УДК 004.451.056.54 (045) = 111

**O.B. Rogozinskiy**

# Methods of protecting the Android OS from spyware

Вінницький національний технічний університет

**Анотація**

*В даній науковій роботі описується різні категорії шкідливих дій вірусів та їх класифікація, види пісочниць та сфера їх використання. Проведено аналіз та вплив вірусів на операційну систему Android та відомі розв'язки проблем вірусного впливу на ОС Android. Підготовлена вся науково-літературна база, за допомогою якої описується проблема і рішення.*

**Ключові слова**: ОС Android; Пісочниця; Шкідливе програмне забезпечення; Шпигунське програмне забезпечення; Троян Android.Titan.1.

**Abstract**

*In the present research work describes the different categories of harmful effects of viruses and their classification, types of sanding and scope of their use. The analysis and the impact of viruses on the Android operating system and known problem solutions viral effect on OS Android. Prepared all scientific and literary framework through which describes the problem and solution.*

**Keywords**: OS Android; Sandbox; Malware; Spyware; Trojan Android.Titan.1.

## RESULTS OF THE RESEARCH

There are more and more gadgets in the world every day that help us in our modern lives. Almost 91% of people currently use phones, tablets, laptops, and personal computers. Every day more and more innovations in the field of IT are released, which impress with their functionality, they are the most diverse applications for each sphere of human life. Of course, people use smartphones every day, according to statistics from the American company Pew Reseach Center, the global network includes about 1 billion cases in a day. (considering that fact that one person maynot have only one smartphone)

These devices have started pushing PCs out of the world market, as they are not inferior to the computer in terms of functionality, but their dimensions are quite compact.

Since the share of mobile OS in the world has recently become quite large, attackers have begun to use it for their own purposes. A variety of Android applications have begun to infect with powerful viruses which infect your mobile device so that you are no longer the owner of the phone, but simply an intermediate link between the virus and the smartphone.

Since the protection of smartphones today plays an important role, the relevance of scientific work is beyond doubt.

The purpose of scientific work is to increase the security of the Android mobile OS. The end result of scientific work is the creation of its own system for checking Android applications, which should perform tasks to track illegal and covert actions of applications.

The tasks of scientific work consist of the following points:

1. Investigate the categories of virus software;
2. Investigate the types of sandboxes;
3. Develop a useful model for solving Android security problems.

Categories of harmful actions of viruses

Viruses in smartphones and tablets on Android are quite diverse. It can be applications and programs with a specific malicious purpose. The most common virus on smartphones is the extortionist, which locks the screen of a phone or other device and demands to pay money. If the virus has blocked the

screen, you do not need to pay money to the attacker, it would be better to find a way to clear the virus or unlock the screen and then remove the application that locks the screen of the Android OS.

Viruses can steal money from bank accounts. They get SMS messages with pin codes which are sent to confirm the transfer. All this is hidden from the user and he may not even notice how the virus steals money from the bank account.

There are also viruses that steal personal information, they can turn on the camera on a phone or other device, spy on the owner or pass information without the user's knowledge. Even if all applications and programs are closed and the screen is locked, this does not guarantee that the virus has gone into standby mode, it can be active and use the camera or microphone even in this state.

There is one special type of virus software. The essence of its work is to cause the greatest possible harm to the user from all sides. Doctor Web warns of the appearance of a dangerous malware that infects mobile devices running the Android operating system. Trojan Android.Titan.1 has a well-developed functionality and can cause significant damage to the owner of an infected gadget.

To spread evil intentions, attackers use mass SMS-mailings. The potential victim receives a message stating that the delivery of a postal item is delayed, as well as a link, the transition to which involves obtaining detailed information about the "problem". In fact, this link leads to one of the pages of the popular cloud storage service, where the Trojan is located.

When you visit specific address, the malicious apk file is automatically downloaded to your mobile device. However, in order to infect the operating system, the user must perform its installation. After that, a malware shortcut appears on the home screen of your smartphone or tablet. At the first successful start, this shortcut is removed, and the Trojan continues to work in stealth mode. At the same time, the last SMS-dialogue is erased from the device's memory, which in most cases will be represented by the same spam message, thanks to which the virus got to the target device. In the future, Titan.1 operates without the participation of the user and begins its activity on its own, booting with the operating system.

The main feature of this Trojan is that its main functionality is implemented as a separate Unix-library (detected as Android.Titan.2), while most known malware for Android uses a standard executable dex-file. Such technique is quite rare, and thanks to it can’t be detected by anti-virus programs.

As for the functionality of Titan.1, the virus is able to send detailed information about the infected device to the remote server, replace phone numbers in the address book, send SMS, make calls to a given number, make a hidden recording of phone conversations and send files to attackers, block incoming or outgoing calls from certain numbers, answer calls and delete information about them from the system log, etc.

Types of sandboxes:

There are several basic prevention mechanisms based on different principles. The first were the classic HIPS-techniques based on self-education of the system and memorization of user’s actions. They are also called "HIPS with pop-ups". An example is the development of companies such as Outpost or Acronis. These products constantly ask the user whether to allow any application to perform this or that action.

Blockers based on blacklists became the most developed variants of HIPS. The essence of such systems is to check the entry of an unknown file, program or action in a list of previously known untrusted objects. The blacklist can be an antivirus signature database or a list of suspicious actions.

Another type of HIPS involves working with whitelists: such systems check suspicious programs for inclusion in the list of trusted programs allowed to run.

However, each of these approaches has its drawbacks. Yes, pop-up systems require a certain level of competence from the user. Techniques based on blacklists have a fairly high level of non-operation and false positives.

