ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Techniques for Detecting Suspicious Facebook Applications

[1] B.Vijitha, [2]Dr.V.Sucharita, [3]CH. Niharika, [4]K. Mounika, [5]K.Tejaswini
[1][2][3][4][5] CSE College: Narayana Engineering College , Gudur.

Abstract: Suspicious applications refers that those applications which are under Facebook creates Malware in our personal computers, mobiles. By clicking on the URL of those suspicious face book applications it simply redirects to our personal web browser. It thefts our personal information and by viewing like the genuine applications and asks us for permission to install. By increasing of the more number of face book users day to day. Users who are under this can share, comment, and play games; due to this the hackers can easily recognize our problem. To overcome the above suspicious applications from face book. We introduced FRappE which detects the suspicious face book applications by creating extension to our web Browser. The FRappE performs verification on the URL of the suspicious applications and finally detects the suspicious applications.

Keywords-suspiciousapps, malware, social networks

INTRODUCTION

Social networks enable and develop third party applications to increase user experience on those in playing video games. Facebook generally consists more number of users who frequently use their accounts and also different types of apps are installed every day. Hackers have understood the many number of users are installing third party applications and makes business in this one. Hackers create malware producing third party applications and posted it on the face book. Due to the above problems suspicious app detecting technique can be determined the suspicious app detecting technique mainly Uses the tool frappe which evaluates different types of facebook users by their likes comments, the evaluator performs verification by looking the on demand and aggregate features. Facebook page keeper determines the suspicious applications by seeing the posts and likes of different users. Generally this paper we use two framework extensions frappe and frappe lite these two are used one is on client side and one is on admin side.Generally frappe is based on only on the on-demand features and frappe uses both on-demand and aggregate features. On-demand features consists of app name permission set and some other features .aggregate features include url's.Here the url plays a major role in detecting suspicious applications frappe meams facebook rigorous application evaluator, that is considered as browser extension for protecting our personal computers and mobiles from malware and virus content. This technique can be implemented by considering one user interface like facebok we have to create a face book environment like home page, friend requests ,sending messages, firstly user login if he/she have an account this is upto user after user login then internally admin login and performs frappe verification, by adding url to the malicious website.

LITERATURE SURVEY: We discuss how applications work on face book, and we outline the datasets that we use in this paper.

FACEBOOK APPS: Through face book applications, it enables third-party developers to offer various services to its users .installation of a Facebook application by a user does not involve the user downloading and executing an application binary. Which are unlike typical desktop and Smartphone applications? The user grants the application server only when a user adds a Facebook application to its profile permissions must be granted.

1) To access a subset of the information such as user's e-mail id listed on the user's Facebook profile

2) To perform certain actions with respect to the user such as attaining the ability to post on the user wall.These permissions are granted by the Facebook to application by handling an oauth2.0 token to the application server for every user who installs the application.

OPERATIONS OF MALICIOUS APPLICATIONS: Malicious Facebook applications typically operate as follows.

- Step 1: hackers convince users to install the app, usually with some fake promise (e.g., free i pads).
- step 2: once a user installs the app, it redirects the user to a web page where the user is requested to perform tasks, such as completing a survey, again with the lure of fake rewards.
- step 3: the app thereafter accesses personal information (e.g., birth date) from the user's profile, which the hackers can potentially use to profit.
- step 4: the app makes malicious posts on behalf of the user to the user's friends to install the same app (or some other malicious app, as we will see later).

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

WARNINGBIRD: Detecting Suspicious URLs in Twitter Stream: Twitter can suffer from malicious tweets containing suspicious URLs for spam, phishing, and malware distribution. Previous Twitter spam detection schemes have used account features such as the ratio of tweets containing URLs and in the Twitter graph. Malicious users, however, can easily fabricate ac-count features. Moreover, the account creation date, or relation features extracting relation features from the Twitter graph is time and resource consuming. Previous suspicious URL detection schemes have classified URLs using several features including lexical features of URLs, URL redirection, HTML content, and dynamic behavior. How-ever, evading techniques exist, such as time based evasion and crawler evasion. In this paper, we propose WARNINGBIRD, a suspicious URL detection system for Twitter. In-stead of focusing on the landing pages of individual URLs in each tweet, we consider correlated redirect chains of URLs in a number of .We focus on these shared resources to detect suspicious URLs. We have collected a large number of tweets from the Twitter public timeline and trained a statistical classifier with features derived from correlated URLs and tweet context information. Our classifier has high accuracy and low false positive and false-negative rates. We also present WARNINGBIRD as a real-time system for classifying suspicious URLs in the Twitter.

