Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Detecting mobile malware threats to homeland security through static analysis

Seung-Hyun Seo[a], Aditi Gupta[a], Asmaa Mohamed Sallam[a], Elisa Bertino[a], Kangbin Yim[b,*]

[a] Department of Computer Science, Purdue University, West Lafayette, IN 47907, US
[b] Department of Information Security Engineering, Soonchunhyang University, 646 Eupnae, Shinchang, Asan 336-745, Republic of Korea

ARTICLE INFO

Article history:
Received 26 November 2012
Received in revised form
28 February 2013
Accepted 8 May 2013
Available online 6 June 2013

Keywords:
Mobile malware
Homeland security
Smartphone
Android OS

ABSTRACT

Recent years have seen the significant increase in the popularity of smartphones. This popularity has been accompanied with an equally alarming rise in mobile malware. Recently released mobile malware targeting Android devices have been found to specifically focus on root exploits to obtain root-level access and execute instructions from a remote server. Thus, this kind of mobile malware presents a significant threat to Homeland Security. This is possible because smartphones can serve as zombie devices which are then controlled by hackers' via a C&C server. In this paper, we discuss the defining characteristics inherent in mobile malware and show mobile attack scenarios which are feasible against Homeland Security. We also propose a static analysis tool, DroidAnalyzer, which identifies potential vulnerabilities of Android apps and the presence of root exploits. Then, we analyze various mobile malware samples and targeting apps such as banking, flight tracking and booking, home&office monitoring apps to examine potential vulnerabilities by applying DroidAnalyzer.

1. Introduction

Hackers have spread PC malware (specially targeted for Window Operating System) to attack the government and industry sectors. Stuxnet (Albright et al., 2010) demonstrated, in June 2010, a PC malware which targets SCADA (Supervisory Control And Data Acquisition) (SCADA,) systems to control and monitor specific industrial processes. However, with the rapidly expanding population of mobile devices, smartphones are fast becoming the target of choice for hackers.

Mobile malware which specifically target smartphones can become a significant threat towards Homeland Security (2011). Smartphones have a variety of feature-rich, user-friendly mobile applications which are commonly referred to as "apps". They enrich the functionality of the smartphone while enhancing the user experience. These applications are distributed via online application stores called app markets. These markets have lowered the entry barrier allowing users to easily discover and download new apps. On the flipside, it has also provided an easy distribution method for malware. Although official app markets such as Apple's AppStore or Google Play store employ a vetting system to screen out malware, those apps are only loosely regulated. More seriously, third-party app markets allow the distribution of apps without any extensive security inspection. This open approach has made these app markets enticing targets for the dispersion of mobile malware.

The most popular technique used by mobile malware authors is to insert malware within legitimate apps and then repackage them for distribution. Since the malware is disguised within an app that looks legitimate, unwary users unknowingly install them. The mobile malware can be commonly classified with a range of factors such as monetization, collecting user information, stealing credential for future abuse, making mobile bot-nets and gaining root level access, just to name a few (Felt et al., 2011b; Zhou and Jiang, 2012). Currently, the most widely used mobile malware targeting Android devices takes advantage of root exploits to obtain root privileges and execute instructions from a remote server (Fisher, 2011). This type of malware is especially dangerous since it can create bot-nets, which remotely control the infected devices and function as a network for which hackers can manipulate to attack other computer systems. In March 2011, Google removed 21 free apps embedded malicious code, with root access exploits from Google Play store. However, the app was already downloaded more than 260,000 times by Android smartphones within 48 h (Android users infected with malware, 2011).

This type of mobile malware significantly threatens Homeland Security, because it can quickly alter users' smartphones into zombie devices. From this point, the infected phones can attack main server systems of public infrastructures. Recently, the

* Corresponding author. Tel.: +82 41 530 1741.
E-mail addresses: seo29@purdue.edu (S.-H. Seo), aditi@purdue.edu (A. Gupta), asallam@purdue.edu (A. Mohamed Sallam), bertino@purdue.edu (E. Bertino), yim@sch.ac.kr (K. Yim).

1084-8045/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2013.05.008

government and industry sectors such as military, healthcare service, banks, businesses and airlines have increasingly integrated smartphone-usage into their service operations. We can easily find mobile banking apps, flight tracking apps, home&business office security monitoring apps, and healthcare service apps from the app markets. In the case that these apps were to include malicious code, it presents a grave threat towards our lifestyle. If apps like PlaneFinder, FlightTrader, and FlightAware, which are able to track flights in real time, are used by terrorists, it presents a dangerous precedence. The terrorists can target a specific flight using information such as location data. The US army has also developed apps which help soldiers communicate, gather intelligence, or even identify enemy combatants (Homeland Security, 2011). If a soldier downloads apps embedded malware that can disable a cell tower or leak information stored in smartphone, it can compromise security and safety of the soldier. The rogue mobile banking apps, such as Droid09 (Malicious Banking App), launch phishing attacks to access a customer's financial account leaving the customer vulnerable to identity theft. If malware is inserted in home&office security apps which can arm or disarm your security system (burglary, cameras, fire) and monitor your security cameras, would be a breach of privacy.

