Detection of Suspicious URL in Social Networking Site Twitter: Survey Paper

Jyoti D.Halwar
PG Student
Pune University

Sandeep Kadam
Assistant professor
D.Y.Patil College Of Engg.

Vrushali Desale
Professor
D.Y.Patil College Of Engg.

ABSTRACT
Twitter is very popular social networking site used by billions of people to share the information with each other. To communicate with each other over the long distance. But it also attracts the attackers in carrying out different attacks or get the information being shared by the twitter users. Twitter users can send the messages to each other in the form of tweets, that tweets have the size limitation of maximum 140 characters. So to share the web pages URL shorting is used. Attackers send the suspicious URLs in tweets and move the users to malicious pages. This paper presents a survey of different methods used to detect the suspicious URL (sites) in twitter stream. This paper also presents a WARNING BIRD APPLICATION. It is a near real time system to detect the suspicious URLs by classifying them.

Keywords
Suspicious URL, Twitter, URL redirection, conditional redirection, classification.

1. INTRODUCTION
The online social networking websites like Facebook, twitter, Myspace etc. are used by millions of people to communicate with each other though they're so much away from one another. Simply because of this on-line social networking site people can send their information, video, audio or even web pages also. This can be the terribly huge advantages of those sites and aim of the developer. In this on-line social networking website the net service providers are important component. They are connected with the user through some interface.

Twitter allows the users to send their messages in the form of tweets which has a size limitation of maximum 140 characters. This site is susceptible to malicious tweets containing URLs for spam, phishing, and malware distribution. Conventional Twitter spam detection schemes utilize account options like the magnitude relation of tweets containing URLs and also the account creation date, or relation options within the Twitter graph. These detection schemes are not feasible because it consume a lot of time and resources. Typical suspicious URL detection schemes utilize many options as well as lexical options of URLs, URL redirection, HTML content, and dynamic behaviour. However, evading techniques like time-based evasion and crawler evasion exist.

In twitter suppose 2 users Alice and Bob are communicated then Alice is tweeting his text within the form of tweet. As Bob is friend of Alice so that Bob obtaining all the post of Alice on his window. It means that Bob is follower of Alice. He will see the all post of Alice. Once more rather than causing to all or any the post there is additionally post may be causing to only 1 particular person by mentioning his or her name by using @. In this way twitter is functioning.

Now, on this social web site have some benefits additionally their some disadvantage. As we all know network is big half through this network the planet is thus closed and connected. While without network support this sites are not working properly. So, within the network large amount of people are sharing information among themselves. The some kinds of folks are needed to urge the info or it means that they hacked the user personal and confidential information and those folks we are able to say that offender. So, in the network common varieties of network attacks are there. Alice and Bob are connected, and if the Alice sends account details to Bob then at that point the third party person get that data then terribly large loss of the each Alice and Bob have to be compelled to survive. So, that within the network security is extremely vital for confidential information. This main dangerous and high problem is within the network. Still the researchers are working on them. They additionally survived from this situation. As a result of because the world is growing facilities are provided by the service suppliers is additionally growing but at the same time the offender additionally growing there ways are unceasingly modified for assaultive. So there is very huge challenged for the researchers to sight them and noise from rock bottom. This offender loss the user information, unceasingly irritating the user they also build the slow speed of user's system. Up till now we tend to perceive the offender that creates unwanted interrupt into the user work. Currently however they interrupt in users work. Thus there are numerous ways that of attacking spam, phishing and malware etc.

This paper, presents a WARNINGBIRD, a suspicious URL detection system for Twitter. This system investigates correlations of URL send chains extracted from many tweets. As a result of attackers have limited number of resources and attackers uses them again and again, this system collects various tweets from the Twitter public timeline and build a applied math classifier victimisation them. Analysis results show that this classifier accurately and expeditiously detects suspicious URLs. This WARNINGBIRD system is a near real time system for classifying suspicious URLs within the Twitter stream.

