ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Data Transfer Protocol for Controlling Malicious Data in OSN

M. Shalima Sulthana[1], Vempalli Sravani[2]

M.Tech(CSE)., Academic Assistant in IIIT RGUKT-RKVALLEY, IDUPULAPAYA,VEMPALLI, Kadapa, India[1]

M.Tech(CSE), Academic Assistant in IIIT RGUKT-RKVALLEY, IDUPULAPAYA,VEMPALLI, Kadapa, India[2]

ABSTRACT: Facebook applications are one of the reasons for Facebook attractiveness. Unfortunately, numerous users are not aware of the fact that many malicious Facebook applications exist. Online social media services like Facebook witness an exponential increase in user activity when an event takes place in the real world. This activity is a combination of good quality content like information, personal views, opinions, comments, as well as poor quality content like rumours, spam, and other malicious content. Although, the good quality content makes online social media a rich source of information, consumption of poor quality content can degrade user experience, and have inappropriate impact in the real world. In addition, the enormous popularity, promptness, and reach of online social media services across the world makes it essential to monitor this activity, and minimize the production and spread of poor quality content. Multiple studies in the past have analysed the content spread on social networks during real world events. However, little work has explored the Facebook social network. Two of the main reasons for the lack of studies on Facebook are the strict privacy settings, and limited amount of data available from Facebook, as compared to Twitter. With over 1 billion monthly active users, Facebook is about times bigger than its next biggest counterpart Twitter, and is currently, the largest online social network in the world. In this literature survey, we review the existing research work done on Facebook, and study the techniques used to identify and analyse poor quality content on Facebook, and other social networks. We also attempt to understand the limitations posed by Facebook in terms of availability of data for collection, and analysis, and try to understand if existing techniques can be used to identify and study poor quality content on Facebook.

KEYWORDS: Facebookapps, malicious, Online Social Networks, spam.

1. INTRODUCTION

Online Social Networks (OSN's) enable and inspire third-party applications (apps) to enhance the user experience on these platforms like FaceBook, Twitter. Interesting or entertaining ways of communicating among on-line friends and diverse activities such as playing games or listening to songs are examples of such enhancements. For example, Facebook provides developers an API [2] that facilitates app integration into the Facebook user experience. There are 500K apps available on Facebook [3], and on average, 20M apps are installed every day [1]. Further-more, many apps have acquired and maintain a really large user database. It has been observed that FarmVille and CityVille apps have 26.5M and 42.8M users to date.

Recently, hackers and malicious users have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications [4]–[6]. Malicious apps can provide a lucrative business for hackers, given the status of OSN's, with Facebook leading the way with 900M active users [7]. There are many ways that hackers can benefit from a malicious app:

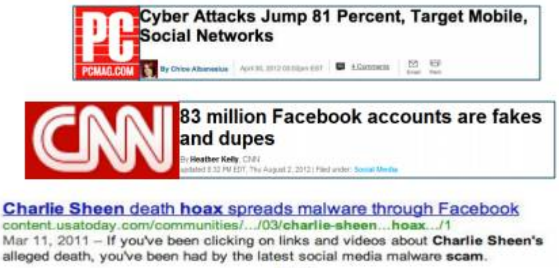
a) The app can reach large number of users and their friends to spread spam.
b) The app can obtain users personal information such as e-mail address, home town, and gender, and
c) The app can "reproduce" by making other malicious apps popular.

DOI: 10.15680/IJIRCCE.2017. 0502090

In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day [8].

Despite the above worries, today a user has very limited information at the time of installing an app on his Facebook profile. In other words, the problem is the following: Given an app's identity number (the unique identifier assigned to the app by Facebook), can we detect if the app is malicious? Currently, there is no commercial service, publicly available information, or research-based tool to advise a user about the risks of an app. Malicious apps are widespread and they easily spread, as an infected user jeopardizes the safety of all its friends. So far, the researches has been done regarding spam and malware on Facebook which has focused on detecting malicious posts and social spam campaigns [9]–[11]. At the same time, in a seemingly backwards step,

Facebook has dismantled its app rating functionality. A recent study has shown how app authorizations correlate to privacy risks of Facebook apps. Finally, there are some community based feedbacks driven efforts to rank applications, such as WhatApp? [12]; though these could be very powerful in the future, so far they have received little acceptance. The Fig.1 shows how the social malware is rampant on Facebook.



