ISSN 2395-1621

Detecting Suspicious URL's On Twitter

[#1]Jadhav Shraddha, [#2]Jadhav Indu, [#3]More Anuja

[1]jadhav.shraddha102@gmail.com
[2]indujadhav@gmail.com
[3]anujamore1907@gmail.com

[#123]TSSM's Bhivarabai College of Engineering and Research, Narhe, Pune-41

ABSTRACT

Social network services are increasing popular. Communicating with friends forms a social network that can be used to promptly share information with friends. In targeted attacks, social networking sites are often used to collect personal information and various attacks based on a specific user profile. Malware can be used to facilitate social relationship, sends messages containing malicious URL's. Because users are curious and trust on their friends, they typically click on malicious URL's without verification.

We are implementing such a system which will allow to detect the suspicious URL's on twitter account. So that it will help to users to maintain their security and to trustworthy sharing of the information on twitter accounts. This will help users to get prevented from suspicious links.

ARTICLE INFO

Article History

Received :4th March 2016

Received in revised form :

6th March 2016

Accepted :8th March 2016

Published online :

10th March 2016

Keywords : Malware, malicious URL's, suspicious URL's.

I.INTRODUCTION

Based on advances in information technology, websites offer various convenient web services such as information retrieval, chat rooms, Web 2.0-based services, blogs, albums, and multimedia sharing. Social network services (SNSs), such as Facebook, Twitter, and Myspace, have recently proliferated offering interactive information platforms that allow users to share and to interact.

Incident investigation reports have indicated that cybercrimes, such as targeted attacks or advanced persistent threats (APTs) often use SNSs to collect personal information and launch social engineering attacks. In other words, the convenience of SNSs facilitates potential cyber-attacks on SNS platforms. For example, a social-network-based worm spreads by attempting to steal account information and infect additional users by using a social engineering trick that sends malicious URL posts or emails. Because SNS users typically trust their friends, they are often breached by these worms, which rapidly spread through the friendship connections of victims.

II.LITERATURE REVIEW

Zhang et al. [8] proposed a content-based method for detecting phishing web sites, suggesting that phishing sites are created based on minor modifications from the authenticated sites and exhibit low page ranks in the Google search results. A set of heuristics was proposed based on domain name, lexical signatures of web links, and the HTML content of web pages. Five keywords were extracted from each web page based on TF-IDF (term frequency/inverse document frequency) algorithm and the Google search was applied to verify the website authenticity.

According to McGrath et al. [9], a brand name should appear in the URL of a web site. They collected and analyzed the URLs of phishing and non-phishing websites, determining that diverse countries host phishing sites, phishing domains are rarely hosted in their registered country, and phishing domains last approximately 3 days.

Fette et al. [8] extracted email features such as HTML tags, the number of links, use of JavaScript, and number of domains, to distinguish phishing emails by using a support vector machine (SVM). Bergholz et al. [3] proposed using email features namely, the structure of the

email body, web link properties, and a keyword list, which were generated using dynamic Markov chain training and class-topic models. Their results indicated that using these features improved the detection rate.

Abu-Nimeh et al. [3] chose the 43 most popular keywords as features and evaluated the performance level by using various machine learning classification algorithms.

Ma et al. [8] adopted semantic features from McGrath [9] and bag-of-words features from Kolari et al. [3]. In addition, Ma et al. addressed features specific to the hosted machine such as the IP address, WHOIS information, domain name, and geographic location. Machine learning algorithms namely, the native Bayesian theorem, Support Vector Machine (SVM), and logistic regression, were applied to evaluate the detection of suspicious URLs when using various combinations of features and data sets. Their subsequent studies [3] have yielded the similar conclusions, indicating that the features of URL semantics and host information are essential for identifying malicious web links when a suitable machine learning technique is applied. Based on the relevant literature, the characteristics of malicious web links are crucial when classifying suspicious URLs because links formerly sent through email are now being sent through social networks. A post that contains a suspicious URL is similar to an email that contains a phishing link. Spammers or attackers leverage social trust to propagate malicious posts in social networks. Therefore, the features of malicious web links and social relationship should be considered when attempting to detect suspicious web links.

