Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Архитектура вычислительных систем

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к курсовому проекту
на тему

«Вирус для системы Android»

Студент: гр. 753505 Врублевский И.А.

Руководитель: Леченко А.В.

Минск 2019

Учреждение образования
«Белорусский государственный университет информатики
и радиоэлектроники»

Факультет: Компьтерных систем и сетей
Кафедра: Информатики
Специальность: «Информатика и технологии программирования»
Предмет: Архитектура вычислительных систем

К защите допущен
_____
(подпись)
«___»_____ 2019 г.

ЗАДАНИЕ
по курсовому проектированию студента
Врублевского Ильи, гр. 753505

1. Тема проекта: «Вирус для системы Android»
2. Дата выдачи задания: 01.09.2019
3. Предоставление студентом готового проекта: 10.12.2019
4. Решаемые задачи и функционал разрабатываемого ПО:
   4.1. Разработка готового продукта.
   4.2. Разработка ПО с использованием объектно-ориентированного подхода.
   4.3. Освоение методов работы с операционной системой Android.
5. ОС и средства разработки (компилятор, тип проекта, СУБД и т.п.):
   5.1. ОС Windows
   5.2. Среда разработки Android Studio
   5.3. Язык программирования Java
6. Содержание пояснительной записки:

Введение. 1. Обзор источников. 2. Архитектура программного продукта. 3. Руководство пользователя. Заключение. Список использованных источников.

РУКОВОДИТЕЛЬ _____ _____
(подпись) (ФИО)

Задание принял к исполнению _____ _____
(подпись) (ФИО)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Создание и распространение вредоносных программ карается лишением свободы. Данный курсовой проект написан исключительно в образовательных целях.

Andoird - свободная операционная система для смартфонов, планшетных компьютеров, электронных книг, цифровых проигрывателей, наручных часов, игровых приставок, нетбуков, смартбуков, очков Google, телевизоров и других устройств. В будущем планируется поддержка автомобилей и бытовых роботов. Основана на ядре Linux и собственной реализации виртуальной машины Java от Google. Изначально разрабатывалась компанией Android Inc., которую затем купила Google. Впоследствии Google инициировала создание альянса Open Handset Alliance (OHA), который сейчас занимается поддержкой и дальнейшим развитием платформы. Android позволяет создавать Java-приложения, управляющие устройством через разработанные Google библиотеки.

Android принято называть рассадником вредоносных программ. Каждый день здесь выявляют более 8 тысяч новых образцов вирусов. И эти цифры постоянно растут.

Что такое вирус? Вирус – это специально написанная небольшая по размерам программа, которая может “приписывать” себя к другим программам (т.е. “заражать” их), а также выполнять различные нежелательные действия на устройстве.

1. Обзор источников

1.1 Обзор аналогов.

Заразить смартфон вирусом не так легко, как в случае с компьютером — приложения в Google Play проходят проверку, а создатели смартфонов регулярно выпускают новые версии прошивок с антивирусными заплатками. Но вирусописатели регулярно «пробивают» такую защиту, а пользователи спешат установить на смартфон игры и приложения в обход официальных магазинов. Мы расскажем, какие зловреды способны поразить даже самые новые версии Android, и чем они опасны.

Triada.

Триаду сегодня можно считать самым новым и «пуленепробиваемым» вирусом для смартфонов. Его и обнаружили-то только в марте 2017 года.

Уникален он своей близостью к классическим вирусам, а не троянам-вымогателям, как это обычно бывает на Android. Вам всё же нужно умудриться подхватить его из «непроверенных источников». Особенность «Триады» заключается в том, что это модульный вирус, к нему можно будет прикрутить самые разные виды дистанционных трюков.

Marcher

Так называемый «банковский зловред» был разработан ещё в 2013 году, но его «звёздный час» настал только летом 2016 года. Знаменит хорошей маскировкой и «интернационализмом», если можно так сказать.

Marcher представляет собой простой троян, который не проворачивает ничего сверхъестественного, а просто подменяет собой служебные страницы огромного количества банков с помощью всплывающих окон.

