УДК 004.056

Д. В. Совецький
Науковий керівник: Ю. В. Баришев

МЕТОДИ ЗАХИСТУ ВІД ПРОГРАМНИХ ЗАКЛАДОК В ОС ANDROID

Вінницький національний технічний університет

Анотація

Проаналізовано особливості поводження шкідливого програмного забезпечення для операційного середовища Android, зокрема розглянуто принципи роботи шпигунського програмного забезпечення. Проаналізовано відомі алгоритми пошуку шкідливого програмного забезпечення. За результатами аналізу створено базу сигнатур та застосунок для виявлення шпигунського програмного забезпечення в операційному середовищі Android.

Ключові слова: *шпигунське програмне забезпечення, операційне середовище Android, сигнатури, сканування.*

Abstract

Peculiarities of malware performance developed for the operational system Android was analyzed, in particular spyware performance basics were considered. Known malware detection algorithms were analyzed. The signature base and the application for spyware scanning at operational system Android were developed based on these analyses results

Key words: *hashing, hash constructions, generic attacks, multicollisions, pseudo-random number generators, pseudo-random number sequences.*

На сьогоднішній день операційне середовище Android містить багато різних несправностей, починаючи від низького рівня захисту в ядрі Linux, так і включаючи рівні компонентів Library, Application Framework, та закінчуючи самими за стосунками [1]. Тому метою досліджень є покращення захисту ОС Android від шпигунських програмних закладок.

Як правило, такі дії як: крадіжка грошей з мобільного рахунку чи платіжних карт, крадіжка особистої інформації включаючи прослуховування, визначення місцезнаходження, доступ до камери проводяться за допомогою спеціальних програм (віруси), які тим чи іншим способом встановлюються на пристрій. У більшості випадків віруси потрапляють на пристрій під виглядом якихось нешкідливих застосунків: браузерів, плеєрів, ігор, книг, і навіть антивірусів [2]. Причому це може бути застосунок, який тільки "прикидається" оригінальним, а насправді має абсолютно інший зміст, або оригінальний застосунок, але з доданим шкідливим кодом.

Отже, робота присвячена дослідженню програмних закладок у встановлених застосунках та розробці методів захисту. Дослідження проведено на основі створення програмної закладки прослуховування мобільного пристрою на прикладі розробленої гри. Прослуховування здійснено засобами вбудованого мікрофона в мобільному пристрої. Імітується робота користувача, при якій користувач встановлює гру. При встановленні операційне середовище сповіщує про доступ до параметрів, які запитує застосунок. Після узгодження, гра встановлюється. Аналіз таких дій показав, що за статистикою 70% користувачів мобільних пристроїв з операційним середовищем Android, узгоджують весь доступ до компонентів, не звертаючи увагу про небезпечні параметри [2]. Таким чином розглянута ситуація, при якій причиною прослуховування є необережність користувачів. Однак також можливий випадок, коли розроблена гра використовує мікрофон для своїх цілей і паралельно прослуховує мобільний пристрій. Головною задачею користувача є відкриття застосунку, при якому спрацьовує сервіс зловмисника для прослуховування. Отже, сервіс неможливо зупинити, якщо сама гра буде закрита і видалена з фонового режиму. Таким чином, постає питання, щодо захисту різних гаджетів від даної проблеми. Пошук небезпечних програмних закладок буде відбуватись виключно за сигнатурою та евристичним методом [3].

Антивірус для Android сканує програми під час їх встановлення та оновлення, на вимогу користувача (якщо користувач натиснув кнопку просканувати), за розкладом (розклад вибирається в настройках продукту). Крім цього скануються файли, які зберігає користувач з браузера в теку Download. Крім цього, є режим розширеного захисту, в цьому випадку перевіряються файли на карті пам'яті при будь-якій їх зміні, а також всі нові файли, що записуються на карту пам'яті [4].

Приклад схеми перевірки коду з базою даних сигнатур наведено на рис.1.

