Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Анализ внутренней структуры APK-файлов

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Кузяева Артема Ильгизовича

Научный руководитель

старший преподаватель _____ И.Ю. Юрин

31.12.2016 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

31.12.2016 г.

Саратов 2017

ВВЕДЕНИЕ

Современный человек уже не может представить свою жизнь без мобильного устройства (смартфона или планшета), которое всегда находится под рукой. Мы доверяем этим устройствам очень многое: начиная от безобидных изображений, заканчивая личными фотографиями и паролями от банковских карт. Android является самой популярной операционной системой, которая используется на мобильных устройствах (85% от общего числа пользователей).

Любая операция, совершаемая человеком, при обращении со смартфоном, происходит с помощью приложений: некоторые из них установлены по умолчанию, другие – необходимо устанавливать самостоятельно. Ежемесячно из официального источника для получения приложений «Google Play Market» пользователи скачивают около полутора миллиардов приложений [1], также необходимо учитывать и другие источники получения файлов для установки приложений.

Настолько популярную тему не могли обойти злоумышленники, которые всячески пытаются поместить свое вредоносное приложение на мобильное устройство пользователя. По данным «Лаборатории Касперского», в 2015 году было зарегистрировано около трех миллионов вредоносных установочных пакетов для операционной системы Android, среди которых 884 тысячи вредоносных мобильных приложений и 7 тысяч мобильных банковских троянов. Например, троян, который изымал данные для аутентификации пользователей в популярной социальной сети «Вконтакте», полностью проходил проверку безопасности и публиковался злоумышленниками в официальном магазине «Google Play Market» около 10 раз в течение нескольких месяцев – по данным специалистов, действию трояна подверглось от 100000 до 500000 человек. [2]

Если взглянуть на цифры, приведенные выше, то не останется сомнений в актуальности темы об исследовании приложений на факт наличия в них каких-либо вредоносных факторов. Причем такая проверка должна проводиться до того, как приложение окажется в источниках для скачивания приложений.

Целью данной дипломной работы является разработка и реализация программы для анализа внутренней структуры APK-файлов, получения основных сведений о приложении, находящемся внутри таких файлов, а также обнаружения факторов, свидетельствующих о возможной вредоносной активности приложения.

Для достижения поставленной цели требуется решить следующие задачи:

- рассмотреть базовую модель работы операционной системы Android;
- рассмотреть механизм взаимодействия операционной системы и приложения;
- рассмотреть основные компоненты разработки Android-приложений;
- произвести исследование параметров приложения, которые могут свидетельствовать о его вредоносной активности;
- произвести анализ большого количества APK-файлов для составления базы сигнатур и форматов часто встречающихся файлов, а также классифицированного списка ссылок.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 110 страниц, из них 46 страниц – основное содержание, включающее 34 рисунка и список использованных источников из 21 наименования.

КРАТКОЕ СОДЕРЖАНИЕ

1) Принцип работы приложений в операционной системе Android

В первом разделе рассмотрены принципы работы Android-приложений, компоненты, использующиеся для их разработки, и то, как они взаимодействуют с системой для корректной работы.

В подразделе 1.1 «Описание архитектуры операционной системы Android» описана базовая модель операционной системы Android, представленная в виде иерархии.

В подразделе 1.2 «Виртуальная машина Dalvik» описана виртуальная машина, которая используется для работы в Android до версии 4.4.

В подразделе 1.3 «Среда исполнения ART» описана среда исполнения, которая используется в Android, начиная с версии 4.4.

В подразделе 1.4 «Компоненты разработки Android-приложений» описаны основные модули, которые используются разработчиками при создании приложений для операционной системы Android.

2) Описание формата файлов APK

В данном разделе дано описание формата APK-файлов, разновидностей директорий и служебных файлов, описана структура файла-манифеста приложения.

В подразделе 2.1 «Основная информация о APK-файлах» приведено описание APK-файла, рассмотрен алгоритм сборки APK-файла, описаны алгоритмы сжатия APK-файлов.

В подразделе 2.2 «Внутренняя структура APK-файла» рассмотрены основные составляющие APK-файла. В подразделе 2.2.1 описано предназначение и значимость файла манифеста-приложения, в подразделе 2.2.1.1 рассмотрена структура этого файла, а в подразделе 2.2.1.2 описано понятие разрешения в Android-приложениях. В подразделе 2.2.2 описано содержимое и предназначение директорий с ресурсами.

3) Реализация программы для анализа внутренней структуры APK-файлов

Автором была разработана и реализована программа для анализа внутренней структуры APK-файлов, получения и просмотра в удобном формате основной информации о приложении, находящемся внутри этого файла. Также разработанная программа производит анализ исследуемого APK-файла на предмет возможной вредоносной активности. Продукт написан на языке программирования Java версии 8.

В подразделе 3.1 «Описание работы программы» подробно раскрыт механизм работы приложения, приведены снимки экрана, иллюстрирующие процесс взаимодействия пользователя с разработанной программой.

Завершается работа приложением А – «Листинг программы ApkCheck.jar».

\

ЗАКЛЮЧЕНИЕ

Профессионалы в области информационной безопасности наблюдают непрерывный рост цифровых угроз. Растет и количество вредоносного программного обеспечения, нацеленного на мобильную платформу Android. В последнее время все чаще подтверждается тенденция к коммерциализации мобильных вредоносных программ. Некоторые вредоносные приложения предназначены не только для кражи данных, но и для получения незаконных доходов путем отправки SMS-сообщений на платные номера.

