Static Analysis - fakeAV_148B76C664F2854E2947

APP SCORE

Average CVSS Score: 5.3

App Security Score: 35/100

Trackers Detection: 0/227

FILE INFORMATION

Name: fakeAV_148B76C664F2854E2947AF01160FFA99_LabelReader.apk

Size: 20.96MB

MD5: 0a9d7da32cf6d7db5b6407321b673d3e

SHA1: 30b6d55096b008a2dc7b54382f094568346362ef

SHA256: 8bc0f8a088ead0745b5c4f12d3044c253f70a7ff368aef1e64ebbea3fcc51

APP INFORMATION

Name: Label_Reader

Package Name: com.example.androiddefender2

Main Activity: com.example.androiddefender2.MainActivity

Target SDK: 16

Min SDK: 9

Max SDK:

Android Version Name: 1.0

Android Version Code: 1

PLAY STORE INFORMATION

CERTIFICATE

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unk
Signature Algorithm: dsa
Valid From: 2013-08-10 17:15:36+00:00
Valid To: 2040-12-26 17:15:36+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unkn
Serial Number: 0x52067538
Hash Algorithm: sha1
md5: 8c1ac87f0d91056c992dbba9f92445fc
sha1: bef7c90edce577a4b04c25d32b452f9b1209a8c7
sha256: 0218aa9ba94f0b1d4d1a781560c2118b3c1cad9efb4bda5198b8
sha512: 2cbb4d9b1e5e70b7d7b102e36d6b8a3e64540039c6dd9f8d744

Certificate Status: Bad
Description: The app is signed with `SHA1withRSA`. SHA1 hash algorith

PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
com.android.launcher.permission.INSTALL_SHORTCUT	normal		Allows an application to install a shortcut in Launcher.

ANDROID LIBRARY BINARY ANALYSIS

ISSUE	SEVERITY	DESCRIPTION	FILES
No issue found info			

APKiD ANALYSIS

APKiD not enabled.

FILE

BROWSABLE ACTIVITIES

ACTIVITY INTENT

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (com.worker.androiddefender2.CallReceiver) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (com.worker.androiddefender2.MessageReceiver) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Broadcast Receiver (com.worker.androiddefender2.ServiceStarter) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Broadcast Receiver (DefenderAppWidgetProvider) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
High Intent Priority (999) [android:priority]	medium	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

ISSUE	SEVERITY	CVSS	CWE	OWASP	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	**2.3**	**CWE-327**		com/j256/ormlite/field/FieldType.java com/j256/ormlite/android/AndroidCompiledStatement.java com/j256/ormlite/android/AndroidDatabaseConnection.java com/j256/ormlite/android/AndroidConnectionSource.java com/j256/ormlite/android/AndroidDatabaseResults.java com/j256/ormlite/android/apptools/OrmLiteBaseActivity.java com/j256/ormlite/android/apptools/OrmLiteSqliteOpenHelper.java com/j256/ormlite/dao/LazyForeignCollection.java com/j256/ormlite/dao/DaoManager.java com/j256/ormlite/dao/EagerForeignCollection.java
App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	high	**5.9**	**CWE-89**	**M7: Client Code Quality**	com/j256/ormlite/android/AndroidCompiledStatement.java com/j256/ormlite/android/AndroidDatabaseConnection.java com/example/androiddefender2/DBHelper.java
The App logs information. Sensitive information should never be logged.	info	**7.5**	**CWE-532**		com/j256/ormlite/android/AndroidLog.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/j256/ormlite/logger/LocalLog.java com/example/androiddefender2/DefenderAppWidgetProvider.java com/worker/helper/ORMDatabaseHelper.java com/worker/androiddefender2/AVService.java system/Communicator.java system/XMLParser.java system/ThreadControl.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	**5.5**	**CWE-276**	**M2: Insecure Data Storage**	com/example/androiddefender2/ScanningActivity.java com/example/androiddefender2/SingleScanActivity.java com/worker/androiddefender2/FilesWorker.java
IP Address disclosure	warning	**4.3**	**CWE-200**		com/example/androiddefender2/UpdateActivity.java com/example/androiddefender2/DefenderApplication.java com/worker/androiddefender2/MemoryFunctions.java
The App uses an insecure Random Number Generator.	high	**7.5**	**CWE-330**	**M5: Insufficient Cryptography**	com/worker/androiddefender2/SystemFunctions.java com/worker/androiddefender2/SignaturesWorker.java
App can write to App Directory. Sensitive Information should be encrypted.	info	**3.9**	**CWE-276**		com/worker/androiddefender2/MemoryFunctions.java

