FRAPPE -Detecting Malicious Facebook Applications

ABSTRACT:

With 20 million installs a day [1], 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. First, we identify a set of features that help us distinguishmalicious apps from benign ones. For example, we find that malicious apps often share names with other apps, and they typically request fewer permissions than benign apps. Second, leveraging these distinguishing features, we show that FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and a high true positive rate (95.9%). Finally, we explore the ecosystem of malicious Facebook apps and identify mechanisms that these apps use to propagate.

INTRODUCTION:

Online social networks (OSNs) enable and encourage third-party applications (apps) to enhance the user experience on these platforms. Such enhancements include interesting or entertaining ways of communicating among online friends and diverse activities such as playing games or listening to songs. For example, Facebook provides developers an API that facilitates app integration into the Facebook user- experience. There are 500K apps available on Facebook, and on average, 20M apps are installed every day. Furthermore, many apps have acquired and maintain a really large user base. For instance, FarmVille and CityVille apps have 26.5M and 42.8M users to date. Recently, 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:

1) the app can reach large numbers of users and their friends to spread spam;

2) the app can obtain users' personal information such as e-mail address, home town, and gender; and

3) the app can "reproduce" by making other malicious apps popular.

To make matters worse, the deployment of malicious apps is simplified by ready-to-use toolkits starting at $25. In other words, there is motive and opportunity, and as a result, there are many malicious apps spreading on Facebook every day.