Cyber Attacks Jump 81 Percent, Target Mobile, Social Networks

By Chloe Albanesius | April 30, 2012 03:50pm EDT | 4 Comments | Email Print

83 million Facebook accounts are fakes and dupes

By Heather Kelly, CNN
updated 8:32 PM EDT, Thu August 2, 2012 | Filed under: Social Media

Charlie Sheen death hoax spreads malware through Facebook
content.usatoday.com/communities/.../03/charlie-sheen...hoax.../1
Mar 11, 2011 – If you've been clicking on links and videos about Charlie Sheen's alleged death, you've been had by the latest social media malware scam.

Fig.1

II. RELATED WORK

1) Detecting and Characterizing Social Spam Campaigns Authors: Hongyu Gao, Jun Hu, Christo Wilson,Zhichun Li, Yan Chen, Ben Y. Zhao.

Description: Authors presented a primary study to calculate and analyze spam campaigns launched on online social networks. They calculated a huge anonymized dataset of asynchronous "wall" messages in between Facebook users. System detected generally 200,000 malicious wall posts with embedded URLs, originating from more than 57,000 user accounts. Authors found that more than 70% of all malicious wall posts advertise phishing sites. To study the distinctiveness of malicious accounts, and see that more than 97% are compromised accounts, rather than "fake" accounts formed solely for the principle of spamming. Finally, when adjusted to the local time of the sender, spamming dominates actual wall post in the early morning hours when users are normally asleep.

2) Is this App Safe? A Large Scale Study on Application Permissions and Risk Signals

Authors: Pern Hui Chia, Yusuke Yamamoto, N.Asokan

Description: Third-party applications capture the attractiveness of web and platforms providing mobile application.

Many of these platforms accept a decentralized control strategy, relying on explicit user consent for yielding permissions that the apps demand. Users have to rely principally on community ratings as the signals to classify the potentially unsafe and inappropriate apps even though community ratings classically reflect opinions regarding supposed functionality or performance rather than concerning risks. To study the advantages of user-consent permission systems through a large data collection of Facebook apps, Chrome extensions and Android apps. The study confirms that the current forms of community ratings used in app markets today are not reliable for indicating privacy risks an app creates. It is found with some evidences, indicating attempts to mislead or entice users for granting permissions: free applications and applications with mature content request; "look alike" applications which have similar names as that of popular applications also request more permissions than is typical. Authors find that across all three platforms popular applications request more permissions than average.

3) Social Applications: Exploring A More Secure Framework
Authors: Andrew Besmer, Heather Richter Lipford,Mohamed Shehab, Gorrell Cheek
Description: OSNs such as Orkut, Facebook and others have grown-up rapidly, with hundreds to millions of active users. A new feature provided on several sites is social applications and services written by third party developers that supply additional functionality linked to a user's profile. However, present application platforms put users at risk by permitting the discovery of huge amounts of personal data and information to these applications and their developers. This paper generally abstracts main view and defines the current access control model gave to these applications, and builds on it to generate a more secure framework.

III.PROPOSED SYSTEM

Now a days, hackers have started taking advantage of the popularity of this third-party apps platform and deploying several malicious applications. These malicious apps can provide a lucrative business for hackers, given the popularity of online operating system, with Facebook leading the way with 900M active users. There can be enumeral ways that hackers can benefit from a malicious app, some of the them are:
(a) The app can reach huge number of users and their
friends to spread spam,
(b) The app can obtain users' personal information
such as email address,maritial status home town, and
gender, And
(c) The app can be re-created by making other
malicious application popular.

As a result of the above problems, there are many malicious apps spreading on Facebook every day. Because user has very limited information at the time of installing an app on his Facebook profile as user doesnot able to recognize the proposed app is malicious or not only the identity number Problems with existing system:

Hackers spread malwares and spam in facing using app. Many malicious apps are spreading on facebook. To develop FRAppE, a suite of resourceful and efficient classification techniques for detecting whether an app is malicious or not. To build FRAppE, use data from MyPageKeeper, a security app in Facebook that monitors the Facebook profiles of no of users near about 2.2 million of user. Analyze 111K apps that made 91 million posts over nine months. This is debatably the first comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and understanding malicious apps, and synthesizes this information into an effective and fast detection approach.

