COMP4801 Final Year Project

A Smart Email Client to help user Identify Malicious URLs

Project Plan

Cheng Ngai Tong, Michael (3035270202)
Leung Tak Fung, Benson (3035377725)

Supervisor: Dr. Chim T W

Table of Contents

1. Introduction

Email spam is a serious problem in the cyber world. More than 50% of global mail traffic in 2019 are spam mails [1]. Many of those spam mails contain malicious URLs (Uniform Resource Locator). It is noticed that there are many url checkers available on the internet. However, one can hardly see email clients integrating the function of checking the safety of a URL. This project plans to build a smart email client which can help users to identify malicious url.

2. Background

Malicious URL is a URL that points to malicious website which hosts malicious content. Users visiting those malicious websites suffer from different kinds of attacks including drive-by download attacks and phishing [2]. In the drive-by download attack, malware is downloaded to the user's device, and hackers may control users' device to perform other cyber attacks [3]. Phishing sites are websites with appearance identical to other legitimate websites with the purpose of luring user's private information such as phone number and credit card number [4]. User may suffer monetary loss in phishing attacks.

There are hackers hiding the malicious URLs using a web service called URL shortening service. URL shortening is a web service that can create a short URL as an alias of any URL submitted by users. User visiting the short URL will be redirected to the page pointed by the original URL [5]. The purpose of this service is to convert long URLs to URL with reasonably short length for easy sharing. Some URL shortening service can also track the number of visitors of the short URL and provide the statistics to the link-creating user [6]. Hackers use this service to hide their malicious URLs, and users can hardly know whether the short URL will redirect them to malicious web site without accessing it [5]. It is found that there were short URLs linking to sites hosting different malicious contents [5].

There are different methods to detect a malicious URL.
One of the most common approaches to detect malicious URL is blacklisting. It is to store a list of malicious URLs reported by users or generated by other analysis techniques. A URL is considered malicious if it is in the list [7]. Blacklisting is easy to implement but it is infeasible to include all the malicious URL in the list. One needs to update the list from time to time in order to detect new URLs generated by hackers [4].
Another approach to detect malicious URL is the machine learning approach. This approach extracts feature representations from a large number of malicious URLs and benign URLs, and use them to train a prediction model, which can make predictions on new URLs [4]. Possible features include lexical features from the URL

string, the host of the resource pointed by the URL, HTML and JavaScript content, etc [4].

3. Objective And Scope

This project aims to build an email client with a robust classification system to identify malicious urls in emails so that the chance of user visiting a malicious site is reduced.

The email client will include the basic functions of an email client, including sending and receiving emails from email server.

Apart from the basic functions, the client will check all the urls in the email content. It will retrieve the destination of the urls if they are short URLs, useful data for classification such as title and description. The retrieved data will be displayed to user together as a preview of the page with a warning if the url is classified as malicious by the classification system.

In addition, the email client will be able to receive feedback from the user. User can report a URL in the email as malicious or benign. The classification will use the feedback from user to improve its accuracy in future classification.

To reduce the complexity of the classification problem, the classification will focus on the static features such as the lexical patterns in URLs and features including title, description in websites pointed by the URLs to do classification. The execution dynamics such as javascript execution in websites will not be taken into account.

4. Methodology

This project will be divided into two parts:

- Malicious URL Classification Model
  This project will use the machine learning approach to train a classification model. Logistic regression algorithm will be used to analyze the data. It is one of the common algorithms that solves binary classification problem. The Python library scikit-learn will be used to implement the classification model.

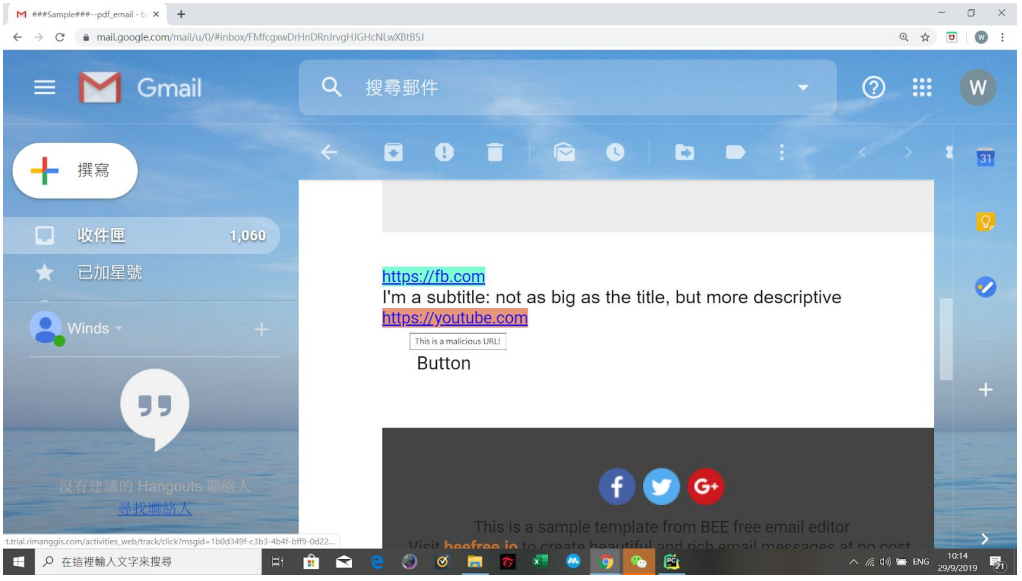
  List of malicious and benign URLs can be collected from data sets available on the internet. The list of URLs will be divided into a training set and a testing set.

