Nowadays, Android has become the leading mobile operating system platform, it recently passed the two billion marks of monthly active devices. Undoubtedly, with such huge growth, it is apparent that it will attract several malware authors targeting these devices. However, controlling or affecting Android devices can occur by placing malicious applications in their marketplace (Google Play), which is the absolute method to install their applications. (Evaluating Malware Mitigation by Android Market Operators). Malicious software (Malware) is considered to be a significant threat that opposes on the Internet today, it appears in many extensive forms and variations, such as viruses, worms, Trojan horses, botnets and rootkits. Malwares determined to mainly act against the user’s interest, thus it can cause many harmful activities, which includes, spam, Denial of Service (DoS), gain access to user’s information. And, can reduce the efficiency of the device by draining the battery. (SCALABLE & an empirical study of malware evolution). Malware spread itself by exploiting vulnerabilities or social engineering techniques that deceive both the user and operating system to perform the activities mentioned earlier, for example, by downloading a malicious app, it can lead to stealing login information and commit fraud or sending spam that may affect other users.

In recent study conducted by Kaspersky it illustrates the evolution of malware, *“From the beginning of January till the end of December 2016, Kaspersky Lab registered nearly 40 million attacks by malicious mobile software and protected 4,018,234 unique users of Android-based devices”*

**Statistics about how many malwares in market now?**

**Lorenz’s first paper**

In fact, Android applications are generally written in the Java programming language and executed on top of the Dalvik virtual machine [4], but native code invocation is however possible via JNI or Linux ELF binary execution. This mixed environment seems to suggest the need to reconstruct and keep in sync out-of-the-box semantics through virtual machine introspection (VMI) [10] for both the OS and Dalvik views, as very recently shown in [25].

**USED:**

**Evaluating Malware Mitigation by Android Market Operators**

<https://www.usenix.org/system/files/conference/cset16/cset16-paper-kikuchi.pdf>

<https://venturebeat.com/2017/05/17/android-passes-2-billion-monthly-active-devices/>

**App Store, Marketplace, Play! An Analysis of Multi-Homing in Mobile Software Ecosystems**

<http://ceur-ws.org/Vol-879/paper5.pdf>

One of the major threats on the Internet today is malicious software, often referred to as malware.

Malware comes in a wide range of forms and variations, such as viruses, worms, botnets, rootkits, Trojan horses, and denial of service tools. To spread, malware exploits software vulnerabilities in browsers and operating systems, or uses social engineering techniques to trick users into running the malicious code.

In recent years, Android has become the dominant mobile operating system. Unsurprisingly, this also means that it has become more attractive for criminals to target Android devices. A key attack vector to get malware on these devices is via Android app markets, as they are the main mechanism through which users obtain their apps.

# Well known examples of malicious activity include denial of service, spam, information gathering, and resource gathering. In all cases, this activity is based on the use of software, also called “malcode” or “malware.

# ^An empirical study of malware evolution

Abstract

All Android markets are confronted with malicious apps,

but they differ in how effective they deal with them.

1 Introduction

In recent years, Android has become the dominant mobile

operating system. Unsurprisingly, this also means

that it has become more attractive for criminals to target

Android devices. A key attack vector to get malware on

these devices is via Android app markets, as they are the

main mechanism through which users obtain their apps.

Criminals put malware-laden apps in these markets and

then use a variety of ways to get users to install them.

Next to “Google Play”, the official market operated by

Google, there are many third-party markets. All markets