To detect malicious post MyPage-Keeper is used, a security app which was launched by Facebook [13] in June 2011. It monitors the Facebook profiles of 2.2 million users. It crawls user's wall post and news feed continuously and identifies malicious posts and notifies the infected users. Over 111K apps are analyzed that made 91 million posts over 9 months. This review paper presents a comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and understanding malicious apps and synthesizes this information into an effective detection approach.

MyPageKeeper primarily detects malicious posts in Facebook and notify victims. The Sample dataset contains apps for which the ground truth is, they are malicious or not. For collecting sample malicious apps, we use a heurestic: if a post is flagged by MyPageKeeper as malicious which is posted by an app, they app is malicious. Then same amount of benign apps are collected to make the comparison fair. Benign apps are those apps who are not part of malicious apps and also vetted by socialbaker.com, a website that collects app statistics. But the major enabling factor is malicious Facebook app.Fig.2 shows the news about Malicious Facebook app infections and the need for malicious facebook app Identification

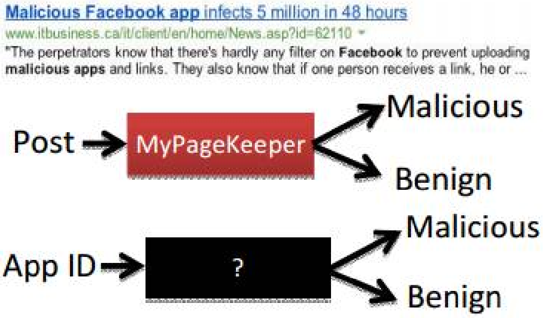
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

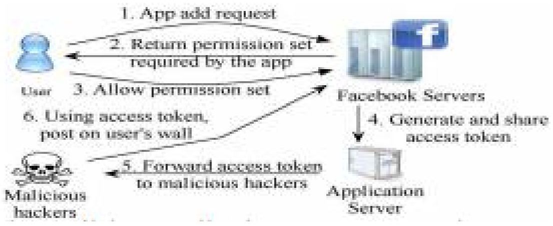
Vol. 5, Issue 2, February 2017



Malicious Facebook app infects 5 million in 48 hours
www.itbusiness.ca/it/client/en/home/News.asp?id=62110
"The perpetrators know that there's hardly any filter on Facebook to prevent uploading malicious apps and links. They also know that if one person receives a link, he or ...

Fig.2

The major problem statement is to identify malicious Facebook apps given an app ID? Facebook enables third-party developers to offer services to its users by means of Facebook applications. Unlike typical desktop and smart phone applications, installation of a Facebook application by a user does not involve the user downloading and executing an application binary. Instead, when a user adds a Facebook application to her profile, the user grants the application server: 1) permission to access a subset of the information listed on the user's Facebook profile (e.g., the user's e-mail ad-dress), and 2) permission to perform certain actions on behalf of the user (e.g., the ability to post on the user's wall). Facebook grants these permissions to any application by handing an OAuth 2.0 [14] token to the application server for each user who installs the application.



1. App add request
2. Return permission set required by the app
User
3. Allow permission set
Facebook Servers
6. Using access token, post on user's wall
4. Generate and share access token
5. Forward access token to malicious hackers
Malicious hackers
Application Server

Fig.3. Steps involved in hackers using malicious applications to get access tokens to post malicious content on victims'

Thereafter, the application can access the data and perform the explicitly permitted actions on behalf of the user. Fig.3 depicts the steps involved in the installation and operation of a Facebook application. Operation 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 iPads).

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 lure the user's friends to install the same app (or some other malicious app).

This way the cycle continues with the app or colluding apps reaching more and more users. Personal information or surveys can be sold to third parties [15] to eventually profit the hackers.Malicious hackers make posts into compromised user's wall. Their friends see the post, click the link which leads to the malicious app installation page as shown in Fig.4.Once installed, they redirect users to different pages for collecting victims personal information and Make her complete surveys so that they can earn money. Once the app is installed, hackers get permission to post any time on the victims wall. So, they make the same post and appears victims friends news feed and thus the cycle repeats and the app spreads in Facebook