ANDROID API

API	FILES

API	FILES
Get System Service	designer/TabsOperation.java com/example/androiddefender2/ScanningActivity.java com/example/androiddefender2/UpdateActivity.java com/example/androiddefender2/DefenderApplication.java com/example/androiddefender2/NumbersList.java com/example/androiddefender2/SingleScanActivity.java com/worker/androiddefender2/SkanerSystemWorker.java com/worker/androiddefender2/SystemFunctions.java com/worker/androiddefender2/TimeAlarm.java com/worker/androiddefender2/PreparerWirusesSkaner.java com/worker/androiddefender2/AVService.java com/worker/androiddefender2/CallReceiver.java
Inter Process Communication	designer/TabsOperation.java com/example/androiddefender2/ScanningActivity.java com/example/androiddefender2/BySupportActivity.java com/example/androiddefender2/DefenderApplication.java com/example/androiddefender2/HomeActivity.java com/example/androiddefender2/VirusInfoDialogActivity.java com/example/androiddefender2/SingleScanActivity.java com/example/androiddefender2/ScanActivity.java com/example/androiddefender2/DefenderAppWidgetProvider.java com/example/androiddefender2/ByWithScanActivity.java com/example/androiddefender2/CustomActGroup.java com/example/androiddefender2/PayFormActivity.java com/example/androiddefender2/BlackList.java com/example/androiddefender2/PrivacyActivity.java com/example/androiddefender2/SupportActivity.java com/example/androiddefender2/MainActivity.java com/worker/androiddefender2/NetworkAlarm.java com/worker/androiddefender2/SystemFunctions.java com/worker/androiddefender2/TimeAlarm.java com/worker/androiddefender2/MessageReceiver.java com/worker/androiddefender2/AVService.java com/worker/androiddefender2/ServiceStarter.java com/worker/androiddefender2/CallReceiver.java
Java Reflection	com/j256/ormlite/table/DatabaseTableConfig.java com/j256/ormlite/table/DatabaseTableConfigLoader.java com/j256/ormlite/field/DatabaseFieldConfigLoader.java com/j256/ormlite/field/DataPersisterManager.java com/j256/ormlite/field/FieldType.java com/j256/ormlite/field/DatabaseFieldConfig.java com/j256/ormlite/field/DataPersister.java com/j256/ormlite/field/types/VoidType.java com/j256/ormlite/field/types/SerializableType.java com/j256/ormlite/field/types/BaseDateType.java com/j256/ormlite/field/types/DateTimeType.java com/j256/ormlite/field/types/SqlDateType.java com/j256/ormlite/field/types/TimeStampType.java com/j256/ormlite/field/types/BaseEnumType.java com/j256/ormlite/field/types/BaseDataType.java com/j256/ormlite/android/DatabaseTableConfigUtil.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/j256/ormlite/android/apptools/OpenHelperManager.java com/j256/ormlite/misc/JavaxPersistence.java com/j256/ormlite/db/BaseDatabaseType.java com/j256/ormlite/logger/LoggerFactory.java com/example/androiddefender2/CustomActGroup.java com/worker/androiddefender2/CallReceiver.java
Starting Activity	com/example/androiddefender2/BySupportActivity.java com/example/androiddefender2/VirusInfoDialogActivity.java com/example/androiddefender2/ScanActivity.java com/example/androiddefender2/DefenderAppWidgetProvider.java com/example/androiddefender2/ByWithScanActivity.java com/example/androiddefender2/CustomActGroup.java com/example/androiddefender2/PayFormActivity.java com/example/androiddefender2/BlackList.java com/example/androiddefender2/SupportActivity.java com/example/androiddefender2/MainActivity.java com/worker/androiddefender2/NetworkAlarm.java com/worker/androiddefender2/TimeAlarm.java com/worker/androiddefender2/MessageReceiver.java com/worker/androiddefender2/ServiceStarter.java com/worker/androiddefender2/CallReceiver.java

API	FILES
Local File I/O Operations	com/example/androiddefender2/BySupportActivity.java com/example/androiddefender2/SettingsActivity.java com/example/androiddefender2/UpdateActivity.java com/example/androiddefender2/DefenderApplication.java com/example/androiddefender2/VirusInfoDialogActivity.java com/example/androiddefender2/SingleScanActivity.java com/example/androiddefender2/ScanActivity.java com/example/androiddefender2/PayFormActivity.java com/example/androiddefender2/PrivacyActivity.java com/example/androiddefender2/SupportActivity.java com/worker/androiddefender2/SkanerSystemWorker.java com/worker/androiddefender2/NetworkAlarm.java com/worker/androiddefender2/MemoryFunctions.java com/worker/androiddefender2/TimeAlarm.java com/worker/androiddefender2/PreparerWirusesSkaner.java com/worker/androiddefender2/MessageReceiver.java com/worker/androiddefender2/ServiceStarter.java com/worker/androiddefender2/CallReceiver.java
Starting Service	com/example/androiddefender2/DefenderApplication.java
Sending Broadcast	com/example/androiddefender2/DefenderApplication.java com/worker/androiddefender2/SystemFunctions.java
Android Notifications	com/worker/androiddefender2/SkanerSystemWorker.java com/worker/androiddefender2/SystemFunctions.java com/worker/androiddefender2/TimeAlarm.java com/worker/androiddefender2/PreparerWirusesSkaner.java
HTTP Requests, Connections and Sessions	system/Communicator.java

