Frappe Technique for Detecting Fb Malicious Application in OSN

MRS. SHAIK RUHI APSHA[1], MR. SHAIK JILANI BASHA[2]

[1]PG Scholar, Department of CSE, PACE Institute of Technology and Sciences,Vallur, Prakasam, Andhrapradesh, India

[2]Assistant Professor, Department of CSE, PACE Institute of Technology and Sciences,Vallur, Prakasam, Andhrapradesh, India

Abstract: With 20 million installs a day, third-party apps are a main reason for the reputation and addictiveness of Facebook. Unluckily, hackers have realized the potential of using apps for scattering malware and spam. The problem is already major, as we find that at least 13% of apps in our dataset are malicious to date, the research community has focused on detecting malicious posts and campaigns. In this paper, we ask the question: given a Facebook application, can we decide if it is malicious? Our key contribution is in developing FRAppE Facebook's Rigorous Application Evaluator arguably the first tool focused on finding 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. First, we identify a set of features that aids us distinguish malicious apps from benign ones. For example, we discover that malicious apps often share names with other apps, and they typically request fewer permissions than benign apps. Second, leveraging these distinguishing features, we demonstrate that FRAppE can identify malicious apps with 99.5% accuracy, with no false positives and a low false negative rate (4.1%). Finally, we explore the ecosystem of malicious Facebook apps and recognize mechanisms that these apps use to spread interestingly, we find that many apps collude and support each other; in our dataset, we find 1,584 apps enabling the viral propagation of 3,723 other apps through their posts. Long-term, we see FRAppE as a step towards creating an independent watchdog for app assessment and ranking, so as to warn Facebook users before installing apps.

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

I. INTRODUCTION

Online social networks (OSNs) empower and encourage 0.33-party applications (apps) to decorate the purchaser revel in on the ones levels. Such upgrades include charming or attractive techniques for offering amongst on-line companions and awesome carrying activities, for instance, playing recreations or tuning in to tunes. For example, Facebook gives engineers an API [2] that encourages utility becoming a member of into the Facebook patron encounter. There are 500K programs available on

Facebook [3], and all topics considered, 20M packages are brought every day Moreover, severa programs have acquired and keep up a truely large patron base. For example, FarmVille and City Ville programs have 26.5M and 42.8M customers to date. As of late, programmers have started out exploiting the ubiquity of this outsider packages stage and sending malevolent applications [4]–[6]. Malicious programs can supply a profitable commercial organization to programmers, given the prominence of OSNs, with Facebook the usage of the path with 900M dynamic customers [7]. There are sever a techniques that programmers can income via a malevolent utility: 1) the software can collect huge quantities of customers and their partners to unfold unsolicited mail; 2) the software can collect customers' non-public records together with e mail deal with, home metropolis, and gender; and three) the software can produce‖ through making specific malicious apps famous. To make subjects extra horrible, the association of malicious packages is stepped forward with the aid of prepared-to-rent toolkits beginning at $25 [8]. As such, there's purpose and opportunity, and consequently, there are numerous pernicious applications spreading on Facebook constantly [9]. Despite the above troubling patterns, nowadays a customer has pretty confined information at the season of introducing an software program software on Facebook. As such, the hassle is the accompanying: With 20 million installs a day, zero.33-birthday celebration programs area main purpose for the popularity and addictiveness of Facebook. Unfortunately, hackers have decided out the potential of the usage of Applications for spreading malware and direct mail. The problem is already considerable, as we discover that as a minimum 13% of applications in our dataset are malicious. So a protracted manner, the research community has targeted on detecting malicious posts and campaigns. In this project, Our key contribution is in

growing FRAppE— Facebook's Rigorous Application Evaluator— arguably the first device centered on detecting malicious programs on Facebook. To increase FRAppE, we use data accumulated through using looking the posting conduct of 111K Facebook packages seen across 2.2 million customers on Facebook. First, we apprehend a set of functions that assist us distinguish malicious programs from benign ones. For example, we discover that malicious programs regularly percentage names with unique programs, and that they normally request fewer permissions than benign packages. Most research diagnosed with unsolicited mail and malware on Facebook has targeted on distinguishing noxious posts and social direct mail campaigns [10]–[12]. In the meantime, in an seemingly in contrary stride, Facebook has disassembled its software application score usefulness as of overdue. A current-day art work examines how software program authorizations and group value determinations connect to safety risks of Facebook packages [13].