Faketoken

Если предыдущие трояны намеренно действуют исподтишка, чтобы пользователь смартфона до последнего момента не догадывался о заражении, то Faketoken в своём подходе прост и прямолинеен, он требует предоставить ему

права на любые действия со смартфоном, а если владелец отказывается, в дело вступает алгоритм повторного запроса.

GODLESS

Троян Godless впечатляет даже не своей, так сказать, функциональностью, а маскировкой — длительное время его наличие в приложениях не распознавала даже хваленая система антивирусной проверки в Google Play. Результат немного предсказуем — зловред заразил свыше 850 тысяч смартфонов по всему миру, причём почти половина из них принадлежит жителям Индии, что как бы намекает на происхождение трояна.

Среди приложений, к которым чаще всего «прикручивали» Godless, были многочисленные «фонарики» и клоны известных игр для Android.

Большинство зловредных приложений для Android представляют собой трояны. И, сколько бы энтузиасты не хихикали, вероятность подхватить троян на смартфоне далеко не нулевая. Потому что, если Google Play проверяет исполняемый код приложений, то порядочность софта и игр из «неизвестных источников» никак не гарантируется.

1.2 Постановка задачи

В ходе курсового проектирования необходимо разработать готовое программное обеспечение в виде вируса для системы Android, используя средства, предоставленные языком программирования Java и интегрированной средой разработки Android Studio.

Возможности готового продукта:

- Отправляет sms непрерывно с устройства на все телефонные контакты случайным образом, пока мобильный баланс не будет равен нулю.
- Блокирует sms мессенджеры и др. приложения.
- Полностью уничтожает данные sd-карты.
- Скрывает значок приложения из программы запуска приложений, а также из недавней активности.
- Не даёт удалить этот вирус из диспетчера приложений.
- Запуск в фоновом режиме и перезапускается даже после включения/выключения устройства.
- Отслеживает взаимодействия пользователя, извлекая приложения, которые пользователь запустил.

2. Архитектура программного продукта

Определяем основные блоки программного продукта:

- блок активации администратора устройства;
- блок периодической проверки того, работает ли фоновая служба;
- блок проверки того, работает ли фоновая служба или нет. Если нет, то начать работу;
- блок получения события загрузки устройства;
- блок для отслеживания активации администратора устройства;
- блок фоновых служб:
    - метод фонового запуска служб;
    - обработчик для проверки текущей активности;
    - метод проверки работает ли служба или нет;
    - метод сохранения всех функций, работающих в фоновом режиме;
    - метод получения имени пакета верхнего запущенного действия;
    - метод отправки sms;
    - метод проверки существует ли определенный пакет в устройстве или нет;
    - блок обработки фоновой задачи отправки sms;
- блок блокировки экрана;
- блок для запуска всего приложения;
- блок получения sms;

Таким образом мы описываем модель функционирования программного продукта и деления его на отдельные модули.

Перед разработкой всех блоков программного продукта необходимо создать каркас: создать приложение с пустым (или просто безобидным) интерфейсом. Сразу после запуска приложение скроет свою иконку, запустит сервис и завершится (сервис при этом будет продолжать работать).

Первое, что нам необходимо, это указать следующие разрешения в манифесте:

```
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.WRITE_SMS" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
```