URLS

URL	File
http://defenderandroid.org	com/example/androiddefender2/SupportActivity.java

FIREBASE DATABASES

MALWARE CHECK

Domain	Status
defenderandroid.org	good

EMAILS

TRACKERS

Tracker Name	URL

FILE ANALYSIS

STRINGS

```
"app_name" : "Label_Reader"
"hello_world" : "Hello world!"
"menu_settings" : "Settings"
"title_activity_main" : "Android Defender"
"title_activity_update" : "UpdateActivity"
"title_activity_settings" : "SettingsActivity"
"title_activity_privacy" : "PrivacyActivity"
"title_activity_support" : "SupportActivity"
"title_activity_home" : "HomeActivity"
"Scansystem" : "Сканирование системы"
"title_activity_scan" : "ScanActivity"
"empty" : ""
"title_activity_scanning" : "ScanningActivity"
"scan_result" : "Результаты сканирования"
"new_signatur_count" : "Количество новых сигнатур"
"list_updates" : "Список обновлений"
"clear_files" : "0/0"
"zero_percent" : "0%"
"version_base" : "Версия баз:"
"count_signaturs" : "Количество сигнатур:"
"last_scan_date" : "Дата последнего сканирования:"
"settings_autostart" : "Автозапуск (запуск при старте системы)"
"settings_startscan" : "Запускать сканер при запуске"
"settings_minimize" : "Минимизировать при запуске"
"settings_message" : "Уведомления"
"warning_msg_f" : "Ваше устройство не полностью защищено"
"warning_msg_s" : "Преобретите полную версию антивируса"
"btn_save" : "Сохранить настройки"
"btnCancel" : "Назад"
"date_last_scan_text" : "Последнее сканирование:"
"txtMond" : "Пн."
"txtTuesd" : "Вт."
"txtWedn" : "Ср."
"txtThursd" : "Чт."
"txtFri" : "Пт."
"txtSatur" : "Сб."
"txtSand" : "Вс."
"push_auto_scan" : "Включить автоматическое сканирование"
"txt_sub_center_home_block" : "светлый центральный блок"
"txt_logo_image" : "Логотип"
"txt_dark_center_block" : "Темный центральный блок"
```

```
"start_auto_scan" : "Начать автоматическое сканирование"
"start_scan_btn" : "Начать сканировать"
"scan_application" : "Сканировать приложения"
"scan_sd" : "Сканировать SD карту"
"txt_img_warn" : "Внимание"
"full_protect" : "Полная защита устройства"
"status_scan" : "Статус сканирования"
"finded_warnings" : "Найденные угрозы"
"process_scan" : "Процесс сканирования"
"by_and_remove_virus" : "Купить и устранить угрозы"
"go_with_virus" : "Продолжить незащищенным"
"set_settings_app" : "Настройки приложения"
"privacy_sms" : "Защита от кражи СМС"
"privacy_settings" : "Настройки приватности"
"privacy_phone" : "Защита от записи тел. разговоров"
"privacy_geolokation" : "Запретить несанкц. геолокацию"
"black_list" : "Черный список"
"by_prg" : "Купить"
"privacy_reklam_text" : "Активация приложения дает вам
неограниченные возможности управления программой. Вы
можете самостоятельно настроить все необходимые модули
контроля безопасности вашего устройства. Кроме того, вы
можете управлять черным списком."
"title_activity_black_list" : "BlackList"
"not_get_call" : "Не принимать звонки"
"not_get_sms" : "Не принимать СМС"
"add_to_black_list" : "Добавить в черный список"
"reklam_black_list" : "Функция черный список доступна только в
купленной версии приложения. Вы можете индивидуально
настраивать контакт на прием только СМС или только Звонков, А
также запретить все."
"show_black_list" : "Показать список номеров"
"title_activity_numbers_list" : "NumbersList"
"delete_from_black_list" : "Удалить из черного списка"
"actual_base" : "Актуальность баз"
"txt_upd_string" : "Список обновлений"
"txt_upd_reklam" : "Обновление антивирусных баз доступно только
в платной версии. Если антивирусные базы не будут оставаться
актуальными, вы рискуете подвергнуть ваше устройство риску
заражения"
"txt_update_system" : "Обновление системы"
"txt_full_guard" : "Ваше устройство полностью защищено"
"full_reklam_scan_text" : "Ваше устройство подвержено
заражению. Приобретите полную версию антивируса"
```

```
"virus_remove" : "устранена"
"virus_not_remove" : "не устранена"
"stop_scan" : "Стоп"
"privacy_activate" : "Приложение активировано. У вас есть неограниченые возможности управления программой. Вы можете самостоятельно настроить авто статус сканирования, обновление антивирусных баз."
"activate_application" : "Активация приложения"
"i_have_key_activation" : "У меня уже есть ключ активации"
"txt_go_scan" : "Старт"
"txt_pause_scan" : "Пауза"
"txt_prepare_status_scan" : "Статус сканирования"
"txt_scan_string" : "Сканировать приложения"
"test_file" : "/data/new.mp3"
"notify_scanning" : "Сканирование..."
"notify_scanning_process" : "Процесс сканирования"
"notify_scanning_files" : "Проверка файла №"
"prepare_scan_string" : "Найдено угроз: 0. Устранено угроз: 0"
"scanning_found_defect" : "Найдено угроз: %s."
"scanning_deleted_defect" : "Устранено угроз: %s"
"prepare_files_step" : "Подготовка файлов"
"scanning_system_step" : "Сканирование системы"
"scanning_sdcard_step" : "Сканирование SD карты"
"filter_incoming_header" : "Фильтр входящего звонка"
"filter_incoming_message" : "Входящий звонок с номера %s заблокирован"
"filter_outcoming_header" : "Фильтр исходящего звонка"
"filter_outcoming_message" : "Произведен исходящий вызов на номер %s"
"warning_you_have_virus" : "Внимание, обнаружен вирус %s."
"txt_activate" : "Активировать"
"txt_err_activate_code_empty" : "Код активации не может быть пустым"
"txt_err_activate_code_incorrect" : "Неверный код активации"
"title_activity_by_support" : "BySupportActivity"
"action_settings" : "Settings"
"txt_scanning_warning" : "Дождитесь завершения сканирования"
"txt_results_scan" : "Результаты сканирования"
"txt_results_version" : "Версия антивирусных баз"
"txt_error_scan_settings" : "Для начала сканирования, отметьте одну из опций сканирования"
"txt_error_sdcard_notexists" : "SD карта не найдена на вашем устройстве"
"txt_sucefful_activated" : "Приложение успешно активировано,
спасибо за покупку"
"btn_save_small" : "Сохранить"
"txt_last_base_av" : "На данный момент у вас самые актуальные базы"
"txt_filtered" : "Фильтруется"
"txt_cancel" : "Отмена"
"txt_information" : "Информация"
"txt_delete_phone" : "Удалить телефон"
"txt_succefuly_delete_phone" : "Номер %s успешно удален из черного списка"
"title_activity_single_scan" : "SingleScanActivity"
"txt_ok" : "OK"
"txt_add_black_header" : "Добавлено"
"txt_add_black_message" : "Номер телефона %s добавлен в черный список"
"txt_add_black_error_header" : "Ошибка добавления"
"txt_add_black_warning_header" : "Предупреждение"
"txt_add_black_warning_message" : "Номер телефона %s уже есть в черном списке"
"txt_add_black_warning_params_header" : "Ошибка параметров"
"txt_add_black_warning_params_message" : "Номер телефона не может быть пустым. Хотябы одна из опций ограничения должна быть включена"
