ANDROID FORENSICS

Bitdefender

OVERVIEW

- **Forensics:** *the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.*
- **Forensics revolves around what information can be extracted from:**
  - **Applications**
  - **Device**
  - **User information**

DATA ACQUISITION - APPLICATION DATA

COLLECTING ALL DATA RELATED TO USER (AND/OR) SYSTEM APPLICATIONS

- USING ANDROID SDK TOOLS – ANDROID DEBUG BRIDGE (ADB) BACKUP COMMAND
- APPLICATIONS TARGETING ANDROID 12 HAVE THIS DISABLED BY DEFAULT
- PREVIOUSLY YOU COULD RESTRICT THIS USING THE ANDROID:ALLOWBACKUP MANIFEST TAG

```
adb backup [-f <file>] [-apk | -noapk] [-obb | -noobb] [-shared | -noshared]
                [-all] [-system | -nosystem] [<packages...>]

- write an archive of the device's data to <file>
```

All apps backup: **adb backup -apk -obb -shared -all –system**
3rd party installed apps: **adb backup -apk -obb -shared -all –nosystem**
On some systems the arguments must be passed as a string
adb backup '-apk -obb -shared -all –system'

DATA ACQUISITION - APPLICATION DATA

EXTRACTED DATA IS STORED TO AN .AB (ADB BACKUP) FILE IN A SPECIFIC FORMAT

- EXTRACT DATA (ADBEXTRACTOR) AND ANALYZE

```
apps/org.myapp/_manifest
apps/org.myapp/a/org.myapp-1.apk
apps/org.myapp/f/share_history.xml
apps/org.myapp/db/myapp.db-journal
apps/org.myapp/db/myapp.db
apps/org.myapp/sp/org.myapp_preferences.xml
```

```
java -jar abe.jar unpack backup.ab dec_backup.tar
```

DATA ACQUISITION - APPLICATION DATA

- For SD content acquisition
  - Standard file transfer mechanism
  - Take out SD CARD – use forensics tools (e.g. Autopsy)
  - adb tool: `adb pull /sdcard/`
- Without root or the adb backup files there is no other way to extract private app data

Data Acquisition – User Content

- **User data:**
  - **SMS**, call log, contacts, **MMS** messages, accounts
  - extract using an application as proxy
    - An old example application
    - Apps can be found on Google Play
- **Otherwise can not be accessed without root**
  - content is saved in application **SQLite** dbs
    - E.Q. `/data/data/com.android.providers.telephony/databases`

SYSTEM - ANALYSIS

- Linux related data
  - Forensics tools for Linux
- Android OS related Data
  - Data is collected using available tools such as:
    - ADB – tools are executed through its shell
      - PM – applications related information
      - Logcat – system and application logging
      - Dumpsys – very useful system information dumper

SYSTEM - ANALYSIS

- **PM RELATED COMMANDS. CHECKING INSTALLED APPLICATIONS**

Want do we want (to know)	How can we get it - Command
All installed applications with path	pm list packages -f
Third party installed applications with path	pm list packages -f -3
Third party installed applications with path and install source	pm list packages -f -3 -i
Disabled third party applications	pm list packages -d -3 –f
When was an application installed (look for **firstInstallTime**)	pm dump <package_name> dumpsys package <package_name>

SYSTEM - ANALYSIS

- **Activation mechanism.**
  - **How to identify application callbacks**
- **Checking applications receivers for events/specific intents**
  - **Query for specific receivers for package has been added snce Android 7.0**

Want do we want (to know)	How can we get it - Command
Alarms registered on the device	dumpsys alarm
Jobs registered on the device	dumpsys jobscheduler
Intents broadcast current state and history	dumpsys activity

SYSTEM - ANALYSIS

- **Activation mechanism. Callbacks and extra (dangerous) functionality**

Want do we want (to know)	How can we get it - Command
View enabled device admin applications by package name	dumpsys device_policy
Show default MIME Types used applications, package warning messages and other	dumpsys package
Show android accessibility enabled applications information	dumpsys accessibility

SYSTEM - ANALYSIS

- **SYSTEM STATE INFORMATION; CPU, MEMORY, WIFI**

Want do we want (to know)	How can we get it - Command
Show process CPU usage	dumpsys cpuinfo
Show applications memory usage	dumpsys meminfo
Application usage history	dumpsys usagestats
See accounts and account history	dumpsys account
Wifi network related information	dumpsys wifi
Entire device state (a lot of data)	dumpstate

SYSTEM - ANALYSIS

- **UI/Launcher modification and extensions**

Want do we want (to know)	How can we get it - Command
Show installed widgets	dumpsys appwidget
Show information about shortcuts	dumpsys shortcut
Get notifications information	dumpsys notification

APPLICATION ANALYSIS

- **RUNTIME INFORMATION EXTRACTION**
  - **LOGCAT**
    - **ANDROID SYSTEM AND APPLICATION LOGGING**
    - **IDENTIFIED BY PROCESS PID/APPLICATION**
    - **SUPPORTS MULTIPLE DATA BUFFERS; USE ALL**

Command
adb logcat -b all -v threadtime
adb logcat -b radio -b main -b events -b crash -b system -v threadtime

APPLICATION ANALYSIS

- **APK INFORMATION EXTRACTED FROM THE RUNNING INSTANCE**

Command
pm dump **<package_name>**
dumpsys package **<package_name>**

TARGETED APPLICATION FORENSICS

- For some applications, you can find forensics artefacts on the file system
- Even with the original application removed, these artefacts can remain
- Can providing a basic timeline, at minimum

Application	File system artifact path
WhatsApp	/sdcard/Android/media/com.whatsapp/WhatsApp/Media/WhatsApp Documents/
Telegram	/sdcard/Download/Telegram/


Q&A