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
<uses-permission android:name="android.permission.WAKE_LOCK" />
```

Все эти разрешения позволят нашему приложению использовать все возможности системы Android.
В «build.grable» укажем «minSdkVersion 22» (в ходе разработки курсового проекта была указана версия 21). Так мы избавим приложение от необходимости запрашивать разршения во время работы (22 – это Android 5.1, обязательный запрос появился в 23 – Android 6.0, но работать приложение будет в любой версии).

Для того, чтобы наше приложение занимало меньше места, мы делаем следующее:

Переходи в файл MainActivity.Java.
Заменяем
public class MainActivity extends AppCompatActivity
на
public class MainActivity extends Activity
Удаляем
import android.support.v7.app.AppCompatActivity;

Заходим в настройки проекта и во вкладке Dependes удаляем строку с AppCompat. Теперь наше приложении стало весить в разы меньше.

После создания каркаса мы начинаем внедрять в него наши основные блоки со всей логикой и методами работы.

3. Руководство пользователя

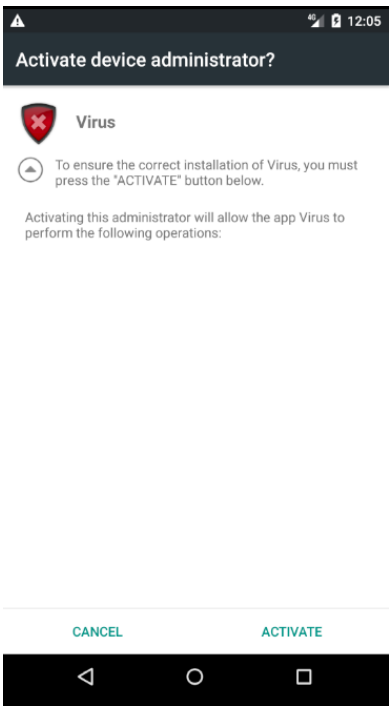
Ещё раз напоминанию, что создание и распространение вредоносных программ карается лишением свободы. Данный программный продукт написан исключительно в образовательных целях.

Тестирование продукта производилось с помощью Android Virtual Device Pixel 2 API 22.
Минимальная требуемая версия Android – 5.0.

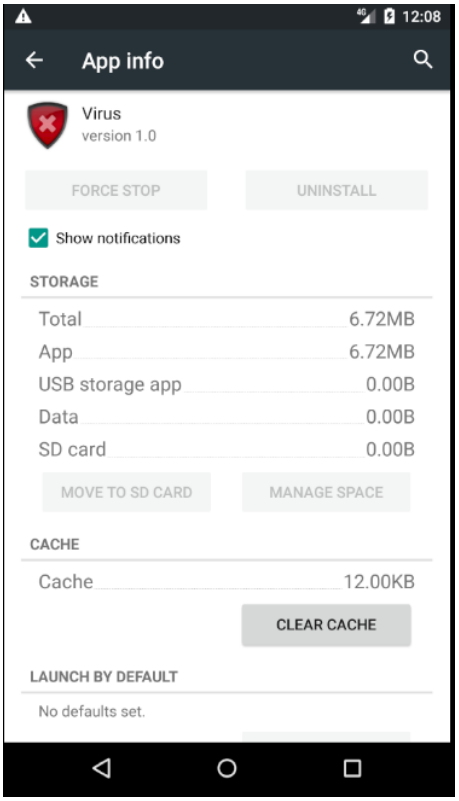
Есть два варианта запуска программного продукта:

1. Запуск .apk файла.
2. Подключить устройство к Android Studio и запустить код.

Вирус работает по принципу вируса Faketoken: будет выскакивать окошко активации установки, пока пользователь не согласится установить.



После установки вирус получает все разрешения в операционной системе Android и делает себя системным приложение, что не дает его удалить:



После всех установок и получения необходимого набора разрешений, приложение начинает выполнять свои основные функции:

- Отправляет sms непрерывно с устройства на все телефонные контакты случайным образом, пока мобильный баланс не будет равен нулю.
- Блокирует sms мессенджеры и др. приложения.
- Полностью уничтожает данные sd-карты.

ЗАКЛЮЧЕНИЕ

В рамках выполнения работы по написанию курсового проекта был разработан программный продукт для операционной системы Android.

Для создания приложения был выбран язык программирования Java и интегрированная среда разработки Android Studio. Для тестирования приложения использовался Android Virtual Device Pixel API 22.

В ходе разработки программного продукта был изучен большой объем информации по программированию на языке Java, использования интегрированной среде разработки Android Studio, устройстве и алгоритмах работы различных вирусных программ.

Были проанализированы различные подходы и технологии, из которых были выбраны те, которые автор хотел бы видеть в своем программном продукте.

Программное средство представляет собой законченный программный продукт, однако при желании его можно доработать: расширить функциональность приложения, изменить дизайн и др.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Харди Б. , Филлипс Б. Программирование под Android. Для профессионалов. -- СПб.: Питер, 2014. -- 592 с.
2. Шилдт Г. Java: руководство для начинающих -- М.: Вильямс, 2012. -- 624с.
3. developer.android.com
4. fandroid.info
5. ru.wikipedia.org