"support_manager" : "Служба поддержки"
"field_for_key" : "Поле для ввода ключа"
"scan_close" : "Закрыть"
"resume_working" : "Продолжить"
"success_key_header" : "Успешная активация"
"success_key_message" : "Вы успешно активировали приложение, для продолжения нажмите кнопку Продолжить"
"title_activity_virus_info_dialog" : "VirusInfoDialogActivity"
"txt_attention" : "Внимание!"
"txt_may_infection" : "Возможно заражение"
"txt_attention_message" : "На вашем устройстве обнаружена вредоносная активность!"
"txt_attention_process" : "Вирусная активность обнаружена в процессе:"
"txt_attention_protect" : "Для включения защиты активируйте приложение:"
"txt_hack_message" : "Передача данных не защищена!"
"txt_hack_process" : "Ваш телефон не защищен и может быть подвергнут хакерской аттаке"
"txt_sms_message" : "Обнаружена вирусная активность в СМС переписке"
```

```
"title_activity_pay_form" : "PayFormActivity"
"test_test_test" : "Тестим 123"
"scan_is_going" : "Идет сканирование устройства"
"scan_now_working" : "В данный момент идет сканирование
вашего устройства."
"scan_congratiulation" : "Благодарим за установку нашего
антивирусного ПО, мы надеемся что вы останитесь довольны!"
"install_widget" : "Установка виджета"
"install_widget_try_msg" : "Мы стараемся сделать использование
нашего ПО более удобным, не забудьте установить наш виджет."
"widget_fast_scan" : "Быстрое сканирование"
"app_name" : "Label_Reader"
"hello_world" : "Hello world!"
"menu_settings" : "Settings"
"title_activity_main" : "Android Defender"
"title_activity_update" : "UpdateActivity"
"title_activity_settings" : "SettingsActivity"
"title_activity_privacy" : "PrivacyActivity"
"title_activity_support" : "SupportActivity"
"title_activity_home" : "HomeActivity"
"Scansystem" : "Scan system"
"title_activity_scan" : "ScanActivity"
"empty" : ""
"title_activity_scanning" : "ScanningActivity"
"scan_result" : "Scan results"
"new_signatur_count" : "Number of new patterns"
"list_updates" : "List of updates"
"clear_files" : "0/0"
"zero_percent" : "0%"
"version_base" : "Database version:"
"count_signaturs" : "Number of patterns:"
"last_scan_date" : "Last scan date:"
"settings_autostart" : "Autorun"
"settings_startscan" : "Launch scanner when phone starts"
"settings_minimize" : "Minimize upon launch"
"settings_message" : "Notifications"
"warning_msg_f" : "Your device is not fully protected"
"warning_msg_s" : "Buy full version of antivirus"
"btn_save" : "Save settings"
"btnCancel" : "Back"
"date_last_scan_text" : "Last scan date:"
"txtMond" : "Mon."
"txtTuesd" : "Tue."
"txtWedn" : "Wed."
```

```
"txtThursd" : "Thu."
"txtFri" : "Fri."
"txtSatur" : "Sat."
"txtSand" : "Sun."
"push_auto_scan" : "Enable automatic scanning"
"txt_sub_center_home_block" : "светлый центральный блок"
"txt_logo_image" : "Логотип"
"txt_dark_center_block" : "Темный центральный блок"
"start_auto_scan" : "Start automatic scanning"
"start_scan_btn" : "Start scanning"
"scan_application" : "Scan applications"
"scan_sd" : "Scan SD card"
"txt_img_warn" : "Внимание"
"full_protect" : "Full protection of device"
"status_scan" : "Scanning status"
"finded_warnings" : "Threats detected"
"process_scan" : "Scanning process"
"by_and_remove_virus" : "Buy and eliminate threats"
"go_with_virus" : "Continue unprotected"
"set_settings_app" : "Application settings"
"privacy_sms" : "SMS fraud protection"
"privacy_settings" : "Privacy settings"
"privacy_phone" : "Phone call recording protection"
"privacy_geolokation" : "Disable unauthorized geolocation"
"black_list" : "Black list"
"by_prg" : "Buy"
"privacy_reklam_text" : "Activating the application gives you unlimited options of adjusting program settings. You can adjust the settings for any required modules for controlling the security of your device. In addition, you can manage the black list."
"title_activity_black_list" : "BlackList"
"not_get_call" : "Reject calls"
"not_get_sms" : "Reject messages"
"add_to_black_list" : "Add to black list"
"reklam_black_list" : "The black list feature is available only in the application version you have to buy. You can adjust settings to accept just messages or calls from individuals, as well as reject both."
"show_black_list" : "Show list of numbers"
"title_activity_numbers_list" : "NumbersList"
"delete_from_black_list" : "Remove from black list"
"actual_base" : "Database up-to-dateness"
"txt_upd_string" : "List of updates"
"txt_upd_reklam" : "Updating antivirus databases is available for the paid edition only. Unless your antivirus databases are current, you
```

```
device is at risk of being infected."
"txt_update_system" : "System update"
"txt_full_guard" : "Your device is fully protected"
"full_reklam_scan_text" : "Your device is at risk of being infected.
Please purchase the full edition of the antivirus."
"virus_remove" : "eliminated"
"virus_not_remove" : "not eliminated"
"stop_scan" : "Stop"
"privacy_activate" : "Application activated. You now have unlimited
possibilities of managing the program. You can set auto scan status
and schedule antivirus database updates yourself."
"activate_application" : "Application activation"
"i_have_key_activation" : "I already have an activation key"
"txt_go_scan" : "Start"
"txt_pause_scan" : "Pause"
"txt_prepare_status_scan" : "Scan status"
"txt_scan_string" : "Scan applications"
"test_file" : "/data/new.mp3"
"notify_scanning" : "Scanning..."
"notify_scanning_process" : "Scan process"
"notify_scanning_files" : "Checking file №"
"prepare_scan_string" : "Threats found: 0. Threats eliminated: 0"
"scanning_found_defect" : "Threats found: %s."
"scanning_deleted_defect" : "Threats eliminated: %s"
"prepare_files_step" : "Preparation of files"
"scanning_system_step" : "System scan"
"scanning_sdcard_step" : "SD card scan"
"filter_incoming_header" : "Incoming call filter"
"filter_incoming_message" : "Incoming call from phone number %s
blocked"
"filter_outcoming_header" : "Outgoing call filter"
"filter_outcoming_message" : "Outgoing call made to phone number
%s"
"warning_you_have_virus" : "Warning, virus detected %s."
"txt_activate" : "Activate"
"txt_err_activate_code_empty" : "Activation code field can not be
blank"
"txt_err_activate_code_incorrect" : "Incorrect activation code"
"title_activity_by_support" : "BySupportActivity"
"action_settings" : "Settings"
"txt_scanning_warning" : "Please wait until scan is finished"
"txt_results_scan" : "Scan results"
"txt_results_version" : "Virus database:"
"txt_error_scan_settings" : "To start scanning, please select one of the
```

