International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October 2016

Dangerous Detection Applications Facebook

[1]SHAIK SAJEEDA, [2]P NAGESWARA RAO

[1] PG Scholar , Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206.

[2]Assistant Professor, Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206

ABSTRACT-With 20 million installs a day, third-party apps are a major reason for the popularity and addictiveness of Facebook. Unfortunately, hackers have realized the potential of using apps for spreading malware and spam. The problem is already significant, as we find that at least 13% of apps in our dataset are malicious. So far, the research community has focused on detecting malicious posts and campaigns. In this paper, we ask the question: Given a Facebook application, can we determine if it is malicious? Our key contribution is in developing FRAppE—Facebook's Rigorous Application Evaluator—arguably the first tool focused on detecting malicious apps on Facebook. To develop FRAppE, we use information gathered by observing the posting behavior of 111K Facebook apps seen across 2.2 million users on Facebook.

1 INTRODUCTION

What Is A Social Network?

Wikipedia defines a social network service as a service which "focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software."

A report published by OCLC provides the following definition of social networking sites: "Web sites primarily designed to facilitate interaction between users who share interests, attitudes and activities, such as Facebook, Mixi and MySpace."

What Can Social Networks Be Used For?

Social networks can provide a range of benefits to members of an organisation:

Support for learning: Social networks can enhance informal learning and support social connections within groups of learners and with those involved in the support of learning.

Support for members of an organisation: Social networks can potentially be used my all members of an organisation, and not just those involved in working with students. Social

networks can help the development of communities of practice.

Engaging with others: Passive use of social networks can provide valuable business intelligence and feedback on institutional services (although this may give rise to ethical concerns).

Ease of access to information and applications: The ease of use of many social networking services can provide benefits to users by simplifying access to other tools and applications. The Facebook Platform provides an example of how a social networking service can be used as an environment for other tools.

2.PREVALENCE OF MALICIOUS APPS

The driving motivation for detecting malicious apps stemsfrom the suspicion that a significant fraction of malicious posts on Facebook are posted by apps.We find that 53% of malicious posts flagged byMyPageKeeper were posted by malicious apps. We further quantify the prevalence of malicious apps in two different ways. *60% of malicious apps get at least a hundred thousand clickson the URLs they post*.We quantify the reach of malicious apps by determining a lower bound on the number of clicks on the links included in malicious posts. For each malicious app in our D-Sample dataset, we identify all bit.ly URLs in posts made by that application.We focus on bit.ly URLs since bit.ly offers an API [22] for querying the number of clicks received by every bit.ly link; thus, our estimate of the number of clicks received by every application is strictly a lower bound.

3 EXISTING SYSTEM

So far, the research community has paid little attention to OSN apps specifically. Most research related to spam and malware on Facebook has focused on detecting malicious posts and social spam campaigns.

Gao *et al.* analyzed posts on the walls of 3.5 million Facebook users and showed that 10% of links posted on Facebook walls are spam. They also presented techniques to identify compromised accounts and spam campaigns.

Yang *et al.* and Benevenuto *et al.* developed techniques to identify accounts of spammers on Twitter. Others have proposed a honey-pot-based approach to detect spam accounts on OSNs.

Yardi *et al.* analyzed behavioral patterns among spam accounts in Twitter.

Chia *et al.*investigate risk signaling on the privacy intrusiveness of Facebook apps and conclude that current forms of community

ratings are not reliable indicators of the privacy risks associated with an app.

DISADVANTAGES OF EXISTING SYSTEM:

Existing system works concentrated only on classifying individual URLs or posts as spam, but not focused on identifying malicious applications that are the main source of spam on Facebook.

Existing system works focused on accounts created by spammers instead of malicious application.

Existing system provided only a high-level overview about threats to the Facebook graph and do not provide any analysis of the system.

4 PROPOSED SYSTEM:

In this paper, we develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from MyPage- Keeper, a security app in Facebook.

We find that malicious applications significantly differ from benign applications with respect to two classes of features: On-Demand Features and Aggregation-Based Features.

We present two variants of our malicious app classifier— FRAppE Lite and FRAppE.

FRAppE Lite is a lightweight version that makes use of only the application features available on demand. Given a specific app ID, real time.

FRAppE—a malicious app detector that utilizes our aggregation-based features in addition to the on-demand features.

ADVANTAGES OF PROPOSED SYSTEM:

The proposed work is arguably 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 detection approach.

Several features used by FRAppE, such as the reputation of redirect URIs, the number of required permissions, and the use of different client IDs in app installation URLs, are robust to the evolution of hackers.

Not using different client IDs in app installation URLs would limit the ability of hackers to instrument their applications to propagate each other.

5 MALICIOUS APPS ECOSYSTEM

Our analysis in Section III shows thatmalicious apps are rampanton Facebook and indicates that they do not operate in isolation. Indeed,we find thatmalicious apps collude at scale—many malicious apps share the same name, several of them redirect to the same domain upon installation, etc. These observed behaviors indicate well-organized crime, with a few prolific hacker groups controlling many malicious apps. A common way in which malicious apps collude is by having one app post links to the installation page of another malicious app. In this section, we conduct a forensics investigation on the malicious app ecosystem to identify and quantify the techniques used in this cross promotion of malicious apps.

6.CONCLUSION

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, using a large corpus of malicious Facebook apps observed over a 9-month period, we showed thatmalicious apps differ significantly from benign apps with respect to several features

7.REFERENCES

[1] C. Pring, "100 social media statistics for 2012," 2012 [Online]. Available:

[2] Facebook, Palo Alto, CA, USA, "Facebook Opengraph API," [Online]. Available: http://developers.facebook.com/docs/reference/api/

[3] "Wiki: Facebook platform," 2014 [Online]. Available: http://en. wikipedia.org/wiki/Facebook_Platform

[4] "Pr0file stalker: Rogue Facebook application," 2012 [Online]. Available: https://apps.facebook.com/mypagekeeper/?status=scam_report-_fb_survey_scam_pr0file_viewer_2012_4_4

[5] "Whiich cartoon character are you—Facebook survey scam," 2012 [Online]. Available: https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_whiich_cartoon_character_are_you_2012_03_30

[6] G. Cluley, "The Pink Facebook rogue application and: survey scam," 2012 [Online]. Available: http://nakedsecurity.sophos.com/2012/02/27/pink-facebook-survey-scam/

[7] D. Goldman, "Facebook tops 900 million users," 2012 [Online]. Available: http://money.cnn.com/2012/04/23/technology/facebookq1/index.htm

[8] R. Naraine, "Hackers selling $25 toolkit to create malicious Facebook apps," 2011 [Online]. Available: http://zd.net/g28HxI

[9] HackTrix, "Stay away from malicious Facebook apps," 2013 [Online]. Available: http://bit.ly/b6gWn5

[10] 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.

[11] H. Gao *et al.*, "Detecting and characterizing social spam campaigns," in *Proc. IMC*, 2010, pp. 35–47.

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

AUTHOR'S DETAILS:

SHAIK SAJEEDA

PG Scholar , Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206.

P NAGESWARA RAO

Assistant Professor, Department Of CSE. Gandhi Academy Of Technical Education, Ramapuram (kattakommu Gudem), Chilkur(M), Kodad, Telangana 508206