2. RELATED WORK
2.1 URL Shortening
Twitter's simplicity is one of the reasons the social media platform has become so popular. Status updates are limited to a maximum of 140 characters, but it's surprising how much information you can pack into such a small space. Inevitably, however, you'll want to share a link to some great content, and your tweet will tip past the 140-character limit. URL shorteners are tools which make long hyperlinks much shorter, enabling you to include useful links in your tweets without having to worry about going over the character limit. Here are five powerful URL shorteners to help you get the most out of your Twitter status updates. Some Sites listed below which are providing URL shortening services. Sites such as TinyURL.com, Bit.ly, Is.gd, Goo.gl, T.co provides some features like No account required Add Tiny URL to

your browser's toolbar, Hide affiliate links, free Customize your link, Integration with your Google Account, Detailed analytics, Automatic QR codes, Stability, Security.

By using this sites and taking advantages of features of these sites attackers are able to tweet the suspicious URL on Twitter

2.2 Examples of Suspicious Sites in Twitter

2.2.1 blackraybansunglasses.com

The blackraybansunglasses.com, is a suspicious site associated with spam tweets. It was first got captured in April 2011 and it was closed after August 2011. blackraybansunglasses.com has a page, redirect.php, which is responsible for conditionally redirection of users to random spam pages. This site evaluates the type of user whether it is visitors are normal browsers or crawlers. It redirects the normal browsers to random spam pages and redirects the crawlers to google.com stopping crawler from reaching to spam pages.

Another important point is that this site uses Normal Twitter API which is not used by advanced spammers because if they use this API. Spam detection system can differentiate the suspicious tweet and normal tweets. This site takes the advantage of this point.

2.2.2 24newspress.net

24newspress.net was first encountered at the end of June 2011 and it was closed after October 2011. This site does not perform conditional redirection to avoid investigation. Instead, it uses a number of IP addresses, domain names number of different shortened URLs and different Twitter accounts to distribute tweets to Twitter users. Furthermore, it misapplies the Mobile Twitter Web interface to convey its spam tweets.

3. EXISTING METHODS

3.1 Twitter Spam Detection

Many Twitter spam detection schemes are introduced. Most have targeted on a way to collect an oversized number of spam and non-spam accounts and extract the features that may effectively distinguish spam from nonspam accounts. To observe spam accounts, some schemes manually analyse the collected data, some use honey-profiles to lure spammers, some monitor the Twitter public timeline to observe accounts that post tweets with blacklisted URLs, and however others monitor Twitter's official account for spam news. Some systems considers account options together with the numbers of followers and friends, account creation dates, URL ratios, and tweet text similarities, which might be expeditiously collected however easily fictitious. Some systems targeted on relations between spam nodes and their neighboring nodes like a bi-directional link magnitude relation and betweenness centrality, as a result of spam nodes sometimes cannot establish strong relationships with their neighboring nodes. Some systems targeted on the grammar similarity of spam messages. Spammers, however, can easily fabricate grammar options of their spam messages.

3.2 Suspicious Uniform Resource Locator Detection

Many suspicious URL detection schemes are proposed. They will be classified into either static or dynamic detection systems. Some light-weight static detection systems concentrate on the lexical options of a URL like its length, the quantity of dots, or every token it has and additionally contemplate underlying DNS. Some static schemes focuses on hypertext mark-up language content and Java Script codes to observe drive-by transfer attacks. These systems cannot detect suspicious URLs with dynamic content like obfuscated JavaScript, Flash, and ActiveX content. Therefore, dynamic detection systems that use virtual machines and instrumented internet browsers for in-depth analysis of suspicious URLs are preferred. But yet, all of those detection systems should fail to observe suspicious sites with conditional behaviours.

3.3 ARROW: Generating Signatures to Observe DrivebyDownload

This system considers variety of related URL redirect chains to generate signatures of drive-by transfer attacks by using honeyclients to observe drive-by transfer attacks and collect logs of hypertext transfer protocol redirection traces from the compromised honeyclients. From these logs, it identifies central servers that square measure contained during a majority of the HTTP traces to a similar binaries and generates regular expression signatures exploitation the central servers' URLs. ARROW merges domain names with a similar science addresses to avoid science quick flux and domain flux. If honeyclients cannot access malicious landing pages attributable to conditional redirections, ARROW cannot acquire any hypertext transfer protocol traces.

4. WARNINGBIRD

Warning bird system works in 4 modules described as follows:

4.1 Data Collection

The data collection component works by using two subcomponents named gathering of tweets with URLs and crawling for URL redirections. Twitter Streaming APIs is used to collect tweets with url and its context. At whatever point this segment acquires a tweet with a URL, it executes a slithering string that takes after all re-directions of the URL and finds the comparing IP addresses. The slithering string attaches these recovered URL and IP binds to the tweet data and pushes it into a tweet line. As we have seen, crawler can't achieve malignant arriving Urls when they utilize restrictive redirections to sidestep crawlers.