Many researchers have studied mechanisms for detecting and preventing mobile malware (Burguera et al., 2011; Chin et al., 2011; Enck et al., 2010, 2011, 2009; Felt et al., 2011a; Grace et al., 2012, 2012b, 2012a; Lange et al., 2011). However, most of their work has focused on free apps, and paid apps from the third-party app market, without specific categories. They have not investigated the potential threats analysis of mobile malwares or apps related to Homeland Security. Thus, it is necessary to examine public sector-related apps to find potential vulnerabilities.

In this paper, we will address malicious functionality and present a step-by-step analysis of a representative sample. Then, we will show how mobile attack scenarios are applicable to Homeland Security and present real threat. Second, we propose an analysis tool of Android apps, DroidAnalyzer, that detects potential vulnerabilities. To build DroidAnalyzer, we studied various malware samples of Android Malware Genome Project and identified unique characteristic inherent in the malware. We then extracted the risky API and major keywords including typical commands used in mobile malware. DroidAnalyzer has the function to identify the presence of root exploits by utilizing unique features and keywords typical of root exploit malware. In order to discover potential vulnerabilities, we apply DroidAnalyzer to 32 banking apps, 29 airplane booking and tracking apps, transportation reservation apps and 15 home&business office security apps downloaded from Google Play and the third-party app markets. We examine which kinds of risky APIs and permissions are most commonly used through a process of comparing official market apps with those found in the unofficial market. This provides a sufficient baseline with the assumption that official apps are vetted and screened. Finally, we suggest a methodology to better mitigate mobile malware threats against Homeland Security by improving upon existing countermeasures and guidelines for mobile security.

The remainder of this paper is organized as follows: In Section 2, we present threats of mobile malware and attack scenarios against Homeland Security. In Section 3, we introduce an analysis tool for Android apps, DroidAnalyzer. In Section 4, we show the examined results of public sector-related apps and discuss the defense measures against mobile cyber war, and conclude in Section 5.

2. Potential threats of mobile malware against homeland security

In this section, we first analyze the threats of mobile malware according to their current classification as provided (Felt et al., 2011b; Zhou and Jiang, 2012). Through manual analysis of our malware sample, we further specify their functionality. Then, we describe a South Korean banking incident of 2011 (Cyber terror against NH) in order to show how such a scenario could occur with mobile malware and pose a threat to Homeland Security.

2.1. *Threat analysis of mobile malware*

Mobile malware infects smartphone OS to achieve malicious goals or profits. Infection techniques such as Repackaging, Malvertizing, Browser Attacks, Update Attack, Drive-by Download (McAfee, 2011) are commonly used. Among them, repackaging is the most popular technique to deceive users into installing malware. Current mobile malware can be mainly categorized into Monetization, Information Stealing, Mobile Bot-net, and Root Privilege Acquisition (Felt et al., 2011b; Zhou and Jiang, 2012).

2.1.1. *Monetization*

Hackers can cause financial charges to smartphone users by infecting mobile malware that sends premium-rate SMS messages without the knowledge of the user. Original intent of premium-rate calls and SMS messages were to provide services such as news, technical support, stock quotes or adult service, with the cost being reflected in the user's phone bill. Premium-rate calls are now abused for the hacker's profit. Hackers lure infected smartphone users into signing up for a hacker-controlled premium-rate service and activate a service subscription. For example, Android malware, HippoSMS, sent SMS messages to a hard-coded premium-rated number. It removed SMS messages from service providers to prevent users from becoming aware of the additional unwanted charges.

2.1.2. *Information stealing*

For the most part, mobile malware collect users' various information stored in infected smartphones. We call this kind of app a spyware. Android apps can query Android APIs for information about user such as IMEI, IMSI, location, lists of contacts or installed apps and download history. For example, Android spyware, JackeeyWallpaper (JackeeyWallpaper) collects IMEI, IMSI, and the currently entered voicemail number from infected devices, then transmits it to the hacker's server. These spyware writers or hackers might sell users' information including phone numbers, email addresses, IMEI, etc. The contact information could be sold to spammers or phishers. Legitimate user's IMEI is valuable to illegal phone vendors. If a smartphone is stolen, its IMEI would be registered to the black list of IMEI not to connect the cellular networks. Thus, illegal phone vendors seek to replace invalid IMEIs with valid IMEIs. Recent mobile spyware such as Zitmo known as Zeus version on Android is more dangerous than common spyware, because it is aimed at intercepting confirmation SMS sent by banks to their customers. This SMS message may contain user credentials for Internet banking. So, it may be used to incur fraudulent transaction.

2.1.3. *Mobile bot-net*

This mobile malware is risky, because it alters the infected phone into a mobile bot to remotely control the infected phone. That is, the infected phone is a zombie for cyber attacks. It utilizes the HTTP-based web traffic in order to receive bot commands from C&C server. Among our malware samples, we found that a variant of Pjapps, Android-SpywareMinServ had remote control functionality to allow hackers to build a bot-net.