



Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Android Kötücül Yazılım Tespit Sistemleri İncelemesi

Ömer KİRAZ^{a,*}, İbrahim Alper DOĞRU^b

^a Bilgisayar Mühendisliği Bölümü, Mühendislik Mimarlık Fakültesi, Gazi Üniversitesi, Ankara, TÜRKİYE
^b Bilgisayar Mühendisliği Bölümü, Fen Bilimleri Enstitüsü, Gazi Üniversitesi, Ankara, TÜRKİYE

* Sorumlu yazarın e-posta adresi: omerk1818@gmail.com

ÖZET

Akıllı telefonların hayatımıza girmesiyle birlikte akıllı telefonları kullanan kullanıcı sayısı her geçen gün artarak devam etmektedir. Akıllı telefonların fazla talep görmesindeki neden, insanların bir cihazla istedikleri işleri tek dokunuşla kolaylıkla yapabilmesidir. International Data Corporation (IDC) firmasının 2016 2. çeyrek raporuna göre; akıllı telefon pazarında Android %87.6 gibi çok yüksek bir paya sahiptir [1]. Android'in akıllı telefon kullanan kullanıcılar arasında popüler olması ile birlikte açık kaynaklı bir yapıya sahip olması ve markete uygulama yüklenirken detaylı olarak kötücül yazılım incelenmesi yapılmadığından dolayı Android platformu kötü niyetli kişilerin bir numaralı hedefi haline gelmiştir. Android market ve diğer alternatif Android marketlerde kötü niyetli uygulamaların sayısı her geçen gün artmaktadır. G Data'nın 2015 1. Çeyrek raporuna göre; kötücül yazılımların %50.3 finansal amaçlıdır [2]. Finansal amaçlı olmasındaki neden Avrupa kıtasındaki kullanıcıların %41'nin banka işlemlerini akıllı telefonlarını kullanarak yapmasıdır [2]. Bu yüzden Android marketlerde bulunan uygulamaların kötücül olup olmadığını tespit etmek için etkin kötücül yazılım tespiti yapan sistemlere ihtiyaç vardır. Bu çerçevede bu çalışmada kötücül yazılım tespit sistemleri anlatılmıştır.

Anahtar Kelimeler: Android 1, kötücül yazılım tespiti 2, akıllı telefon 3, Android uygulama güvenliği 4, Android güvenliği 5, mobil güvenlik 6

Android Malware Detection Systems Review

ABSTRACT

With the smartphones entering our lives, the number of smartphones continues to increase day by day. The reason why smartphones are in so demand is that people can easily do what they want. According to IDC's 2016 Q2 report, Android dominated the smartphone market with an 87.6% share [1]. The Android platform has become the number one target of malicious people because of Android has an open source and new application installation has not been analyzed in detail. Therefore, the number of Android malicious applications are also increasing every day on Google Play and alternative Android application markets.

According to G Data's 2015 Q1 mobile malware report, 50.3% of malware is for financial purposes [2]. The reason is that 41% of Europe's users use their devices for banking transactions [2]. Hence, there is need for effective malware detection systems which are detect malicious software on Android application markets. In this paper, malicious software detection systems will be explained.

Keywords: *Android 1, malware detection 2, smartphone 3, Android application security 4, Android security 5, mobile security 6*