Помимо роста угроз из-за повышения популярности платформы есть и другие проблемы. Процедура верификации программ, реализуемая в официальных источниках получения приложений недостаточно полная и не подходит для использования на рынке приложений. Поэтому порталы мобильных приложений Android притягивают к себе большое количество вредоносных программ, выглядящих в глазах ничего не подозревающих пользователей как легитимные. В результате покупателям официальных магазинов приложений угрожают вредоносные коды, маскирующиеся под безобидные приложения и игры. Пользователи платформы также подвергаются утечкам персональных данных, скрытым загрузкам на веб-сайтах и другим опасностям.

Именно поэтому существует потребность в дополнительном анализе приложений на наличие в них признаков вредоносной активности или недекларированных возможностей.

В ходе дипломной работы были рассмотрены следующие темы: базовая модель работы операционной системы Android, механизм взаимодействия операционной системы и приложения, основные компоненты разработки Android-приложений – и были исследованы параметры приложения, которые могут свидетельствовать о вредоносной активности, произведен анализ большого количества APK-файлов для составления базы сигнатур и форматов

часто встречающихся файлов, а также классифицированного списка ссылок. Также была разработана и реализована программа, которая позволяет произвести анализ APK-файлов для выявления основных сведений о приложении, наличия потенциальной возможности нанести вред пользователю или его устройству. Для этого было проведено исследование на выборке большого числа APK-файлов, составлена база сигнатур и типов внутренних файлов, а также был составлен классифицированный список ссылок, найденных внутри исследуемых APK-файлов. С помощью разработанного программного продукта пользователи могут в удобном формате просматривать основные сведения о приложении, а также делать выводы о вредоносности приложения.

Таким образом, все поставленные задачи были полностью решены, цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Google’s Play Store Hits 25 billion App Downloads, Kicks Off Five Day Sale To Celebrate [Электронный ресурс]. URL: https://techcrunch.com/2012/09/26/google-play-store-25-billion-app-downloads/ (дата обращения 3.09.2016). Загл. с экрана. Яз. англ.

2 Mobile Malware Evolution 2015 [Электронный ресурс]. URL: https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/ (дата обращения 3.09.2016). Загл. с экрана. Яз. англ.

3 Analysis of the Android Architecture [Электронный ресурс]. URL: https://os.itec.kit.edu/downloads/sa_2010_braehler-stefan_android-architecture.pdf (дата обращения 5.09.2016). Загл. с экрана. Яз. англ.

4 The Dalvik Virtual Machine architechture [Электронный ресурс]. URL: http://davidehringer.com/software/android/The_Dalvik_Virtual_Machine.pdf (дата обращения 6.09.2016) Загл. с экрана. Яз. англ.

5 Dalvik bytecode [Электронный ресурс]. URL: https://source.android.com/devices/ tech/dalvik/dalvik-bytecode.html (дата обращения 20.10.2016) Загл. с экрана. Яз. англ.

6 ART and Dalvik [Электронный ресурс]. URL: https://source.android.com/devices /tech/dalvik/ (дата обращения 23.11.2016) Загл. с экрана. Яз. англ.

7 Activity [Электронный ресурс]. URL: https://developer.android.com/reference /android/app/Activity.html (дата обращения 20.10.2016) Загл. с экрана. Яз. англ.

8 Service [Электронный ресурс]. URL: https://developer.android.com/ reference/android/app/Service.html (дата обращения 20.10.2016) Загл. с экрана. Яз. англ.

9 ContentProvider [Электронный ресурс]. URL: https://developer.android.com/ reference/android/content/ContentProvider.html (дата обращения 20.10.2016) Загл. с экрана. Яз. англ.

10 BroadCastReceiver [Электронный ресурс]. URL: https://developer.android.com/reference/android/content/BroadcastReceiver.html (дата обращения 20.10.2016) Загл. с экрана. Яз. англ.
11 Intent [Электронный ресурс]. URL: https://developer.android.com/reference/android/content/Intent.html (дата обращения 20.10.2016) Загл. с экрана. Яз. англ.
12 Основы создания приложений [Электронный ресурс]. URL: https://developer.android.com/guide/components/fundamentals.html?hl=ru (дата обращения 6.09.2016) Загл. с экрана.
13 Компиляция и сборка Anroid приложения [Электронный ресурс]. URL: https://habrahabr.ru/sandbox/63285/ (дата обращения 08.09.2016) Загл. с экрана.
14 Sign Your App [Электронный ресурс]. URL: https://developer.android.com/studio/publish/app-signing.html (дата обращения 08.09.2016) Загл. с экрана. Яз. англ.
15 Leaving our ZIP undone: how to abuse ZIP to deliver malware apps [Электронный ресурс]. URL: https://www.virusbulletin.com/ virusbulletin/ 2015/03/paper-leaving-our-zip-undone-how-abuse-zip-deliver-malware-apps/ (дата обращения 20.09.2016) Загл. с экрана. Яз. англ.
16 Drake, J. Android Hacker’s Handbook [Электронный ресурс] / J. Drake. Wiley, 2014. 545p.
17 Манифест приложения [Электронный ресурс]. URL: https://developer.android. com/guide/ topics/manifest/manifest-intro.html?hl=ru (дата обращения 09.09.2016) Загл. с экрана.
18 An Analysis of Android App Permission [Электронный ресурс]. URL: http://www.pewinternet. org/2015/11/10/an-analysis-of-android-app-permissions/ (дата обращений 11.09.2016) Загл. с экрана. Яз. англ.
19 Android App permessions explained [Электронный ресурс]. URL: http://www.androidauthority.com/android-app-permissions-explained-642452/ (дата обращения 20.11.2016) Загл. с экрана. Яз. англ.
20 Android supported media formats [Электронный ресурс]. URL: https://

developer.android.com/guide/appendix/media-formats.html (дата обращения 10.09.2016) Загл. с экрана. Яз. англ.
21 Эккель, Б. Философия Java. Библиотека программиста / Б.Эккель СПб. : Питер, 2009. 640 с.