At long remaining, there are some company based completely input driven endeavors to rank programs, as an example, WhatApp? [14]; but the ones might be intense in a while, thus far they are becoming little choice. We speak about past artwork in extra detail in Section VIII. In this paper, we create FRAppE, a tough and speedy of gifted grouping strategies for spotting whether or not or not an utility is malignant or now not. To gather FRAppE, we employ facts from MyPageKeeper, a safety utility in Facebook [15] that presentations the Facebook profiles of .2 million clients. We take a look at 111K programs that made 90 one million posts extra than 9 months. This is arguably the essential thorough evaluation concentrated on malicious Facebook packages that spotlights on measuring, profiling, and comprehension noxious programs and integrates this facts into a powerful popularity method. Our art work makes the accompanying key commitments.

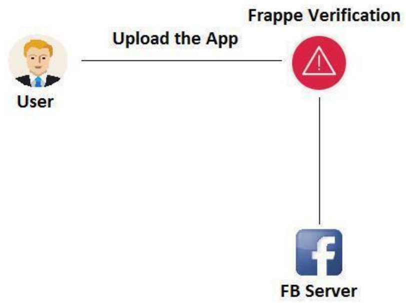


Fig: 1, Process of hackers using malicious apps.

II. BACKGROUND

We discuss how applications work on Facebook, and we out-line the datasets that we use in this paper.

A. Facebook Apps

Facebook enables third-party developers to offer services to its users by means of Facebook applications. Unlike typical desktop and smartphone 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). Face-book grants these permissions to any application by handing an OAuth 2.0 [17] token to the application server for each user who installs the application. Thereafter, the application can access the data and perform the explicitly permitted actions on behalf of the user. Fig. 2 depicts the steps involved in the installation and operation of a Facebook application.

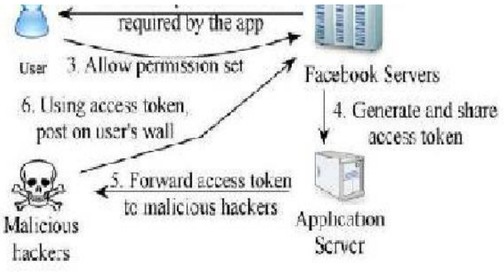

required by the app
User
3. Allow permission set
Facebook Servers
6. Using access token, post on user's wall
4. Generate and share access token
5. Forward access token to malicious hackers
Malicious hackers
Application Server

Fig. 2. Steps involved in hackers using malicious applications to get access tokens to post malicious content on victims' walls.

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, as we will see later).

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 [18] to eventually profit the hackers.

B. Our Datasets

The basis of our study is a dataset obtained from 2.2M Face-book users, who are monitored by MyPageKeeper [15], our security application for Facebook.[1]MyPageKeeper evaluates every URL that it sees on any user's wall or news feed to deter-mine if that URL points to social spam. MyPageKeeperclas-sifies a URL as social spam if it points to a Web page that: 1) spreads malware; 2) attempts to "phish" for personal infor-mation; 3) requests the user to carry out tasks (e.g., fill out sur-veys) that profit the owner of the Web site; 4) promises false rewards; or 5) attempts to entice the user to artificially inflate the reputation of the page (e.g., forcing the user to "Like" the page to access a false reward). MyPageKeeper evaluates each URL using a machine-learning-based classifier that leverages the social context associated with the URL. For any particular URL, the features used by the classifier are obtained by com-bining information from all posts (seen across users) containing that URL. Example features used by MyPageKeeper'sclassi-fier include the similarity of text message across posts and the number of comments/Likes on those posts. MyPageKeeper has false positive and false negative rates of 0.005% and 3%. For more details aboutMyPageKeeper's and low false positives and false negatives.

implementation and accuracy, we refer interested readers to [10].

Our dataset contains 91 million posts from 2.2 million walls monitored by MyPageKeeper over 9 months from June 2011 to March 2012. These 91 million posts were made by 111K apps, which forms our initial dataset D-Total, as shown in Table I.

