Detecting Malicious Attacks in Facebook Applications

N. Devender & R.Sandeep

[1] Assistant Professor, Department of CSE, Balaji Institute of Technology & science, Warangal District, Telangana, India.

[2] M.Tech Student, Department of CSE, Balaji Institute of Technology & science, Warangal District, Telangana, India

Abstract:

The Facebook virus is a dangerous computer worm that infects your system when you visit the social network.Once in the system, it helps cybercriminals invade Facebook's account and spread the same virus to their victim's contacts.In addition, it is often used to steal sensitive information from your computer, so you may lose important information, such as your bank details and password, when your computer has such a threat.Obviously, the Facebook virus is a destructive program designed specifically for malicious purposes.If you want to know how it is distributed, keep reading.

Keywords: Facebook Virus, FRAppE, Malicious apps.

1. Introduction:

Often the Facebook virus is posted via fake information that is full of malicious links.The design of these pieces of information makes people feel really tricky, it will provoke people's innate curiosity, let them click on these links.Once you click on such a link, the Trojan infects the system and begins its activity there.However, the Facebook virus may also come into your computer in these ways: When you agree to allow an illegal or hacking application to access your account or when you install a computer virus that stole a Facebook password, or if your password is too weak, Heart of people have the opportunity to hack your Facebook account.

2. Literature Survey:

Hackers have started taking advantage of the popularity of this third-party apps platform and deploying malicious applications. Malicious apps can provide a lucrative business for hackers, given the popularity of OSNs, with Facebook leading the way with 900M active users. There are many ways that hackers can benefit from a malicious app:

➢ 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 *etal.*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.

3. **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, FRAppE Lite crawls the on-demand features for that application and evaluates the application based on these features in real time.

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

4.1 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. System Model:

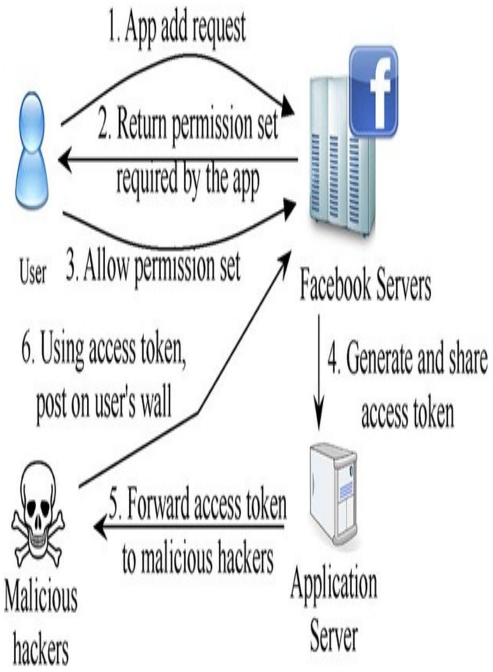
1. App add request
2. Return permission set required by the app
User
3. Allow permission set
Facebook Servers
6. Using access token, post on user's wall
4. Generate and share access token
5. Forward access token to malicious hackers
Malicious hackers
Application Server

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

The System model consists of User Facebook server and Application server. *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,free mobile phones etc).

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 someother malicious app, as we will see later).

5.1 Implementation Modules:

1. Malicious and benign app profiles significantly differ
2. The emergence of AppNets: apps collude at massive scale
3. Malicious hackers impersonate applications.
4.FRAppE can detect malicious apps with 99% accuracy

5.1.1. Malicious and benign app profiles significantly differ:

We systematically profile apps and show that malicious app profiles aresignificantly different than those of benign apps. A striking observationis the "laziness" of hackers; many malicious apps havethe same name, as 8% of unique names of malicious apps areeach used by more than 10 different apps (as defined by their appIDs). Overall, we profile apps based on two classes of features:(a) those that can be obtained on-demand given an application'sidentifier (e.g., the permissions required by the app and the postsin the application's profile page), and (b) others that require across-user view to aggregate information across time and acrossapps (e.g., the posting behavior of the app and the similarity ofits name to other apps).

5.1.2 The emergence of AppNets: apps collude at massive scale:

Weconduct a forensics investigation on the malicious app ecosystemto identify and quantify the techniques used to promote maliciousapps. The most interesting result is that apps colludeand collaborate at a massive scale. Apps promote other apps viaposts that point to the "promoted" apps. If we describe the collusionrelationship of promoting-promoted apps as a graph, we find1,584 promoter apps that promote 3,723 other apps. Furthermore,these apps form large and highly-dense connected components, Furthermore, hackers use fast-changing indirection: applicationsposts have URLs that point to a website, and the website dynamicallyredirects to many different apps; we find 103 such URLsthat point to 4,676 different malicious apps over the course of amonth. These observed behaviors indicate well-organized crime:one hacker controls many malicious apps, which we will call anAppNet, since they seem a parallel concept to botnets.

