ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

DETECTING MALEFIC USING FRIAppE TOOLS

M.Gayathri[1], V.Indhu[2], K.Kalaiselvi[3], Mr.M.Karthikeyen[4] AP/CSE,
Department of Information Technology,
Bharathiyar Institute of Engineering for Women,Deviyakurichi,Salem.

Abstract

Many people installs a day, third-party apps are a major reason for the popularity and addictiveness of Social Networks. Intruders have realized the potential of using apps for spreading malware and spam. The problem is already known, as we find that at least 40% of apps in our dataset are malicious. To develop FRIAppE-(Facebook Rigorous Application Evaluator), we use information gathered by observing the posting behavior of 111K Social Networks apps seen across 500 million users on Social Networks. Finally, we explore the ecosystem of malicious Social Networks apps and identify mechanisms that these apps use to propagate. FRIAppE as a step towards creating an independent watchdog to secure Social Networks, so as to warn Social Networks users before installing apps.

Keywords: **Facebook Apps, Malicious Apps, profiling Apps, Online Social Networks**

I.INTRODUCTION

The favor of online social networks (OSN) is increasing day by day. The online communities created by OSN are a rapid growing on the web empowered by new modes of social interaction among people from around the globe.OSN are useful for keeping in touch with well-wishers and colleague, forming new contacts, research collaboration, information sharing, political campaigns.Some OSN are used for professional contacts, *e.g.* Focus and PartnerUp, where a user can discover business connections, while others, such as Facebook,Whatsapp and Twitter are friendship focused and are primarily used for communication, images and video sharing and divertissement .*AntisocialNetworks*, that is platforms for malicious and illegal activities like DDoS intrusion, malicious propagation, spamming, privacy violations, disk compromise,and the rest. OSN have some genuine properties that make them optimal for injustice by an antagonist: (i) a very large and highly dispersed user base,(ii) collection of users sharing the same social enthusiasm, developing trust relationships and searching access to the same resources, and (iii) platform openness for deploying malicious applications that lure users to install them.All these characteristics give attackers the

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

opportunity to massively manipulate Internet users and push them to perform reclusive acts against the rest of the Internet, without their knowledge. Apart from controlling social network users and driving them to launch intrusions against third parties, an antagonist can also misuse the users themselves In this paper we examine these properties, develop real exploits and analyze their impact.

II. PROBLEM STATEMENT

2.1 EXISTING SYSTEM

Intruders have started taking advantage of the familiar of this third-party apps platform and expanding malicious applications. Malicious apps can provide a profitable business for intruders, given the favour of Online Social Networks, with Facebook leading the way with 1.591 billion monthly active users. There are several ways that intruders can benefit from a malicious apps.Earlier, the research community has paid little attention to Online Social Network apps specifically. Most research related to spam and malicious on Social Network has focused on detecting malicious posts and social spam campaigns.

→Gao *et al.* analyzed posts on the walls of 500 million Facebook users and showed that 40% of links posted on Social Network walls are spam. They also presented approach to identify composed accounts and spam campaigns.

→Yang *et al.* and Benevenuto *et al.* advanced techniques to identify accounts of spammers on Twitter. Others have proposed a honey-pot-based approach to detect malware accounts on Online Social Networks.

→Yardi*et al.* analyzed behavioral patterns among spam accounts in Twitter.Chia *et al.*inspect hazard signaling on the privacy intrusiveness of Facebook apps and complete that current forms of community ratings are not predictable indicators of the privacy risks associated with an app.

2.2 DISADVANTAGES

(a) The app can reach many numbers of users and their friends to spread malwares
(b) The app can obtain users' private information such as email address, home town, mobile number and gender, and
(c) The app can "replicate" by making other malicious apps familiar.
(d) Previous system works concentrated only on classifying individual URLs or posts as spam, but not focused on identifying malware applications that are the main source of spam on Social Network

(e) Existing system works focused on accounts created by spammers in place of malicious application.

(f)Existing system provided only a high-level overview about malware to the Social Network graph and do not provide any analysis of the system.

III. PROPOSED SYSTEM

In this endeavor, we develop FRIAppE, a suite of valuable classification techniques for identifying whether an app is malware or not. To build FRIAppE, we use data from My Page Keeper, a security app in Online Social Network that monitors the Facebook profiles of 500 million users. We analyze 111K apps that made 1.091 billion posts over nine months. This is arguably the first exhaustive study focusing on malicious Social Network apps that focuses on quantifying, profiling, and forbearing malicious apps, and synthesizes this information into an effective detection avenue. Many features

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

used by FRIAppE, such as the favor of change URIs, the number of required permissions, and the use of different User IDs in app installation URLs, are fit to the evolution of intruders. Not using different User IDs in app installation URLs would limit the ability of intruders to instrument their applications to grow each other. We find that malware applications significantly differ from good applications with respect to two classes of features:

(i) On-Demand Features
(ii) Aggregation-Based Features.

We present two variants of our malicious app classifier— FRIAppE Lite and FRIAppE. FRIAppE Lite is a featherweight version that makes use of only the application features available on demand. Given a specific app ID, FRIAppE Lite slides the on-demand features for that application and evaluates the application based on these features in real time. FRIAppE—a malware app detector that utilizes our aggregation-based features in addition to the on-demand features.

IV.ARCHITECTURE DIAGRAM

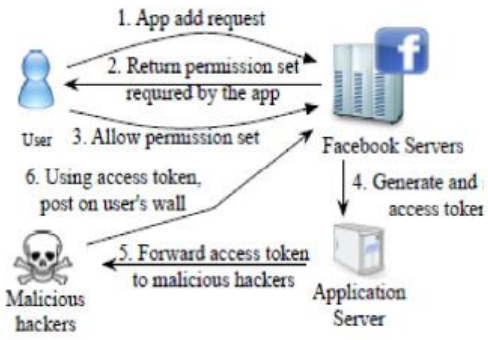

Fig: Overall Architecture Diagram

V. MODULE:

A module is a piece of a program. Programs are possessed of one or more independently developed modules that are not combined until the program is related. A single module can contain one or more methods.

