Chapter 37
The Trend of Mobile Malwares and Effective Detection Techniques

Olawale Surajudeen Adebayo
International Islamic University Malaysia, Malaysia

Normaziah Abdul Aziz
International Islamic University Malaysia, Malaysia

ABSTRACT

The usefulness of mobile phones nowadays has gone beyond making calls and sending text messages. In fact, most of applications available on desktop computer are presently easily accessible on mobile devices, especially smartphone based on Androids, iOS, and Windows phone platforms. However, at the same time, malware is increasingly becoming pervasive on a mobile platform for financial, social and political exploitation. This chapter examines the trends of mobile malware and different efforts of anti-malware writers and researchers in addressing mobile malware on smartphones.

INTRODUCTION

Malware writers have continuing to model their malware towards mobile applications due to the pervasiveness of these important tools and its various benefits. Days have gone when mobile phones were using for calling and sending text messages. Several operations like financial transaction, internet banking, email and text messaging, information communication, private and corporate activities, effective data storage, audio and video coverage, e-commerce, e-government, e-transaction, multimedia among others are now available on the mobile phones most especially smartphones. Smartphones are designed to perform virtually all the functions that can be carried out on the desktop computers. The most popular operating system (OS) that allow smartphones to perform these functions are Android by Google, iOS by Apple and Windows 7 OS. The paper examined the trend of malware on the Android phone and iOS due to their acceptability and ubiquity.

DOI: 10.4018/978-1-5225-7909-0.ch037

Malwares are malicious applications or software targeted at operating system or internet. Mobile malwares are malicious software specifically designed to target the mobile operating system. Smartphone malwares along the line are malicious executable designed to hamper the normal operation of smartphones like Androids, iOS, and windows 7 phones for various reasons like financial gain, challenges or system testing and information stealing. Efforts have been made by several researchers to develop malware detection system to bring about eradication or reduction to the dastard effects of malware on the smartphones. Detection systems are the system design including antimalware algorithm, intrusion detection system, etc. to bring solution to the malware problem. However, old malware detections bank on the signature, IP addresses and anomaly behaviours to detect malware whereas malware writers are evolving new strategy every day.

As anti-malware writers are successfully developing various algorithms against existing malware, malware writers also continue to change their stealthy and obfuscation techniques in order to hide their malicious code. The task of preventing mobile facilities therefore lies on device's security mechanism, and the stakeholders' education. For example, some malwares rely on user interaction before their execution, while others exploit the bugs in the operating system of these important facilities. Moreover, Analysis of malware has to do with identifying the instances of malware by different classification schemes using the attributes of known malware characteristics (Adebayo, Mabayoje, Mishra, & Osho, 2012). The remaining part of the paper is arranged as follows; section two is used to discuss the related researches to this work. In section three and four, mobile application operating system and Security fundamentals were examined respectively. Existing malware detection techniques were examined in section V. Future work was discussed in section six, section seven was used to highlight recommendations. Finally, the paper concluded with section nine.

BACKGROUND

This research studies the existing literatures on the trend of android malware, its analysis and detection system. The usefulness of mobile facilities such as smartphones has increased their target by malware over time. This, in order hand has made the field of malware detection a daunting task most especially on a mobile platform. A malware is a computer program that has various kinds of malicious intents (Karami et al., 2013). Mobile malware on the other hand is malicious software that is specifically designed to attack mobile facilities i.e. mobile phones and smartphones (Buennemeyer et al., 2013). Some commonly known Malware categories are viruses, trojans and worms. Malicious programs present an incessant threat to the privacy and security of sensitive data and the availability of critical services at crucial point in time (Adebayo et al., 2012). The first observable feature adopted by malware most detector at the outset of smartphone is battery power consumption (Thanh, 2013; Blasing et al., 2010; Eder et al., 2013). The technique was basically to the mobile phone power consumption and compares it with the normal power consumption in order to detect occurrence of anomaly. The first malware specifically written for Symbian OS platform was discovered (Cabir) in 2004. After the infection successfully carried out by Cabir malware and its variants (Kim et al., 2008, pp. 239-252), researchers proposed approaches and developed different mechanisms in order to detect malware on a mobile phone. With the advent of smartphones, malware has consistently double on the mobile phone due to its ubiquity.

The F-Secure's Threat report (Yap, 2013) stated that the number of Android malware has been doubling year-on-year since 2011 up to the first quarter of 2013. In a bid to curtail the effect of malware