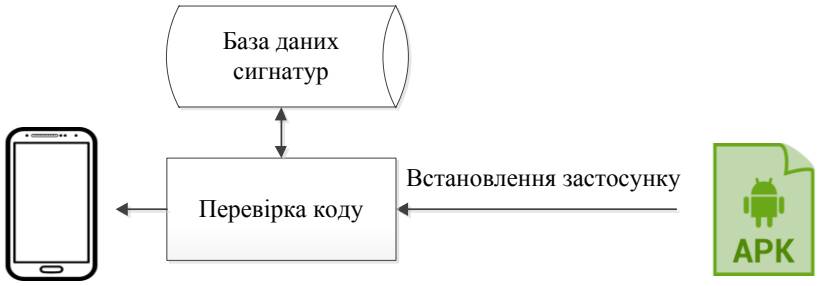

Рис.1.1 – Схема перевірки фрагментів коду з базою даних сигнатур

Сигнатура - це підпис відбиток вірусу. Він являє собою набір унікальних даних, або біт коду, які дозволяють йому бути ідентифіковані. Антивірусне програмне забезпечення використовує сигнатури вірусів, щоб знайти вірус у комп'ютерній файловій системі, що дозволяє виявляти, заносити вірус до карантину і видалити його. У антивірусного програмного забезпечення, вірус підпису називається файлом визначення або DAT-файл [5].

Кілька вірусів можуть мати одну і теж сигнатуру, яка дозволяє антивірусним програмам виявити декілька вірусів. Зазвичай нові віруси мають сигнатури вірусів, які не використовуються іншими вірусами. База сигнатур створена на основі підозрілих фрагментів коду, таких як: startService(), MediaRecorder, new MediaRecorder(), android.permission.RECORD_AUDIO.

Антивіруси, що використовують метод знаходження підозрілої поведінки програм(евристичний метод), не намагаються ідентифікувати відомі віруси, замість цього вони стежать за поведінкою всіх програм. Якщо програма намагається записати якісь дані в файл, що виконується, програма-антивірус може зробити помітку цього файлу, попередити користувача і спитати, що треба зробити. На відміну від методу відповідності визначенню вірусів в словнику, метод знаходження підозрілої поведінки дає захист від абсолютно нових вірусів, яких ще немає в жодному словнику вірусів [6].

В операційному середовищі Android, ні один застосунок за замовчуванням не має дозволу на виконання різних операцій пов’язаних з роботою пристроїв. Різні операції можуть негативно вплинути на додатки, операційну систему чи самого користувача. Сюди може входити: читання або запис особистих даних користувача (наприклад, контактів або електронних листів), отримання gps місцезнаходження, доступ до мікрофону, камери. Таким чином розроблено базу сигнатур, на основі сигнатурного та евристичного методів, створено застосунок для сканування файлової системи на наявність небезпечних закладок.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 1. Основы безопасности операционной системы Android. [Електронний ресурс]. – Режим доступу: URL: http://habrahabr.ru/post/176093/. – Назва з екрану.
2. 2. Aditya Gupta. Learning Pentesting for Android Devices/ Gupta Aditya – Birmingham: Packt Publishing Ltd, 2014. – 129 с. – ISBN: 978-1-78328-898-4.
3. 3. Sheran Gunasekera. Android Apps Security. / Gunasekera Sheran. – New-York: SPI Global, 2012. – 223 с. – ISBN: 978-1-4302-4062-4.
4. 4. Joshua J. Drake. Android Hacker’s Book /Joshua J., Collin M.. – Danvers: Sons Ins, 2014. – 523 с. – ISBN: 978-1-118-60864-7.
5. 5. Elenkov Nikolay.Android Security Internals. / Nikolay Elenkov – San Francisco: No Starch Press, 2014. – 377 с. – ISBN-10: 1-59327-581-1.
6. 6. Bargman N.Hacking Exposed Mobile: Security Secrets & Solutions. /Bargman N., Stanfield M. – Santa-Klar: McGraw-Hill Osborne Media, 2013. – 269 с. – ISBN: 978-0-07-181701-1.

Відомості про авторів

Совецький Дмитро Вадимович – студент групи 1БС-13б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця e-mail: appsandroid@gmail.com

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, Хмельницьке шосе, 95, м. Вінниця

Dmytro V. Sovetskyi – student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, e-mail: appsandroid@gmail.com

Yurii V Baryshev – ph. D., associated professor of information protection chair, Vinnytsia National Technical University, Vinnytsia.