  The URLs will be processed to extract features for classification. In early stage of the project, the model will focus on lexical features in the URL for simplicity. Later, more features such as the features in the HTML file pointed by the URL will be applied to improve the accuracy of the model.
  The training data set will be used to train the classification model.

After the training, the testing set will be used to test the accuracy of the trained model.

- Email Client that integrates the model
  This project aims to develop a web based smart email client, which allows every device to use it. Hence providing a comfortable user interface to attract users is also important.

  The project uses Python as backend, since Python has various library provided, including smtplib, which simplifies the step extracting data from other emails websites. In the early stage of the project, Gmail will be used for testing functions such as using backend to send and receive gmail through smtp. More kinds of email will be supported in the future. The email client first reads through the email contents and extracts all the <a> tag. After that it passes the url to the classification model and receive a true/false response. Finally it adds background color to the <a> tag, green for safe URL and red for malicious URL.



  For frontend, React JS is used to create websites, since it provides most functions for websites, such as animation and handle clicking, moving or dragging. Basic functions such as showing a list of emails or showing details of an email, will be available during early stage. Further improvements, for example seasonal theme, and allowing sending email functions, will be added in the future.

5. Division of Work

Person	**Task**

Cheng	Implementation and testing of the Malicious URL Detection Model
Leung	Implementation of the Email Client Integration of the Email Client and the Classification Model

6. Project Schedule

Date	**Task**
September 1 – 30	- Research on project topic, review the related works - Finish Detailed Project Plan and Project Web Page
October 1-31	- Further research on machine learning in malicious URL detection - Collect and process data available on the internet - Use case
November 1 - December 31	- Preliminary implementation on the classification model - Basic functions of email client (Receive and send email)
January 1 - February 2	- Testing and Refining the classification model - Preparation and Delivery of First presentation and Detailed interim report - Improvements on user interface
February 3 - March 31	- Further testing and refining of the classification model - Apply more features on the classification model to increase its accuracy - Create test cases for testing the client
April 1 - May 5	- Preparation for Delivery of Final report, Final presentation and Project exhibition
June 3	- Project competition

7. Conclusion

The spreading of malicious URL in spam mail is a serious problem in the cyber world and it causes monetary loss and leakage of sensitive information. This project

proposes to build an Email Client that integrates a malicious URL detection model which can lower the chances of user visiting malicious sites.

8. Reference

[1] M. Vergelis, T. Shcherbakova, and T. Sidorina , “Spam and phishing in Q2 2019,” Spam and phishing in Q2 2019, 15-May-2019. [Online]. Available: https://securelist.com/spam-and-phishing-in-q2-2019/92379/.
[2] D. R. Patil and J. Patil, “Survey on Malicious Web Pages Detection Techniques”, International Journal of u- and e-Service, Science and Technology. vol. 8, pp. 195-206, May 2015.
[3] M. Cova, C. Krügel and G. Vigna, “Detection and analysis of drive-by-download attacks and malicious JavaScript code”, Proceedings of the 19th International Conference on World Wide Web, WWW, Raleigh, North Carolina, 2010.
[4] D. Sahoo, C. Liu and C. H. Hoi, “Malicious URL Detection using Machine Learning: A Survey”, arXiv preprint arXiv:1701.07179, vol. 1
[5] S. Zanero, G. Stringhini, “Two years of short URLs internet measurement: security threats and countermeasures”, Proceedings of the 22nd international conference on World Wide Web, May 2013
[6] N. Nikiforakis, F. Maggi, G. Stringhini, M. Zubair Rafique, W. Joosen, C. Kruegel, F. Piessens, G. Vigna, S. Zanero, “Stranger danger: exploring the ecosystem of ad-based URL shortening services”, Proceeding WWW '14 Proceedings of the 23rd international conference on World wide web, April 07 - 11, 2014
[7] B. Eshete, A. Villafiorita, and K. Weldemariam, “BINSPECT: Holistic Analysis and Detection of Malicious Web Pages”, In: Keromytis A.D., Di Pietro R. (eds) Security and Privacy in Communication Networks. SecureComm 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 106. Springer, Berlin, Heidelberg