الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

المدرسة العليا للإعلام الآلي - 08 ماي 1945 – بسيدي بلعباس

Ecole Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbes

MEMOIRE

En vue de l'obtention du diplôme de **Master**

Filière : **Informatique**

Spécialité : **Ingénierie des Systèmes Informatiques (ISI)**

Thème

Techniques d'Apprentissage Automatique pour la Détection de Malwares Android

---

Présenté par **:**

- MAHNANE Ilyes

Soutenu le : **01/07/2019**

Devant le jury composé de :

- M BENDAOUD Fayssal	Président
- M BELFEDHAL Alaa Eddine	Encadreur
- M KAZITANI Mohammed	Examinateur

Année Universitaire : 2018 / 2019

Résumé

Le marché des téléphones intelligents, ou smartphones, a connu un essor considérable au cours de dernières années. Ces téléphones ont dépassé leur fonctionnalité première de communication vocale et sont désormais de véritables mini-ordinateurs, dotés d'un système d'exploitation propre qui permet à l'utilisateur d'installer toutes sortes d'application. Bien que le nombre de modèles de téléphone soit considérable, deux systèmes d'exploitation prédominent largement le marché : l'iOS d'Apple et Android de Google.

Ce dernier permet à n'importe quel utilisateur ayant quelques connaissances en programmation de créer et publier ses propres applications sur le site Google Play, où les autres utilisateurs peuvent les télécharger. Ce site se base sur un système de réputation et de signature pour assurer la sécurité des utilisateurs.

Ce système est loin d'être parfait. D'une part, des applications malicieuses (malwares) se retrouvent régulièrement sur ce marché. Dès qu'il prend connaissance d'une telle contamination, Google réagit en supprimant les applications suspectes du marché. Cependant, le temps nécessaire à cette réaction laisse le temps à de nombreux utilisateurs d'être infectés. D'autre part, de nombreux utilisateurs sont contraints d'utiliser des marchés alternatifs. Par exemple, à l'heure actuelle, Google Play ne supporte pas les applications payantes en Chine. Les utilisateurs se tournent donc massivement vers des marchés alternatifs. Ces marchés ne sont pas contrôlés et sont donc infestés de programmes malveillants : il est crucial pour ces utilisateurs d'être à même de les détecter afin de limiter les risques.

L'objectif de ce travail est de fournir un état de l'art des travaux existants centrés sur l'analyse statique et dynamique des applications Android et les comparer selon plusieurs critères à savoir les caractéristiques extraites, les fichiers analysés et l'efficacité contre les logiciels malveillants en constante évolution.

Mots clés: Android, Analyse dynamique, Analyse statique, Détection de Malware, Apprentissage automatique.

Abstract

The smartphone market, has grown considerably in recent years. These phones have outgrown their primary voice communication functionality and are now real minicomputers, with his own operating system which allows the user to install all kinds of application. Although the number of phone models is considerable, two operating systems largely dominating the market: Apple's iOS and Google's Android.

This allows any user with some programming knowledge to create and publish their own apps on the Google Play site, where other users can download them. This site is based on a system of reputation and signature to ensure the safety of users.

This system is far from perfect. On the one hand, malicious applications (malware) are regularly found on this market. As soon as he becomes aware of such contamination, Google responds by removing suspicious applications from the market. However, the time required for this reaction leaves time for many users to become infected. On the other hand, many users are forced to use alternative markets. For example, Google Play currently does not support paid apps in China. Users are therefore turning massively into alternative markets. These markets are not controlled and are therefore infested with malicious programs: it is crucial for these users to be able to detect them in order to limit the risks.

The objective of this work is to provide a state of the art of existing works centered on the static and dynamic analysis of Android applications and compare them according to several criteria, namely the characteristics extracted, analyzed files and effectiveness against ever-changing malware.

Keywords: Android, Dynamic analysis, Static analysis, Malware Detection, machine learning.