Bayesian classification is based on probabilistic model specification. It employs naive Bayes assumptions: features that describe data instances are conditionally independent given the classification hypothesis. The maximum a posteriori estimation is computed by incorporating prior information. It is considered a generative approach to classification and has been successfully applied in medical diagnosis, text classification, and spam detection. In addition, Bayesian classification is insensitive to noisy data [1,3] and incremental improvement properties enhance the level of performance when the volume of data increases. These properties are suitable for use in virtual social environments. Therefore, Bayesian classification was used to establish the classification process in the proposed system.

III.PROBLEM DEFINITION

To implement the detection system to detect the suspicious URL's on twitter.

IV.PROPOSED METHODOLOGY

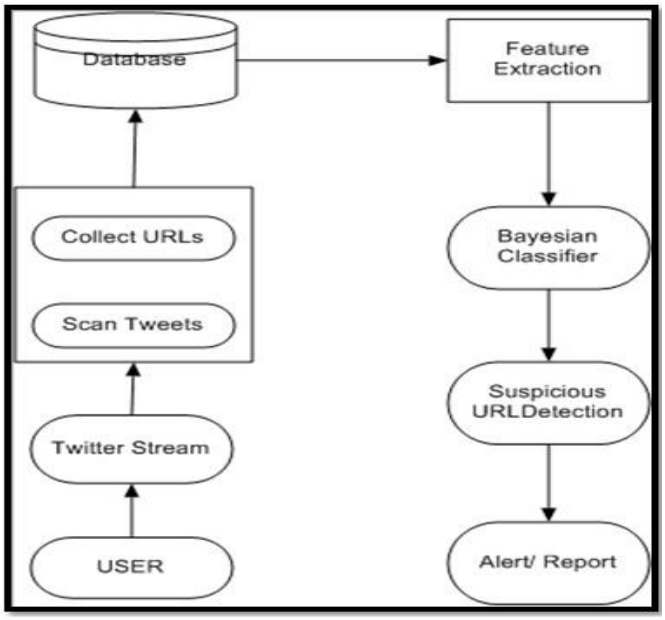

Fig 1. Architecture

Proposed system and overall process for detecting SNS-based malicious URLs. In the first module, data collection, posts are collected including time and content. Posts that lack URL information are considered benign. In the second module, feature extraction, the proposed features (elaborated in subsequent sections) are retrieved and a feature vector is constructed for classification. In the third module, the Bayesian classification model, posts are classified based on a pertained classification model.

REFERENCES

[1].Chia-Mei Chen , D.J. Guan, Qun-Kai Su "Feature set identification for detecting suspicious URLs using Bayesian classification in social networks" sciencedirect 2014.

[2]. Nupur S. Gawale , Nitin N. Patil " Implementation of A System To Detect Malicious URLs for Twitter Users" , International Conference on Pervasive Computing (ICPC) 2015.

[3]. Saeed Abu-Nimeh, Dario Nappa, Xinlei Wang, Suku Nair, "A comparison of machine learning techniques for phishing detection, in: Proceedings of the Anti-Phishing Working Group eCrime Researchers" Summit, 2007

[4]Jonell Baltazar, Joey Costoya, Ryan Flores, " The Real Face of Koobface: The Largest Web 2.0 Botnet Explained, Technical report", Trend Micro Threat Research, 2009.

[5] D.J. Guan, Chia-Mei Chen, Jia-Bin Lin, "Anomaly based malicious URL detection in instant messaging", in: Proceedings of the Joint Workshop on Information Security (JWIS), 2009.

[6]SPIEGEL Staff, Documents Reveal Top NSA Hacking Unit. Technical report, Spiegel Online, 2013. <http://www.spiegel.de/international/world/the-nsauses- powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>.

[7]Jaikumar Vijayan, "Dhs Warns of Spear-Phishing Campaign Against Energy Companies", Technical report, ComputerWorld, 2013. <http:// www.computerworld.com/s/article/9238190/DHS_warns_of_spear_phishing_campaign_against_energy_companies?taxonomyId=82>.

[8]Yue Zhang, Jason Hong, Lorrie Cranor, CANTINA "a content-based approach to detecting phishing web sites", in: Proceedings of the International World Wide Web Conference (WWW), 2007.

[9]D. Kevin McGrath, Minaxi Gupta, Behind phishing: "an examination of phisher modi operadi", in: Proc. of the USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2008.

[10]Ian Fette, Norman Sadeh, Anthony Tomasic, "Learning to detect phishing emails", in: WWW '07: Proceedings of the 16th International Conference on World Wide Web, 2007, pp. 649–656.