4.2 Feature Extraction

The peculiarity extraction segment has three subcomponents: gathering of indistinguishable spaces, discovering entrance point Urls, and concentrating gimmick vectors. This segment screens the tweet line to figure out if a sufficient number of tweets have been gathered. Particularly, our framework utilizes a tweet window rather than individual tweets. this part checks whether collected have 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

Next, this part tries to discover the entrance point URL for each of the w tweets. In the first place, it measures the recurrence with which every URL shows up in these tweets. It then finds the most successive URL in every URL redirect chain in the w tweets. The found Urls subsequently turn into the entrance focuses for their redirect chains. In the event that two or more Urls offer the most elevated recurrence in a URL chain, this segment chooses the URL closest to the start of the chain as the passage point URL.

At last, for every passage point URL, the segment discovers URL redirect chains that contain the entrance point URL, and concentrates different peculiarities from these URL redirect chains alongside the related tweet data. These gimmick

qualities are then transformed into genuine esteemed peculiarity vectors.

When we bunch space names or discover entrance point Urls, we overlook whitelisted areas to decrease false positive rates. Whitelisted spaces are not assembled with different areas and are not chosen as entrance point Url. Our whitelisted area names incorporate the Alexa Top 1000 destinations, some prominent URL shortening locales, and a few areas that we have physically checked.

4.3 Training

The Training part has two subcomponents: recovery of record statuses and preparing of the classifier. Since we utilize a disconnected from the net administered learning calculation, the peculiarity vectors for preparing are generally more established than gimmick vectors for grouping. To name the preparation vectors, we utilize the Twitter account status; Urls from suspended records are viewed as vindictive though Urls from dynamic records are viewed as kindhearted. We occasionally overhaul our classifier utilizing marked preparing vectors

4.4 Classification

The classification part executes our classifier utilizing information characteristic vectors to group suspicious Urls. At the point when the classifier gives back various malevolent gimmick vectors, this segment hails the relating Urls and their tweet data as suspicious. These Urls, recognized as suspicious, will be conveyed to security specialists or more refined element investigation situations for a top to bottom examination.

5. CONCLUSION

Conventional suspicious URL detection systems are ineffective in their protection against conditional redirection servers that distinguish investigators from normal browsers and redirect them to benign pages to cloak malicious landing pages. WARNINGBIRD is robust when protecting against conditional redirection, because it does not rely on the features of malicious landing pages that may not be reachable. WARNINGBIRD is a near real time classification system to classify large samples of tweets from the Twitter public timeline to detect the suspicious URL in Tweets.

6. REFERENCES

[1] S. Lee and J. Kim, “WarningBird: Detecting suspicious URLs in Twitter stream,” in Proc. NDSS, 2012.

[2] H. Kwak, C. Lee, H. Park, and S. Moon, “What is Twitter, a socialnetwork or a news media?” in Proc. WWW, 2010.

[3] Antoniades, I. Polakis, G. Kontaxis, E. Athanasopoulos, S. Ioannidis, E. P. Markatos, and T. Karagiannis, “we.b: The web of short URLs,” in Proc. WWW, 2011.

[4] Klien and M. Strohmaier, “Short links under attack: geographical analysis of spam in a URL shortener network,” in Proc. ACM HT, 2012.

[5] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song, “Design andevaluation of a real-time URL spam filtering service,” in Proc. IEEE S&P, 2011.

[6] Whittaker, B. Ryner, and M. Nazif, “Large-scale automatic classification of phising pages,” in Proc. NDSS, 2010.

[7] M. Cova, C. Kruegel, and G. Vigna, “Detection and analysis of drive-by-download attacks and malicious JavaScript code,” in Proc. WWW, 2010.

[8] J. Zhang, C. Seifert, J. W. Stokes, and W. Lee, “ARROW: Generatingsignatures to detect drive-by downloads,” in Proc. WWW, 2011.

[9] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, “Beyond blacklists: Learning to detect malicious web sites from suspicious URLs,” in Proc. ACM KDD, 2009.