scanning options"
"txt_error_sdcard_notexists" : "SD card not found on your device"
"txt_sucefful_activated" : "Application successfully activated, thank you for your purchase"
"btn_save_small" : "Save"
"txt_last_base_av" : "Your databases are currently up-to-date"
"txt_filtered" : "Filtering"
"txt_cancel" : "Cancel"
"txt_information" : "Information"
"txt_delete_phone" : "Remove phone number"
"txt_succefuly_delete_phone" : "Phone number %s successfully removed from black list"
"title_activity_single_scan" : "SingleScanActivity"
"txt_ok" : "OK"
"txt_add_black_header" : "Added"
"txt_add_black_message" : "Phone number %s added to black list"
"txt_add_black_error_header" : "Error while adding"
"txt_add_black_warning_header" : "Warning"
"txt_add_black_warning_message" : "Phone number %s already on blacklist"
"txt_add_black_warning_params_header" : "Parameter error"
"txt_add_black_warning_params_message" : "Phone number field can not be blank. At least one of the restriction options must be enabled."
"support_manager" : "Support service"
"field_for_key" : "Field for license key"
"scan_close" : "Close"
"resume_working" : "Continue"
"success_key_header" : "Successful activation"
"success_key_message" : "You have successfully activated the application. Click Continue to proceed."
"txt_attention" : "Attention!"
"txt_may_infection" : "Possible threat"
"txt_attention_message" : "On your mobile device detected malicious activity!"
"txt_attention_process" : "Virus activity is detected in a system process:"
"txt_attention_protect" : "To protect please activate application:"
"txt_hack_message" : "Your phone conversation is not protected!"
"txt_hack_process" : "Your phone conversation is not protected and can be accessed by hackers."
"txt_sms_message" : "Detected virus activity in SMS messages!"
"title_activity_pay_form" : "PayFormActivity"
"test_test_test" : "tested"
"scan_is_going" : "Device scanning is in process"

