Содержание статьи

- Инструментарий
  - Libmagic.rb
  - Yara-python-dex
  - Androguard
  - Androguard.core.bytecodes.apk и androguard.core.bytecodes.dvm.DalvikVm
  - Strace
  - Dex2jar
- Поиск вредоносных приложений
- Уязвимости APK файлов
- Уязвимости в DEX файлах
- Поиск в анализе кода
- Автоматизируем анализ с помощью androguard
  - Анализ набора данных
  - Анализ одного APK
  - Анализ одного classes.dex
  - Анализ одного classes.dex с использованием фильтра
  - Анализ одного classes.dex с использованием фильтра и сохранением результатов
- Заключение

Привет, читатель, что бы тебе никогда не встретить вредоносный файлик, но если вдруг все-таки встретишь, то в этой статье мы расскажем, как быстрее и проще его найти, что же делает этот и кому вредоносный набор делает, при его помощи можно. В этом поможет Android-malware, Yara, Strace, Dex2jar, Androguard и немного Linux.

В целом, если говорить про анализ вредоносного файла, можно выделить два подхода — это статический анализ и динамический анализ.

Статический анализ предполагает запуск файла без его запуска на выполнение. Это может быть дизассемблер, а также скрипты на его основе или другие инструменты, которые позволяют нам получить информацию о файле, не запуская его. Динамический анализ предполагает запуск файла в изолированной среде, в которой мы можем отследить его поведение, сетевой трафик, а также ресурсы, которые он использует. Вредоносный набор может использовать несколько способов для того, чтобы не запускаться в виртуальной среде, но в большинстве случаев, если вы не ленитесь, то можете обойти все эти ограничения.

Инструментарий

APK инструмент

Один из основных инструментов в статическом бинарном анализе — это APK инструмент. Он позволяет разбирать APK файлы, а также собирать их обратно. Для его использования, нам нужно Java Runtime. А если хотим его из исходников, то еще и ant. Для использования APK инструмента достаточно скачать последнюю версию с официального сайта. Для запуска APK инструмента, нам нужно выполнить следующую команду. В зависимости, от того, в каком виде вы скачали APK инструмент, вы можете использовать или apktool.jar, или apktool.bat. Для Linux-подобных систем, apktool.jar, для Windows — apktool.bat.

```
$ apktool.jar
```

Для использования APK инструмента, нужно выполнить следующую команду:

```
$ apktool.jar d -f -s -o <dir_name> <file_name>
```

Опция d — это decode, опция f — это force, если папка уже существует, то нужно перезаписать ее, опция s — это не декодировать classes.dex, опция o — это output, после нее нужно указать имя папки, куда будет распаковываться APK файл.

Libmagic.rb

Libmagic.rb — это утилита для определения типа файла. Для ее использования нужно выполнить следующую команду:

```
$ file -m magic.mgc -f -b -k -n -p -s -z -e tokens -e soft -e cdf -e elf -e tar -e apprentice -e compress -e simh -e cdf -e dbf -e dump -e dvi -e ea05 -e ea06 -e encrypt -e fsmagic -e fsmatch -e mime -e mime-encoding -e pdf -e pdf -e pdf
```

Файл test.csv

Если нужно сделать выборку по нескольким критериям, то можно использовать несколько фильтров, либо по каждому фильтрует ещё бесконечное число новых значений, либо на каждом фильтрует по нескольким критериям. Для фильтрации по нескольким критериям нужно перечислить через пробел, через запятую или в скобках, если по выражению.

На Python можно сделать следующий скрипт для выполнения таблицы запросов:

```
cmdlet -p=?
cmdlet -p=?
cmdlet -p=?
```