5.1.3 Malicious hackers impersonate applications:

We were surprisedto find popular good apps, such as 'FarmVille' and 'Facebookfor iPhone', posting malicious posts. On further investigation,we found a lax authentication rule in Facebook that enabledhackers to make malicious posts appear as though they came fromthese apps.

5.1.4 FRAppE can detect malicious apps with 99% accuracy:

Wedevelop FRAppE (Facebook's Rigorous Application Evaluator)to identify malicious apps either using only features that can beobtained on-demand or using both on-demand and aggregationbasedapp information. FRAppE Lite, which only uses informationavailable on-demand, can identify malicious apps with99.0% accuracy, with low false positives (0.1%) and false negatives(4.4%). By adding aggregation-based information, FRAppEcan detect malicious apps with 99.5% accuracy, with no falsepositives and lower false negatives (4.1%).

6. Conclusion and Future Work:

Applications present a convenient means for hackers to spreadmalicious content on Facebook. However, little is understood about the characteristics of malicious apps and how they operate. In thiswork, using a large corpus of malicious Facebook apps observedover a nine month period, we showed that malicious apps differsignificantly from benign apps with respect to several features. Forexample, malicious apps are much more likely to share names withother apps, and they typically request less permission than benignapps. Leveraging our observations, we developed FRAppE, an accurate classifier for detecting malicious Facebook applications.Most interestingly, we highlighted the emergence of AppNets—large groups of tightly connected applications that promote eachother. We will continue to dig deeper into this ecosystem of maliciousapps on Facebook, and we hope that Facebook will benefitfrom our recommendations for reducing the menace of hackers ontheir platform.

7. References:

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

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

[3] App piggybacking example. https://apps.facebook.com/mypagekeeper/?status =scam_report_fb_survey_scam_Converse_shoes _2012_05_17_boQ.

[4] Application authentication flow usingoauth2.0.http://developers.facebook.com/docs/authentication/.

[5] Bitdefender Safego. http://www.facebook.com/bitdefender.safgo.

[6] bit.ly API. http://code.google.com/p/bitlyapi/wiki/ApiDocumentation.

[7] Defensio Social Web Security. http://www.facebook.com/apps/application.php?id=177000755670.

[8] Facebook developers.https://developers.facebook.com/docs/appsonfacebook/tutorial/.

[9] Facebook kills App Directory, wants users to search for apps.http://zd.net/MkBY9k.

[10] Facebook Opengraph API. http://developers.facebook.com/docs/reference/api/.

[11] Facebook softens its app spam controls, introduces bettertools for developers. http://bit.ly/LLmZpM.

[12] Facebook tops 900 million users. http://money.cnn.com/2012/04/23/technology/facebook-q1/index.htm.

[13] Hackers selling $25 toolkit to create malicious Facebookapps. http://zd.net/g28HxI.

[14] MyPageKeeper. https://www.facebook.com/apps/application.php ?id=167087893342260.

[15] Norton Safe Web. http://www.facebook.com/apps/application.php?id=310877173418.

[16] Permissions Reference. https://developers.facebook.com/docs/ authentication/permissions/

[17] Pr0file stalker: rogue Facebook application.https://apps.facebook.com/mypagekeeper/?status=scam_report_fb_survey_scam_pr0file_viewer_2012_4_4.

[18] Selenium -Web Browser Automation.http://seleniumhq.org/.

[19] SocialBakers: The receipe for social marketing success.http://www.socialbakers.com/.[20] Stay Away From Malicious Facebook Apps.http://bit.ly/b6gWn5.

[21] The Pink Facebook -rogue application and survey scam.http://nakedsecurity.sophos.com/2012/02/27/pink-facebook-survey-scam/.

N. Devender is 2 years experienced Assistant Professor in the Department of Computer Science & Engineering, BALAJI INSTITUTE OF TECHNOLOGICAL SCIENCES-NARSAMPET, Warangal, India and his research area includes Cloud Computing , IoT, Data Mining , Network Security etc.,

R.Sandeep Currently doing M.Tech in Computer Science & Engineering at BALAJI INSTITUTE OF TECHNOLOGICAL & SCIENCES-NARSAMPET, Warangal, India. His research interests includes Cloud Computing, Network Security, Mobile Computing, etc,