"scan_now_working" : "Scanning of your device is now in process"
"scan_congratiulation" : "Thanks for installing our anti-virus software, we hope that you will be satisfied!"
"install_widget" : "Widget installation"
"install_widget_try_msg" : "We do our best to make this software much easier to use dont forget to install our widget."
"widget_fast_scan" : "Quick scanning"
"txt_sms_process" : "Virus activity is detected in a SMS message:"

ACTIVITIES

---

com.example.androiddefender2.MainActivity
com.example.androiddefender2.UpdateActivity
com.example.androiddefender2.SettingsActivity
com.example.androiddefender2.PrivacyActivity
com.example.androiddefender2.SupportActivity
com.example.androiddefender2.HomeActivity
com.example.androiddefender2.ScanActivity
com.example.androiddefender2.ScanningActivity
com.example.androiddefender2.BlackList
com.example.androiddefender2.NumbersList
com.example.androiddefender2.BySupportActivity
com.example.androiddefender2.SingleScanActivity
com.example.androiddefender2.VirusInfoDialogActivity
com.example.androiddefender2.PayFormActivity
com.example.androiddefender2.ByWithScanActivity

PROVIDERS

RECEIVERS

---

com.worker.androiddefender2.CallReceiver
com.worker.androiddefender2.MessageReceiver
com.worker.androiddefender2.ServiceStarter
com.worker.androiddefender2.TimeAlarm
com.worker.androiddefender2.NetworkAlarm
DefenderAppWidgetProvider