Our Project Modules are given below:

- ➔ Detecting malware apps
- ➔ Malware apps ecosystem
- ➔ Apps collusion
- ➔ Hosting domain
- ➔ Cross promotion as a sign of malware intentions

5.1 DETECTING MALACIOUS APPS

To identify malware social network applications.We present two variants of our malware app classifier FRIAppE lite and FRIAppE. FRIAppE Lite is a featherweight version that makes use of only the application features available on demand. Given a specific app id, FRIAppE lite slide the on-demand feature for that application and evaluates the application based on these features in actual time.FRIAppE a malware app detector that utilizes our aggregation-based features in addition to the on-demand features.

5.2 MALICIOUS APP ECOSYSTEM

In this section, a conduct a forensics investigation on the malware app ecosystem to identify and quantify the techniques use in this cross promotion of malware apps. Background on app cross promotion: cross promotion among apps, which is refused as per facebook platform

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

policy, happens into different ways. The promoting app can post a URL that points directly to another app, or it can post a link that points to a redirection URL, which points dynamically to any of a set of apps. promotion graph characteristics: from the app promotion dataset the collected above, we construct a graph that has an random edge between any two apps that promote each other via direct or indirect promotion, we refer to this graph as the "the promotion graph".

5.3 APP COLLABORATION

We attempt to identify the major intruder groups involved in malware app collusion.

Posted url crusade: Two apps are part of a campaign if they redirect to the similar domain once they are installed by a user. We exclude apps that alter to apps.social networks.com

5.4 HOSTING DOMAINS

We investigate the hosting domain that enables redirection web sites.First,we find that most of the URLs in the posts are shortened ,and 85% of them use the bit.ly shortening service.we consider all the bit.ly URLs among our dataset of indirection links an resolve them to the full URL.we find that one-third of these URLs are hosted on amazonaws.com.Secon,we find that 45% of the domains hosting malware apps each host at least 60 different apps.This shows that intruder heavily reuse domains for hosting malware apps.

5.5 CROSS PROMOTION AS A SIN OF MALICIOUS INTENTIONS:

Thus far,we studied cross promotion among malware apps based on post marked as malicious by mypagekeeper.However, mypagekeeper may have failed to flag the post of many malicious apps. Therfore, here we study the prevalence of cross promotion simply by observing whether the post made by an app includes a url that points to another app. This enable us to discover a new set of malicious apps that we have failed to identify so far.

Our detection part is

1.Malware and beneficiant app profiles significantly differ.
2.The development of AppNets: apps collude at massive scale
3.Malicious intruders impersonate applications.
4.FRIAppE can detect malicious apps with 99.7% accuracy.

VI. CONCLUSION:

Applications gift a convenient means that for intruders to unfold malware content on social network. However, very little is known regarding the characteristics of malicious apps and the way they operate. In this work, employing a giant corpus of malicious Facebook apps discovered over a 9 month amount, we have a tendency to show that malicious apps dissent significantly from benign apps with applicability many options. For example, malicious apps are rather more doubtless to share names with other apps, and that they generally request fewer permissions than benign apps. Investment our observations, we have a tendency to developed FRAppE, an accurate classifier for detective work malicious Facebook applications. Most probably, we have a liability to highlight the emergence of AppNetslarge teams of tightly connected

All Rights Reserved © 2016 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

applications that promote every other. we are going to still dig deeper into this system of malicious apps on Facebook, and that we hope that Facebook can profit from our recommendations for reducing the menace of intruders on their platform.

REFERENCES

[1] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida. Detecting spammers on Twitter. In CEAS, 2010.

[2] A. Besmer, H. R. Lipford, M. Shehab, and G. Cheek. Social applications: exploring a more secure framework. In SOUPS, 2009.

[3] C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2, 2011.

[4] P. Chia, Y. Yamamoto, and N. Asokan. Is this app safe? A large scale study on application permissions and risk signals. In WWW, 2012.

[5] F. J. Damerau. A technique for computer detection and correction of spelling errors. Commun. ACM, 7(3), Mar. 1964.

[6] H. Gao, Y. Chen, K. Lee, D. Palsetia, and A. Choudhary. Towards online spam filtering in social networks. In NDSS, 2012.

[7] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. Detecting and characterizing social spam campaigns. In IMC, 2010.

[8] M. Gjoka, M. Sirivianos, A. Markopoulou, and X.

Yang. Poking facebook: characterization of osn applications. In Proceedings of the first workshop on Online social networks, WOSN, 2008.

[9] J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? In SOUPS, 2011.

[10] A. Le, A. Markopoulou, and M. Faloutsos. Phishdef: Url names say it all. In Infocom, 2010.

[11] K. Lee, J. Caverlee, and S. Webb. Uncovering social spammers: social honeypots + machine learning. In SIGIR, 2010.

[12] S. Lee and J. Kim. Warningbird: Detecting suspicious urls in twitter stream. In NDSS, 2012.

[13] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove. Analyzing facebook privacy settings: user expectations vs. reality. In IMC, 2011.

[14] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker. Beyond blacklists: learning to detect malicious web sites from suspicious urls. In KDD, 2009.

[15] A. Makridakis, E. Athanasopoulos, S. Antonatos, D. Antoniades, S. Ioannidis, and E. P. Markatos. Understanding the behavior of malicious applications insocial networks. Netwrk. Mag. of Global Internetwkg., 2010.

All Rights Reserved © 2016 IJARTET