components; Browser, Tweet Reader, Suspicious URL detection and Phishing detection.

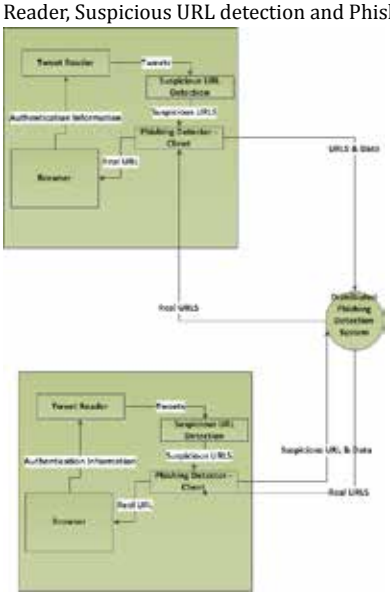

Fig.3: system architecture

Browser: Provide a web browser for viewing tweets and this act as a container for realtime detection of phishing tweets. When a user click on phishing tweet, this browser redirect to redirect to real site . Browser get this redirection information from Distributed phishing detection system through phishing detector client.

Tweet Reader: tweet reader reads from Twitter using Twiiter API.

Suspicious URL Detection: Block diagram for this detection system is shown in fig.4.

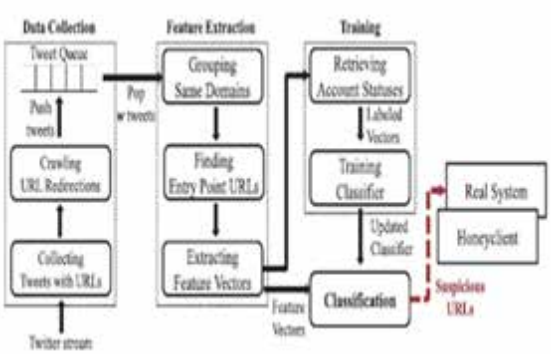

Fig.4[13]: System overview

This part of system includes 4 components; data collection, feature extraction, training, and classification.

Data collection: The data collection component has two subcomponents: The collection of tweets with URLs and crawling for URL redirections. 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.

Feature extraction: These components have three subcomponents: grouping identical domains, finding entry point URLs, and extracting feature vectors. This component monitors the tweet queue to check 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. Next, the 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 the w tweets. It then discovers the most frequent URL in each URL redirect chain in the tweets. The URLs thus discovered 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, this component finds URL redirect chains that contain the entry point URL, and extracts various features from these URL redirect chains and the related tweet information these feature values are then turned into real-valued feature vectors.

Training: The training component has two subcomponents: retrieval of account statuses and the training classifier. Because we use an offline supervised learning algorithm, the feature vectors for training are relatively old values than feature vectors for classification. To label the training vectors, use the Twitter account status; URLs from suspended accounts are considered malicious and URLs from active accounts are considered benign. It periodically updates our classifier by using labeled training vectors.

Classification: The 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 in-depth investigation.

3.3.2 Features Derived from Tweet Context Information:
The features derived from the related tweet context information are variations of previously discovered features. Our variations focused on the similarity of tweets that share the same entry point URLs.

Number of different sources: Sources are applications that upload the current entry point URL to Twitter. Attackers usually use the same source application, because of maintaining a number of different applications are difficult. If the number of different sources of an entry point URL that occurs n times is s, this feature can be normalized as s/n.

Number of different Twitter accounts: The number of different Twitter accounts that upload the current entry point URL can be used to detect injudicious attackers who use a small number of Twitter accounts to distribute their malicious URLs. If the number of Twitter accounts uploading an entry point URL that occurs n times is α, this feature can be normalized as α/n.

V. CONCLUSION

Previous suspicious URL detection systems are weak at protecting against conditional redirection servers that distinguish investigators from normal browsers and redirect them to the benign pages to block visit to malicious landing pages. In this paper, propose an improved technique for detecting suspicious URLs in Twitter stream. Unlike the previous systems, this system is robust when protecting against conditional redirection, because it does not rely on the features of malicious landing pages that may not be reachable. Distributed data analytic system evaluates the accuracy and performance.

VI. ACKNOWLEDGMENT

The authors gratefully acknowledge the support and facilities provided by Department of CSE, Vedavyasa Institute of Technology. Authors also extend their thanks to the Head of the Department Prof. Kavitha Murugesan for her immense help during the course of the project.

REFERENCE

[1] H. Kwak, C. Lee, H. Park, and S. Moon, "What Is Twitter, a Social Network or a News Media?" Proc. 19th Int'l World Wide Web Conf.(WWW), 2010. | [2] D. Antoniades, I. Polakis, G. Kontaxis, E. Athanasopoulos, S.Ioannidis, E.P. Markatos, and T. Karagiannis, "we.b: The Web ofShort URLs," Proc. 20th Int'l World Wide Web Conf. (WWW), 2011. | [3] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting Spammers onSocial Networks," Proc. 26th Ann. Computer Security ApplicationsConf. (ACSAC), 2010. | [4] A. Wang, "Don't Follow Me: Spam Detecting in Twitter," Proc.Int'l Conf. Security and Cryptography (SECRYPT), 2010. | [5] 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 DataMining (KDD), 2011. | [6] D. Canali, M. Cova, G. Vigna, and C. Kruegel, "Prophiler: A FastFilter for the Large-Scale Detection of Malicious Web Pages," Proc.20th Int'l World Wide Web Conf. (WWW), 2011. | [7] C. Whittaker, B. Ryner, and M. Nazif, "Large-Scale Automatic Classification of Phising Pages," Proc. 17th Network and the Distributed System Security Symp. (NDSS), 2010. | [8] K. Coronges, R. Dodge," The Influence Of Social Networks On Phishing | Vulnerability", 2011. | [9] M. Khonji, Y Iraaqi,"Enhancing Phishing Email Classifiers: A Lexical URL Analysis Approach", 2012. | [10]A. Kapravelos, M. Cova, C. Kruegel, and G. Vigna, "Escape from Monkey Island: Evading High-Interaction Honeyclients," Proc. Eighth Conf. Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), 2011. | [11] I. Mokube, M. Adams,"Honeypots: Concepts, Approaches and Challenges", 2009. | [12] P. Eckersley, "How Unique Is Your Web Browser?" Proc. 10th Privacy | Enhancing Technologies Symp. (PET), 2010. | [13]S. Lee, J. Kim,"WarningBird: A Near Realtime Detection System for Suspicious URLs in Twitter Stream," in IEEE Transactions on Dependable and Secure Computing, May/June 2013. |