SERVICES

com.worker.androiddefender2.AVService

LIBRARIES

FILES

META-INF/MANIFEST.MF
META-INF/MYKEY.SF
META-INF/MYKEY.DSA
assets/fonts/TREBUC.TTF
assets/fonts/TREBUCBD.TTF
assets/fonts/TREBUCBI.TTF
assets/fonts/TREBUCIT.TTF
assets/fonts/arial.ttf
assets/AffiliateSettings.xml
assets/AndroidDefender.sqlite
assets/VirusesDescription.xml
res/drawable/btn_cam_res.xml
res/drawable/btn_grey_bg.xml
res/drawable/bullet.png
res/drawable/checkbox_draw.xml
res/drawable/checkbox_draw64.xml
res/drawable/clicked_row_background.xml
res/drawable/fon.png
res/drawable/heder.png
res/drawable/heder_non_active.png
res/drawable/lastscan.png
res/drawable/progressbar_blue.xml
res/drawable/progressbar_green.xml
res/drawable/progressbar_st.xml
res/drawable/table_delimitr.xml
res/drawable/text_view_grey.xml
res/drawable/virus_danger_row.xml
res/drawable-hdpi/auto_scan_settings.png
res/drawable-hdpi/btn_full_protect.png
res/drawable-hdpi/btnfon.png
res/drawable-hdpi/center_home_block.png

```
res/drawable-hdpi/checked.png
res/drawable-hdpi/detected.png
res/drawable-hdpi/ic_action_search.png
res/drawable-hdpi/ic_home.png
res/drawable-hdpi/ic_launcher.png
res/drawable-hdpi/ic_privatnost.png
res/drawable-hdpi/ic_settings.png
res/drawable-hdpi/ic_support.png
res/drawable-hdpi/ic_update.png
res/drawable-hdpi/nonchecked.png
res/drawable-hdpi/ok_blue.png
res/drawable-hdpi/progress_fon.png
res/drawable-hdpi/progress_fon_blue.png
res/drawable-hdpi/progress_fon_nonactive.png
res/drawable-hdpi/scan_status.png
res/drawable-hdpi/scanning_proccess.png
res/drawable-hdpi/warning.png
res/drawable-land-mdpi/center_home_block.png
res/drawable-land-mdpi/sub_center_home_block.png
res/drawable-ldpi/auto_scan_settings.png
res/drawable-ldpi/btn_full_protect.png
res/drawable-ldpi/btnfon.png
res/drawable-ldpi/center_home_block.png
res/drawable-ldpi/checked.png
res/drawable-ldpi/detected.png
res/drawable-ldpi/ic_home.png
res/drawable-ldpi/ic_launcher.png
res/drawable-ldpi/ic_privatnost.png
res/drawable-ldpi/ic_settings.png
res/drawable-ldpi/ic_support.png
res/drawable-ldpi/ic_update.png
res/drawable-ldpi/nonchecked.png
res/drawable-ldpi/ok_blue.png
res/drawable-ldpi/progress_fon.png
res/drawable-ldpi/progress_fon_blue.png
res/drawable-ldpi/progress_fon_nonactive.png
res/drawable-ldpi/scan_status.png
res/drawable-ldpi/scanning_proccess.png
res/drawable-ldpi/warning.png
res/drawable-mdpi/attention_ico.png
res/drawable-mdpi/auto_scan_settings.png
res/drawable-mdpi/big_blue_ok.png
res/drawable-mdpi/blue_attention.png
res/drawable-mdpi/btn_full_protect.png
```

```
res/drawable-mdpi/btn_scan_act.png
res/drawable-mdpi/btn_start_cam.png
res/drawable-mdpi/btn_start_cam_act.png
res/drawable-mdpi/btnfon.png
res/drawable-mdpi/bullet_red.png
res/drawable-mdpi/calendar.png
res/drawable-mdpi/center_home_block.png
res/drawable-mdpi/checked.png
res/drawable-mdpi/checked20.png
res/drawable-mdpi/checked24.png
res/drawable-mdpi/checked48.png
res/drawable-mdpi/checked64.png
res/drawable-mdpi/chk_version.png
res/drawable-mdpi/detected.png
res/drawable-mdpi/fon_widg.png
res/drawable-mdpi/gray_circle.png
res/drawable-mdpi/guard_att.png
res/drawable-mdpi/guard_btn.png
res/drawable-mdpi/guard_btn2.png
res/drawable-mdpi/hack_image.png
res/drawable-mdpi/horizontal_delim.png
res/drawable-mdpi/ic_action_search.png
res/drawable-mdpi/ic_home.png
res/drawable-mdpi/ic_key.png
res/drawable-mdpi/ic_launcher.png
res/drawable-mdpi/ic_privatnost.png
res/drawable-mdpi/ic_settings.png
res/drawable-mdpi/ic_support.png
res/drawable-mdpi/ic_update.png
res/drawable-mdpi/ico_key.png
res/drawable-mdpi/lastscan.png
res/drawable-mdpi/line_delimiter.png
res/drawable-mdpi/line_white.png
res/drawable-mdpi/message_image.png
res/drawable-mdpi/nonchecked.png
res/drawable-mdpi/nonchecked20.png
res/drawable-mdpi/nonchecked24.png
res/drawable-mdpi/nonchecked48.png
res/drawable-mdpi/nonchecked64.png
res/drawable-mdpi/ok_blue.png
res/drawable-mdpi/ok_green.png
res/drawable-mdpi/phonehack_image.png
res/drawable-mdpi/privacy.png
res/drawable-mdpi/progress_fon.png
```

```
res/drawable-mdpi/progress_fon_blue.png
res/drawable-mdpi/progress_fon_green.png
res/drawable-mdpi/progress_fon_nonactive.png
res/drawable-mdpi/red_attention.png
res/drawable-mdpi/scan_status.png
res/drawable-mdpi/scanning_proccess.png
res/drawable-mdpi/screen_header.png
res/drawable-mdpi/shesterenka.png
res/drawable-mdpi/spider.png
res/drawable-mdpi/sub_center_home_block.png
res/drawable-mdpi/tabs_transparent.png