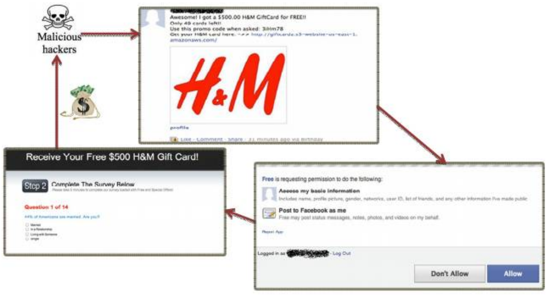

Malicious hackers
[redacted]
Awesome! I got a $500.00 H&M GiftCard for FREE!!
Only 49 cards left!!
Use this promo code when asked: 3iHm78
Get your H&M card here: --> http://giftcardz.s3-website-us-east-1.amazonaws.com/
H&M
profile
Like · Comment · Share · 31 minutes ago via Birthday
Free is requesting permission to do the following:
Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public
Post to Facebook as me
Free may post status messages, notes, photos, and videos on my behalf.
Report App
Logged in as [redacted] · Log Out
Don't Allow
Allow
Receive Your Free $500 H&M Gift Card!
Step 2 Complete The Survey Below
Question 1 of 14
44% of Americans are married. Are you?
Married
In a Relationship
Living with Someone
single

Fig 4:

V.CONCLUSION AND FUTURE

This paper is written as a survey of the base paper “Detecting Malicious Facebook Applications” by Sazzadur Rahman, Ting-Kai Huang, Harsha V. Madhyastha, and Michalis Faloutsos. Applications present convenient means for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of malicious apps and how they operate. In this paper, an analysis of a large corpus of malicious Facebook apps is observed and it is found that malicious apps differ significantly from benign apps with respect to several features. For example, malicious apps are much more likely to share names with other apps, and they typically request fewer permissions than benign apps. Leveraging our observations, FRAppE is developed, an accurate classifier for detecting malicious Facebook applications. We hope that Facebook will benefit from our recommendations for reducing the menace of hackers on their platform.

REFERENCES

[1] C. Pring, “100 social media statistics for 2012,” 2012 [Online].
[2] Facebook,PaloAlto,CA,USA, “Facebook Opengraph API,” [Online].
[3] “Wiki: Facebook platform,” 2014 [Online]. Available: http://en. wikipedia.org/wiki/Facebook_Platform
[4] “Pr0file stalker: Rogue Facebook application,” 2012 [Online].
[5] “Which cartoon character are you—Facebook survey scam,” 2012 [Online].
[6] G. Cluley, “The Pink Facebook rogue application and survey scam,” 2012 [Online].
[7] D. Goldman, “Facebook tops 900 million users,” 2012 [Online].
[8] HackTrix, “Stay away from malicious Facebook apps,” 2013 [Online].
[9] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos, “Efficient and scalable socware detection in online social networks,” in Proc. USENIX Security, 2012, p. 32.
[10] H. Gao et al., “Detecting and characterizing social spam campaigns,” in Proc. IMC, 2010, pp. 35–47.
[11] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary, “Towards online spam filtering in social networks,” in Proc. NDSS, 2012.
[12] “WhatApp? (beta)—A Stanford Center for Internet and Society Website with support from the Rose Foundation,” [Online].
[13] “MyPageKeeper,” [Online]. Available: https://www.facebook.com/ apps/application.php?id=167087893342260
[14] Facebook, Palo Alto, CA, USA, “Application authentication flow using OAuth 2.0,” [Online].
[15] “11 million bulk email addresses for sale—Sale price $90,” [Online].
[16] “bit.ly API,” 2012 [Online].
[17] Facebook, Palo Alto, CA, USA, “Permissions reference,” [Online].
[18] Facebook, Palo Alto, CA, USA, “Facebook developers,” [Online].
[19] “Web-of-Trust,” [Online]. Available: http://www.mywot.com/
[20] C.-C. Chang and C.-J. Lin, “LIBSVM: A library for support vector machines,” Trans. Intell. Syst. Technol., vol. 2, no. 3, 2011, Art. no. 27.
[21] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, “Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs,” in Proc. KDD, 2009, pp. 1245–1254.
[22] A. Le, A. Markopoulou, and M. Faloutsos, “PhishDef: URL names say it all,” in Proc. IEEE INFOCOM, 2011, pp. 191–195.
[23] Facebook, Palo Alto, CA, USA, “Facebook platform policies,” [On-line].

BIOGRAPHY

M. Shalima Sulthana(CSE) Working As Academic Assistant in IIIT RGUKT RKVALLEY,IDUPULAPAYA, VEMPALLI, Kadapa

V. Sravani working as Academic Assistant in IIIT RGUKT RKVALLEY, IDUPULAPAYA VEMPALLI, Kadapa