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 Android»

Студент: гр. 753504 Чижик Е. Л.
Руководитель: ассистент кафедры информатики
Леченко А. В.

Минск 2019

Содержание

Введение

Целью данной работы было изучение способов скрытого сбора информации на платформе Android и создание вредоносного ПО, которое будет эти способы реализовывать. Среди его функций — скрытая запись местоположения, СМС, списка приложений, аудио и фото, а также последующая загрузка полученной информации на сервер по заранее заданному URL. Кроме того, приложение скрывает свою иконку и сохраняет себя в автозагрузку, чтобы обезопасить себя от перезагрузки устройства.

1. Получение разрешений

Начиная с Android 6.0, система запрашивает многие необходимые разрешения в процессе выполнения программы, что очевидно не подходит для приложения, которое стремится не выдавать факт своей работы. Однако, это не будет большой проблемой, ведь все указанные в манифесте приложения разрешения можно получить в процессе установки, если установить целевой версией SDK проекта “22”, то есть Android 5.1.

2. Уменьшение размера приложения

Средней размер стандартного Android-приложения почти никогда не составляет меньше нескольких мегабайт, даже при условии отсутствия в нём большого объема ресурсных файлов и сторонних библиотек. Для моей программы такой размер является излишним. Так как данная программа не подразумевает наличия графического интерфейса, мы можем вырезать из его приложения элементы его реализующие. Самое главное — избавиться от библиотек AppCompat и использовать стандартную Activity.

В результате вышеперечисленных действий размер приложения сократился с нескольких мегабайт до ~20 килобайт.

3. Работа приложения в фоновом режиме

Класс Activity нашей программе не очень нужен, поэтому при первом же запуске мы запускаем наш сервис и отключаем MainActivity с помощью PackageManager, таким образом мы не только навсегда отключим MainActivity, но и сразу же спрячем иконку приложения.

Кроме того, необходимо создать BroadcastReceiver, который активируется при включении устройства и запускает главный сервис.

4. Запись данных

Приложение может сохранять местоположение, СМС, список приложений, аудио и фото с помощью специализированных классов, но, чтобы оно сделало это более одного раза (при запуске), нам необходимо настроить запись по расписанию. Для этого используются классы Alarm Manager и BroadcastReceiver. Я настроил приложение на запись и отправку данных каждые 30 минут.

5. Скрытое использование камеры

При работе с камерой на Android возникают некоторые сложности, так как система предоставляет для этого сразу два API: классический и Camera2, появившийся в версии 5.0 и стал основным в 7.0. К тому Camera2 часто может работать некорректно на более старых версиях ОС.

Стоит также отметить, что делать фото каждые N минут не имеет смысла, ведь гораздо разумнее делать снимок фронтальной камерой при разблокировке смартфона. Для этого необходимо создать отдельный BroadcastReceiver, и задать включение экрана в качестве его триггера в манифесте приложения.

6. Загрузка данных на сервер

Загрузка файлов на сервер с помощью Java весьма осложнена. Подобные действия как правило осуществляют с помощью различных сторонних библиотек, например OkHttp, однако, они серьезно раздувают размер приложения, поэтому я формирую запрос вручную, преобразуя файлы в байтовые массивы.

Заключение

В ходе выполнения данной работы была создана троянская программа, осуществляющая скрытый сбор информации и её загрузку на сервер. В итоге я узнал много нового о способах получения информации, незаметных пользователю и о том, как просто можно спрятать вредоносное ПО на устройстве.

Стоит всё же отметить, что по ходу выпуска новых версий Android, система становится более защищенной от подобных программ и некоторые ключевые возможности данного ПО могут быть недоступны на более поздних версиях ОС.

Список использованной литературы

1. Android Camera2 summary (GPUs) [Электронный ресурс]. - Электронные данные. - Режим доступа: (https://developer.android.com/ reference /android/hardware/camera2/summary)
2. Upload files to WEB API service [Электронный ресурс]. - Электронные данные. - Режим доступа: (https://bitbucket.org/hintdesk/android-upload-files-to-asp.net-web-api-service)
3. Информационная безопасность [Электронный ресурс]. - Электронные данные. - Режим доступа: (https://www.spy-soft.net/)
4. Практическая безопасность [Электронный ресурс]. - Электронные данные. - Режим доступа: (https://www.cryptoworld.su/)