res/drawable-mdpi/user.png
res/drawable-mdpi/vers_check.png
res/drawable-mdpi/warning.png
res/drawable-mdpi/yellow_attention.png
res/drawable-mdpi/zamochek.png
res/drawable-xhdpi/auto_scan_settings.png
res/drawable-xhdpi/btn_full_protect.png
res/drawable-xhdpi/btnfon.png
res/drawable-xhdpi/checked.png
res/drawable-xhdpi/detected.png
res/drawable-xhdpi/ic_action_search.png
res/drawable-xhdpi/ic_home.png
res/drawable-xhdpi/ic_launcher.png
res/drawable-xhdpi/ic_privatnost.png
res/drawable-xhdpi/ic_settings.png
res/drawable-xhdpi/ic_support.png
res/drawable-xhdpi/ic_update.png
res/drawable-xhdpi/nonchecked.png
res/drawable-xhdpi/ok_blue.png
res/drawable-xhdpi/progress_fon.png
res/drawable-xhdpi/progress_fon_blue.png
res/drawable-xhdpi/progress_fon_nonactive.png
res/drawable-xhdpi/scan_status.png
res/drawable-xhdpi/scanning_proccess.png
res/drawable-xhdpi/warning.png
res/layout/activity_black_list.xml
res/layout/activity_by_support.xml
res/layout/activity_bywith_scan.xml
res/layout/activity_home.xml
res/layout/activity_main.xml
res/layout/activity_numbers_list.xml
res/layout/activity_pay_form.xml
res/layout/activity_privacy.xml
```

```
res/layout/activity_scan.xml
res/layout/activity_scanning.xml
res/layout/activity_settings.xml
res/layout/activity_single_scan.xml
res/layout/activity_support.xml
res/layout/activity_support_activate.xml
res/layout/activity_update.xml
res/layout/activity_update_n.xml
res/layout/activity_virus_info_dialog.xml
res/layout/custom_notify.xml
res/layout/dialog_scan_error.xml
res/layout/tab_item.xml
res/layout/table_row.xml
res/layout/table_row_number.xml
res/layout/table_row_scan.xml
res/layout/table_update_row.xml
res/layout/widget_main.xml
res/layout-land/widget_main.xml
res/layout-sw600dp/activity_black_list.xml
res/layout-sw600dp/activity_by_support.xml
res/layout-sw600dp/activity_bywith_scan.xml
res/layout-sw600dp/activity_home.xml
res/layout-sw600dp/activity_main.xml
res/layout-sw600dp/activity_numbers_list.xml
res/layout-sw600dp/activity_pay_form.xml
res/layout-sw600dp/activity_privacy.xml
res/layout-sw600dp/activity_scan.xml
res/layout-sw600dp/activity_scanning.xml
res/layout-sw600dp/activity_settings.xml
res/layout-sw600dp/activity_single_scan.xml
res/layout-sw600dp/activity_support.xml
res/layout-sw600dp/activity_support_activate.xml
res/layout-sw600dp/activity_update.xml
res/layout-sw600dp/activity_update_n.xml
res/layout-sw600dp/activity_virus_info_dialog.xml
res/layout-sw600dp/tab_item.xml
res/layout-sw600dp/table_row.xml
res/layout-sw600dp/widget_main.xml
res/layout-sw600dp-land/widget_main.xml
res/layout-sw720dp/activity_black_list.xml
res/layout-sw720dp/activity_by_support.xml
res/layout-sw720dp/activity_bywith_scan.xml
res/layout-sw720dp/activity_home.xml
res/layout-sw720dp/activity_main.xml
```

```
res/layout-sw720dp/activity_numbers_list.xml
res/layout-sw720dp/activity_pay_form.xml
res/layout-sw720dp/activity_privacy.xml
res/layout-sw720dp/activity_scan.xml
res/layout-sw720dp/activity_scanning.xml
res/layout-sw720dp/activity_settings.xml
res/layout-sw720dp/activity_single_scan.xml
res/layout-sw720dp/activity_support.xml
res/layout-sw720dp/activity_support_activate.xml
res/layout-sw720dp/activity_update.xml
res/layout-sw720dp/activity_update_n.xml
res/layout-sw720dp/activity_virus_info_dialog.xml
res/layout-sw720dp/tab_item.xml
res/layout-sw720dp/table_row.xml
res/layout-sw720dp/widget_main.xml
res/layout-sw720dp-land/widget_main.xml
res/menu/activity_black_list.xml
res/menu/activity_home.xml
res/menu/activity_main.xml
res/menu/activity_numbers_list.xml
res/menu/activity_privacy.xml
res/menu/activity_scan.xml
res/menu/activity_scanning.xml
res/menu/activity_settings.xml
res/menu/activity_support.xml
res/menu/activity_update.xml
res/menu/by_support.xml
res/menu/pay_form.xml
res/menu/single_scan.xml
res/menu/virus_info_dialog.xml
res/xml/widget_manifest.xml
res/xml-sw600dp/widget_manifest.xml
res/xml-sw720dp/widget_manifest.xml
AndroidManifest.xml
classes.dex
resources.arsc
fakeAV_1CA532F171A0B765A46AF995EBAAB1D2_LabelReader.apk
fakeAV_1E178E501B41659FFACE85153615DEA7_LabelReader.apk
fakeAV_36B177910C99872B33E90DEA71B16617_LabelReader.apk
fakeAV_6F237D25472D9D09FC44ECE7DC9CED92_LabelReader.apk
fakeAV_75B8F9DBB1CD79B7FC074F7F499150CF_LabelReader.apk
fakeAV_77BB7F86FB0AC66C97B1AB3573ADFFC1_LabelReader.apk
fakeAV_934527F8EBB5C1088009CC9329DC3DE6_LabelReader.apk
fakeAV_ED1E0689F93B0C57E403489BB5338F59_LabelReader.apk
```