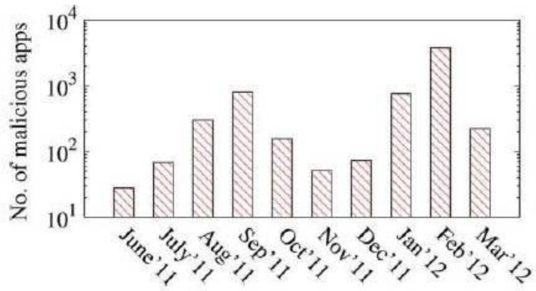
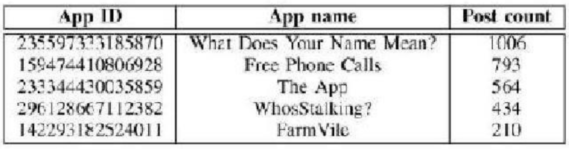


Fig.2 . Malicious apps launched per month in D-Sample dataset.

The D-Sample Dataset: Finding Malicious

Applications: To identify malicious Facebook applications in our dataset, we start with a simple heuristic: If any post made by an application was flagged as malicious by MyPageKeeper, we mark the application as malicious. By applying this heuristic, we identified 6350 malicious apps. Interestingly, we find that several popular applications such as Facebook for Android were also marked as malicious in this process. This is in fact the result of hackers exploiting Facebook weaknesses as we describe later in Section VI-E. To avoid such misclassifications, we verify applications using a whitelist that is created by considering the most popular apps and significant manual effort. After whitelisting, we are left with 6273 malicious applications (D-Sample dataset in Table I). Table II shows the top five malicious applications, in terms of number of posts per application. Although we infer the ground truth data about malicious applications from MyPageKeeper, it is possible that MyPageKeeper itself has potential bias classifying malicious app's posts. For example, if a malicious application is very unpopular and therefore does not appear in many users' walls or news feeds, MyPageKeeper may fail to classify it as malicious (since it works on post level). However, as we show here later, our proposed system uses a different set of features than MyPageKeeper and can identify even



App ID	App name	Post count
235597333185870	What Does Your Name Mean?	1006
159474410806928	Free Phone Calls	793
233344430035859	The App	564
296128667112382	WhosStalking?	434
142293182524011	FarmVile	210

TABLE I
TOP MALICIOUS APPS IN D-SAMPLE DATASET

very unpopular apps with high accuracy Fig. 2 shows the number of new malicious apps seen in every month of the D-Sample dataset. For every malicious app in the D-Sample dataset, we consider the time at which we observed the first post made by this app as the time at which the app was launched. We see that hackers launch new malicious apps every month in Facebook, although September 2011, January 2012, and February 2012 see significantly higher new malicious app activity than other months. Out of the 798 malicious apps launched in September 2011, we find 355 apps all created with the name "The App" and 116 apps created with the name "Profile Viewing." Similarly, of the 3813 malicious apps created in February 2012, 985 and 589 apps have the name "Are You Ready" and "Pr0file Watcher," respectively. Other examples of app names used often are "What does your name mean?," "Fortune Teller," "What is the sexiest thing about you?," and so on.

D-Sample Dataset: Including Benign Applications: To selectan equal number of benign apps from the initial D-Total dataset, we use two criteria: 1) none of their posts were identified as ma-licious by MyPageKeeper, and 2) they are "vetted" by Social Bakers [20], which monitors the "social marketing success" of apps. This process yields 5750 applications, 90% of which have a user rating of at least 3 out of 5 on Social Bakers. To match the number of malicious apps, we add the top 523 applications in D-Total (in terms of number of posts) and obtain a set of 6273 benign applications. The D-Sample dataset (Table I) is the union of these 6273enign applications with the 6273 malicious appli-cations obtained earlier. The most popular benign apps are Far-mVille, Facebook for iPhone, Mobile, Facebook for Android, and Zoo World.

For profiling apps, we collect the information for apps that is readily available through Facebook. We use a crawler based on the Firefox browser instrumented with Selenium [21]. From March to May 2012, we crawl information for every application in our D-Sample dataset once every week. We collected app summaries and their permissions, which requires two different crawls.

D -Summary Dataset: Apps With App Summary: We collect app summaries through the Facebook Open graph API, which is made available by Facebook at a URL of the form https:// graph.facebook.com/App_ID;
Facebook has a unique identifier for each application. An app summary includes several pieces of information such as application name, description, company name, profile link, and monthly active users. If any application has been removed from Facebook, the query results in an error. We were able to gather the summary for 6067 benign and 2528 malicious apps (D-Summary dataset in Table I).

It is easy to understand why malicious apps were more often removed from Facebook.