The most advanced and accurate technologies today are HIPS type "sandbox" (Sandbox). Here, the "sandbox" means the principle of dividing applications into trusted and untrusted and running the latter in a special space separate from the system. It allows you to work with suspicious programs without the risk of infection or damage to the system.

In this case, the "sandboxes" can be implemented in different ways. The most obvious and easily implemented (and therefore the most popular) approach is to use virtualization. In this case, several OS subsystems are simulated, such as the file system and the registry. After the suspicious application

finishes, the HIPS system usually simply cleans the so-called container and destroys all suspicious processes running in it.

A sandbox is usually a tightly controlled set of resources (hard disk space and RAM) for running a guest program. Access to the network, system resources of the operating system, direct information reading from input devices are often either partially emulated or severely limited. Sandboxes are an example of virtualization

The most common sandboxes are of the following types:

• Applets that run on a virtual machine or interpreter that allows you to run Java code from any website without compromising the operating system.

• So-called "prisons" (jail, chroot jail) also allow you to impose resource limits on users and processes of some operating systems.

• Virtual machines that completely emulate a "standard" computer (for example, VirtualBox).

### Methods of disabling malware in Android

The algorithm for disabling malware is quite simple and effective.

Disable this malware is currently possible in only one way - direct shutdown by the user.

This virus has different modifications, depending on which, the state of protection of the virus acquires different degrees of protection. For example, some modifications of the virus can be tracked using various security applications, but it is impossible to disable it. The fact is that the internal code of the Android OS after running such an application changes. These can be a variety of changes, from changing the operation of some keys (Button) to changing the structure of the OS (to block all possible access to the virus). Direct disconnection by the user is as follows, the user tries to track the hidden process with the help of security applications, and then tries to disconnect and backup the system. These actions clearly will not help, because modifications of the virus are quite small with such minimal protection. The next step will be "Reverse Engineering", i.e. to study the source code of the application from the middle to disassemble the functionality of the virus, where the source code in Android is usually easy to view, but the virus code will be encrypted.

It is advisable to develop an application that will scan the user's incoming .apk files (i.e. put them in the sandbox, provide a list of rights and track the behavior of the virus, i.e. the actions that he wants to perform). After that, if the process turns out to be malicious, a message will be displayed to the user that the application is malicious and show a list of rights that it requires, and then ask the user to remove the application. To develop this application, it would be advisable to use a "prison" sandbox. With its help, it will be possible to easily grant rights and easily select rights from the input application.

## CONCLUSION

To sum up the results of this scientific article, it can be noted that the problem described needs to be solved as soon as possible, as any user of the Android mobile operating system can become a victim of this malicious software.

Currently, there is only one way to disable and remove malware (Android.Titan2) virus - by removing it from the user side. Since a wide range of smartphone users do not know how to do this, it is advisable to develop an application based on the sandbox, to safely disable and detect malware that could do it for the user.

Due to the fact that there is no relevant solution to this issue, namely a protective tool, instructions on how to act to the average user when the virus enters the device, antivirus software, offers a useful model that plans to eliminate this malware (Android.Titan2), and malware in general.

### ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сергей Вильянов. Персональные устройства / Вильянов Сергей // Мир ПК.-2013. -342 с.

2. World Devices | PewResearchCenter [Електронний ресурс] . – Режим доступу: URL: http://www.pewresearch.org/data-trend/world-tech/used-world-device/. – Назва з екрану
3. Олійник О.В. Оцінка проблем забезпечення інформаційної безпеки. // Бюлетень Міністерства юстиції України. - №11.-2011-с.74-92.
4. Ендрю Хоог Android Криміналістика: Розслідування, аналіз і мобільна безпека для Google Android / Хоог Ендрю; - Уолтем: Syngress, 2011. – 372с.
5. Бергмен Н. Взлом мобільних пристроїв: секрети і рішення / Бергмен Н., Стентфілд М. – Санта – Клар: McGraw-Hill Osborne Media, 2013. – 269 с.
6. В. Домарев. Безопасность ИТ / Владимири Домарев; - К.: ООО «ТИД ДС», 2002 . -688с.
7. Обзор вирусной активности мобильных устройств за ноябрь 2016 года [Електронний ресурс]-Режим доступу: URL : http://news.drweb.ru/show/review/?lng=ru&i=10321. – Назва з екрану.
8. Разбираемся в системе обеспечения безопасности Android [Електронний ресурс] . – Режим доступу: URL: https://xaker.ru/2012/11/18/android-safe-system/. – Назва з екрану
9. Механизм безопасности HIPS и её разновидности [Електронний ресурс]-Режим доступу: URL : http://www.osp.ru/pcworld/2009/10/10708771/. – Назва з екрану.
10. Использование аплетов в Java машине [Електронний ресурс] . – Режим доступу: URL: http://www.helloworld.ru/texts/comp/lang/java/java/15.htm. – Назва з екрану.
11. Основы безопасности операционной системы Android. Безопасность на уровне Application Framework. Binder IPC [Електронний ресурс]-Режим доступу: URL : http://habrahabr.ru/post/1/76093/. – Назва з екрану.

***Рогозинський Олександр Борисович*** *- студент Вінницького національного університету, Вінниця, група 1БС-20б*

***Rogozinskiy Oleksandr Borisovich*** *- student of group 1BS-20B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia*

*Науковий керівник:* ***Габрійчук Людмила Едуардіївна*** *– старший викладач кафедри іноземних мов Вінницького національного університету, Вінниця*

Supervisor : ***Habriichuck Lydmula Eduardivna****- Senior Lecturer of the Department of Foreign Languages, Vinnytsia National University, Vinnytsia*