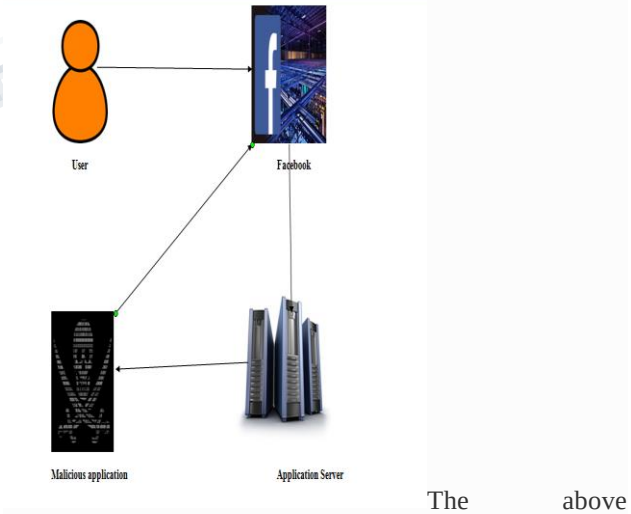
Detection of Malicious URLs by Correlating the Chains of Redirection in an Online Social Network (Twitter)s: Twitter is prone to malicious tweets containing URLs for spam, phishing, and malware distribution. Conventional Twitter spam detection schemes utilize account features such as the ratio of tweets 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 behaviour. However, evading techniques such as time-based evasion and crawler evasion exist. In this paper, we propose WARNINGBIRD, a suspicious URL detection system for Twitter. Our 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. We develop methods to discover correlated URL redirect chains using the frequently shared URLs and to determine their suspiciousness. We collect numerous tweets from the Twitter public timeline and build a statistical classifier using them. Evaluation result that show our classification accurately and efficiently detects suspicious URLs.

Privacy in Social Online Networks

Online social networks have become an important part of the online activities on the web and one of the most influencing media. Unconstrained by physical spaces, online social networks offer to web users new interesting means to communicate, interact, and socialize. While these networks make frequent data sharing and inter-user communications instantly possible, privacy-related issues are their obvious much discussed immediate consequences. Although the notion of privacy may take different forms, the ultimate challenge is how to prevent privacy invasion when much personal information is available. In this context, we address privacy-related issues by resorting to social network analysis and link mining techniques. We first describe the fundamental of social networks, their common representations, and the main motivations associated with their use. Afterwards, we particularly show how privacy attacks can build on social network analysis and link mining techniques to reveal user-sensitive information. The chapter concludes with a discussion of some open challenges to address in future privacy-related works.

METHODOLOGY

ARCHITECTURE:



The above architecture generally explains about the structure of the system. In this architecture the user sent a request to the Facebook to accept its request; the Facebook sends the acknowledgement to the user that it is accepting the request. Facebook redirects to the application server when there is a malware the information is theft by the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

suspicious user and suspicious hackers post on user wall. By posting on the user wall it can be shared and liked by more number of people.

GENERAL GRAPHS ABOUT INFORMATION:

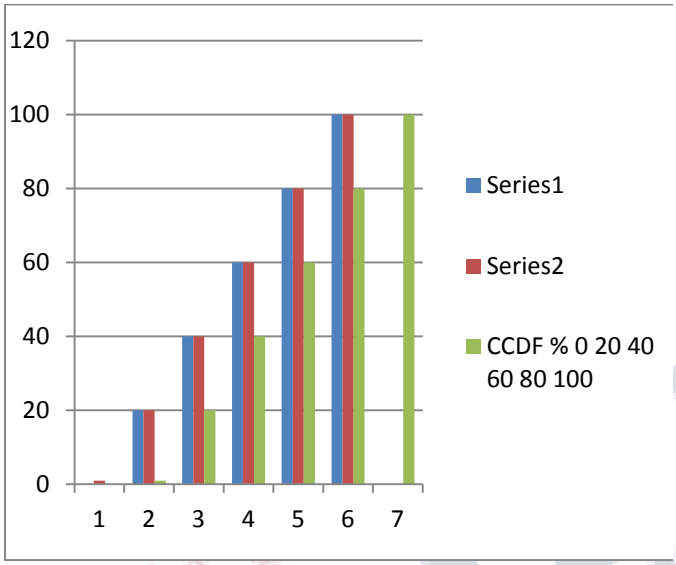


Fig: Distribution of no. of permissions requested by apps

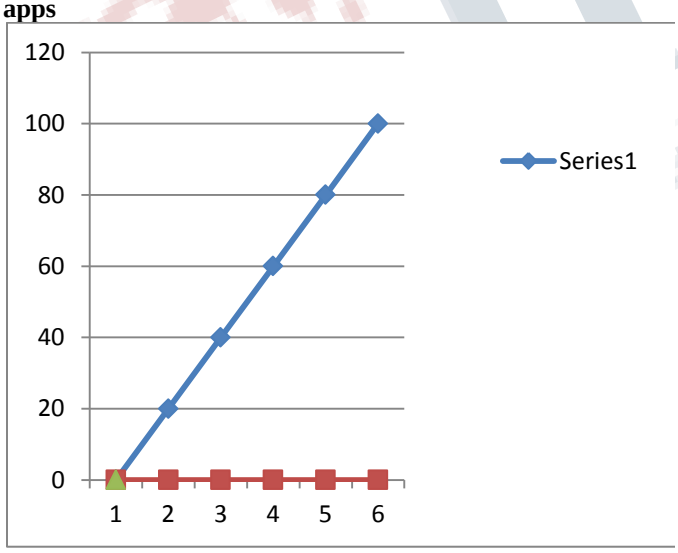


Fig: Accessing information from the profile.