D-Inst Dataset: App Permissions: We also want tostudy the permissions that apps request at the time of installation. For every application App_ID, we crawl https://www.facebook.com/apps/application.php?id=
App _ID, which usually redirects to the application's installation URL. We were able to get the permission
set for 487 malicious and 2255 benign applications in our dataset. Automatically crawling the permissions
for all apps is not trivial [13], as different apps have different redirection processes, which are intended for
humans and not for crawlers. As expected, the queries for apps that are removed from Facebook fail here as
well.

D-Profile Feed Dataset: Posts on App Profi les: Users can make posts on the profile page of an app, which we can call the profile feed of the app. We collect these posts using the Opengraph API from Facebook. The API returns posts appearing on the application's page, with several attributes for each post, such as message ,link, and create time. Of the apps in the D-Sample dataset, we were able to get the posts for 6063 benign and 3227 malicious apps. We construct the D-Complete dataset by taking the intersection of D-Summary, D-Inst, and D-ProfileFeed datasets.

III.IMPLEMENTATION MODULES

Malicious and benign app profiles significantly differ: We systematically profile apps and show that malicious app profiles are significantly different than those of benign apps. A striking observation is the "laziness" of hackers ; many malicious apps have the same name, as 8% of unique names of malicious apps are each used by more than 10 different apps (as defined by their app IDs). Overall, we profile apps based on two classes of features: (a) those that can be obtained on-demand given an application's identifier (e.g., the permissions required by the app and the posts in the application's profile page), and (b) others that require a cross-user view to aggregate information across time and across apps (e.g., the posting behavior of the app and the similarity of its name to other apps).

The emergence of AppNets: apps collude at massive scale:

We conduct a forensics investigation on the malicious app ecosystem to identify and quantify the techniques used to promote malicious apps. The most interesting result is that apps collude and collaborate at a massive scale. Apps promote other apps via posts that point to the "pro moted" apps. If we describe the collusion relationship of promoting-promoted apps as a graph, we find

1,584 promoter apps that promote 3,723 other apps. Furthermore, these apps form large and highly-dense connected components, Furthermore, hackers use fast-changing indirection: applications posts have URLs that point to a website, and the website dynamically redirects to many different apps; we find 103 such URLs that point to 4,676 different malicious apps over the course of a month. These observed behaviors indicate well-organized crime: one hacker controls many malicious apps, which we will call an AppNet, since they seem a parallel concept to botnets.

Malicious hackers impersonate applications:

We were surprised to find popular good apps, such as 'FarmVille' and 'Facebook for iPhone', posting mali cious posts. On further investigation, we found a lax authentication rule in Facebook that enabled hackers to make malicious posts appear as though they came from these apps.

FRAppE can detect malicious apps with 99% accuracy: We develop FRAppE (Facebook's Rigorous Application Evaluator) to identify malicious apps either using only features that can be obtained on-demand or using both on-demand and aggregation based app information. FRAppE Lite, which only uses information available on-demand, can identify malicious apps with 99.0% accuracy, with low false positives (0.1%) and false negatives(4.4%). By adding

aggregation-based information, FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and lower false negatives (4.1%).

IV.CONCLUSION AND FUTURE WORK

Applications current a convenient means for hackers to spread malicious content on Facebook. However, little is understood about the characteristics of malicious apps and how they function In this work, using a large corpus of malicious Facebook apps observed over a nine month period, we showed 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, we developed FRAppE, an accurate classifier for finding malicious Facebook applications. Most interestingly, we highlighted the emergence of AppNets large groups of tightly connected applications that promote each other. We will go on with to dig deeper into this ecosystem of malicious apps on Facebook, and we expect that Facebook will benefit from our recommendations for sinking the menace of hackers on their platform.

REFERENCES

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

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

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

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

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

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

[7] 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.

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

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

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

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

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

[13]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.

[14] A. Makridakis, E. Athanasopoulos, S. Antonatos,
D. Antoniades, S. Ioannidis, and E. P. Markatos.

[15] Understanding the behavior of malicious applicationsin social networks. Netwrk. Mag. of Global Internetwkg., 2010.

Author's Details

Mrs. Shaik Ruhi Apsha received M.C.A from QIS College of Engineering and Technology , Vengamukkapalem affiliated to JNTU Kakinada in 2010 and pursuing M.Tech in Computer Science and Engineering from PACE institute of Technology and Sciences affiliated to the JNTU Kakinada in 2015-17 respectively.

Mr. Shaik Jilani Basha has received B.tech and M.tech PG.He is dedicated to the teaching field from the last 4 years.He has guided 2 PG students and 4 UG students.