Security threats for the Android OS

Bc. Vítězslav Šnorich

Univerzity of Defence, Faculty of Military Leadership,
Kounicova 65, 66210 Brno, Czech Republic
E-mail: vitezslav.snorich@unob.cz

Abstract. The article describes the current threats to the Android operating system and the possibility of attacking the operating system designed for mobile devices. Article deals to identify appropriate applications and actions that contribute to the safe use of mobile devices. The testing equipment was used for the Galaxy Tab 8.4 with a version of the operating system Android 4.4.2 and a graphic interface TouchWiz from Samsung. On devices were tested antivirus programs for android operating system, their reliability, speed and ability to avoid threats. The article contains recommended safety procedures to minimize threats when using a mobile device with Android operating system.

Keywords: Android, antivirus, virus, malware, infiltration, threat, hacker

1 Introduction

Threats such as attacks on mobile devices are becoming more common across all platforms offered. Attacks on mobile devices become more sophisticated and are able to much better camouflage. The biggest success is recorded using social engineering practices. The article describes the current threats to the Android operating system and the possibility of attacking the operating system designed for mobile devices. Article deals to identify appropriate applications and actions that contribute to the safe use of mobile devices. The testing equipment was used for the Galaxy Tab 8.4 with a version of the operating system Android 4.4.2 and a graphic interface TouchWiz from Samsung. On devices were tested antivirus programs for android operating system, their reliability, speed and ability to avoid threats. The article contains recommended safety procedures to minimize threats when using a mobile device with Android operating system.

2 Current threats for operating system Android

Android operating system falls within into the category of open source operating systems. That makes the system much more vulnerable to security incidents. The Android operating system is among the the most commonly used operating system utilized on mobile devices. By the following, this operating system is is becoming increasingly bigger target for attackers and hackers.

As with any operating system. Most often, malicious software gets into the device user mistake or inattention. Users often mindlessly installed applications and they do not follow what rights allocated to them. Before installing the application asks whether to allow access to certain parts of the equipment. Granting access to an application, for example SMS messages could result in an automatic sending of messages to fee-based services. This way, you can also get into the device tracking malicious software. Equipment using this route can also be blocked and subsequently attacker ransom requires from the owner of the device. This type of attack is called Ransomware.

Infection of this kind of malware is usually irreversible for the device. The problem can be solved completely reinstalling devices. If the user can not back up their data on all subsequently come. Hackers and attackers are very proficient in social engineering and use it properly. They are able to lure a user to a good looking application and then infect the device.

Malicious apps may not only come from third party sources. Despite the security distribution channel which promotes the Google Play application can contain only a portion of malicious code. Applications can then ask to download additional data from a server other than where it was published and thus infect the device.

3 Is antivirus needed on Android?

It is not easy to clearly determine if the antivirus software on the mobile device required. An antivirus program on the device is not immediate protection against all the pitfalls for this operating system. If the user ignores basic safety measures such as the installation of uncertified third-party applications antivirus is probably unnecessary.

If the user follows the basic principles of safe use mobile devices, which are described below in the article, it is possible, in my opinion be without antivirus. In case of greater safety and security of their data antivirus software in the device is no obstacle.

4 Recommendation for safe device use

If the user wants to minimize the possibility of attack on your mobile device based on the Android operating system should follow a few basic rules. These rules not particularly restrict the user in everyday work with mobile devices.

4.1 Monitoring applications before the installing

Before installing each application phone alerts to what content and applications authorized to access requests. It is necessary to pay attention what privileges you applications. It is necessary to consider whether the application for playing music or activate the lamp needs for example access to SMS messages and call logs. Recommendation therefore watch carefully worded application requirements and consider whether certain applications are not excessive demands on the necessary permits.

4.2 Do not install applications from untrusted sources

Always install applications from trusted sources. Installing a downloaded app in .apk format may contain malicious software. This malware then take effect after installing the phone and can cause irreversible damage. As far as applications distributed through a channel such as Google Play, it is necessary to pay attention to the updates. To increase safety, it is recommended to disable the automatic updates downloaded applications.

4.3 Size of applications

Attention would also you have had to focus on the size of applications. For example, the large and visually flawless game probably will not be the size of several kilobytes. Even this indicator should take into account when installing applications to mobile devices.

4.4 Using encryption

Android operating systemfrom version 4.4 allows you to turn on the encryption. Encryption phone and memory card. For this option, it is necessary to set up a more sophisticated devices security policy. Even this measure can minimize the risk of data theft from the device.

4.5 Official distribution system

It is generally known that among users of Android operating system is very popular called Custom ROM. These operating systems usually created by a team fans can pose a huge security risk. Nobody knows what is hiding in the Custom Rom. These systems typically lure users to a newer version of Android, which at the official distribution available but also to higher performance devices. If the user decides to use the unofficial version of the operating system does so at his own risk. Therefore, I recommend sticking to the official distribution.

5 Recommended Antivirus

Antivirus programs for Anroid are many. Some are free, some are paid result will do largely the same service. Antivirus programs have been installed and tested at the below mentioned devices. Test compared antivirus software skills against each other.We tested the free version only. All tested antivirus programs meet the expectations of a particular Avast Mobile Security Free Version surprised at the extensive possibilities.

5.1 AVG AntiVirus

These Antivirus is from the Czech antivirus company AVG. This antivirus has been tested in Free. Antivirus has a fast scanning and can reveal security weaknesses such as the aforementioned authorization installing apps from unknown sources. Antivirus also offers performance management and erasing memory and power management. The interface is very user friendly and control is simple and clear.

5.2 Avast Mobile Seciruty

Avast Mobile Security provides many more options for testing. It is worth mentioning safety test WiFi network or theft protection. Offers a useful application management, monitors the data transfer and even comes with an option to run a firewall, which is, however, requires root access. The antivirus test is of course also present

5.3 Eset Mobile Security & Antivirus

The prerogative Antivirus solutions from ESETis ease of handling. It has depth and careful scanning, although signs of its length. You can also use anti-theft protection. In the paid version is unlocked other useful options.

6 Device for testing and used Android description

As devices for testing has been selected GALAXY Tab Pro 8.4 Samsung with a graphic interface TouchWiz. Tablet features a high performance 8 core processor operating at 1.9GHz frequency, there are 2GB of RAM. The device also has a very fine display which provides high resolution. The equipment was chosen because of computing power, satisfactory, good price and clear display.

The device includes an operating system Android version 4.4.2 KitKat. This version of the android operating system market is one of the most common and appears on most mobile devices. The version of the operating system that is used in devices fully supports all applications offered on the distribution portal Google play. Programs focusing on safety devices including. Android operating system as standard offers common security mobile devices such as the standard lock screen also brings the option of encrypting devices and also memory cards. The Android operating system, version 4.4.2 was chosen because the majority representation in the market. It is based on the assumption that automatically ranks among the most frequent targets of attackers.

References

1. Android official websites, https://www.android.com/history/
2. AV-test.org, https://www.av-test.org/en/antivirus/mobile-devices/
3. Kaspersky.com, https://usa.kaspersky.com/internet-security center/threats/mobile#.Vaa6vPmqpBc
4. Pandasecurity.com, http://www.pandasecurity.com/mediacenter/malware/new-threats-for-android-phones-how-do-they-work-beware-of-your-battery/
5. Digitalthrends.com http://www.digitaltrends.com/mobile/android-malware-threat-rears-head-time-means-business/
6. Tomsipro.com, http://www.tomsitpro.com/articles/mcafee-security-android-malware,1-2023.html