Ubiquity of suspicious apps:

- We find that 55% of suspicious posts were flagged by MyPageKeeper was posted by suspicious applications.
- 60% of suspicious applications get more than hounded thousand clicks on the URL they post.
- Based on the survey 64% of the clicks were received for the experiment-"What is the good thing about you?"
- We use monthly active user's metrics to determine such applications in face book.
- Across the posts made by the 6372 suspicious apps in the sample dataset, we found that 3508 of these apps had posted 5600bit.ly URL's total.

Profiling Applications:

By the remarkable effect of the suspicious applications on face book we next go after to develop a tool that can identify suspicious applications. To understand and to build such a tool for identifying the suspicious and original applications we are going to compare the suspicious and original applications with respect to various features. There are two types of features:

1. On-demand features
2. Aggregate features.

1. On demand features: The on demand features associated with an application includes the features that one can obtain the on demand application ID. This includes application name, description, permission set, category and company.

a)Application Summary: We will compare both the suspicious and original apps with respect to the attributes of apps summary like app name and description. Description and company are the attributes with 140 characters and category can be selected from a Facebook list namely games, news etc…..Malicious applications have less description about application compared to the original application.

b) Permission Sets: Suspicious applications requires only one permission from users whereas original application requires more permissions to access the data such as gender, friend lists, e-mail. To detect suspicious application we can also detect by permission set.

c) Redirect URI: Suspicious applications redirect users to domains with poor repute.

d) Client ID in installation of App URL: Mostly, 80% suspicious apps are with the same client ID of original app So Facebook redirects and fetches the user to a URL that encodes the parameters in the URL.

Posts in App Profile: Almost all suspicious apps do not have posts in their profiles.

2. AGGREGATE FEATURES: Aggregate features are worked by taking the entities like Mypagekeeper.Here we

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

consider two features namely app name and URL's that are posted by an application.

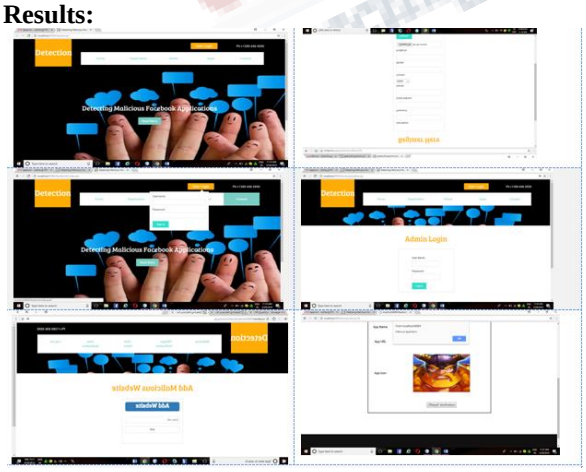
a)App name:80% of suspicious applications have an app name identical to other suspicious application.

b) External link to post ratio: Suspicious application frequently posts links pointing to domains outside of face book where as original apps rarely do so.

DETECTING SUSPICIOUS APPS: It is analyzed by different characteristics of suspicious and benign apps; we use these features to develop efficient techniques to identify suspicious Facebook applications. We have two types of suspicious app classifier like FRAppE&FRAppELite.

1.FRappE: We consider Frappe—in suspicious app detecting the utilizes our aggregated features in additional to the on- demand features. This shows the two features that FRAppE use in additional to those used in FRAppE Lite, since the aggregated features for an app require a cross-user and cross-app views over time. In contrast to Frappe Lite, we vision that Frappe used by face book security application that protect a large population of user.We again conduct a 6 –fold cross validated with the complete dataset for various ratio of benign to suspicious apps . In this we find that, with a ratio of 8:1 in benign to suspicious apps, Frappe's additional features improve the accuracy to 99.6% as to compare to 99.1% with Frappe Lite. In further the true positive rate increases from 96.6% to 96.8%, and we do not have a signal false.New identifying suspicious apps **.**Next we are train Frappe's classifier on the entire sample dataset and use this classifier to identifying new suspicious apps. To do, we apply Frappe to the apps in our total dataset that are not in the sample dataset for these apps, we got lack of information as to whether they are suspicious apps. In the 98 608 apps that we tested in this experiment, 8222 apps were flagged as suspicious by Frappe

Results:



CONCLUSION:

In this paper we are going to detect suspicious apps by implementing FRappE verification. Before the verification process any one application that we considered is added to the malicious website. It is added after performing verification it detects suspicious application.

REFERENCES:

[1]. social media statistics for 2012. http: socialskinny.com/100-social-media-statistics -for-2012.

[2].11 Million Bulk email addresses for sale $90.http://www.allhomebased.com/BulkEmailAddresses.htm.

[3].Pr0file stalker: rogue Facebook application.https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_ pr0file_viewer_2012_4_4.

[4]. Goldman, "Facebook tops 900 million users,"2012[Online].Available:http://money.