MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

好运全程司机 2.5.9.APK

APP名称:	好运全程司机
包名:	com.sdqc56.driver
域名线索:	16条
URL线索:	3条
邮箱线索:	0条
分析日期:	2022年2月2日 20:18

文件信息

文件名: hyqcsj317972.apk

文件大小: 10.45MB
MD5值: c7b0b90d4ad4cccc49125ed052ac7e36
SHA1值: 1e6a067dbe0706473168abc0483b7d7c6a94e0b7
SHA256值: bfc4aab259341050cf0beb2fe34c8b25d6b20ebe95d40adafe4924a02be3f2f5

APP 信息

App名称: 好运全程司机
包名: com.sdqc56.driver
主活动**Activity:** com.sdqc56.driver.activity.SplashActivity
安卓版本名称: 2.5.9
安卓版本: 80

域名线索

域名	是否危险域名	服务器信息
api.sdqc56.com	good	**IP:** 39.99.150.79 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
appgallery.cloud.huawei.com	good	**IP:** 117.78.15.51 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000 查看地图: Google Map

域名	是否危险域名	服务器信息
pic5.sdqc56.com	good	**IP:** 39.99.145.32 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map
api2.sdqc56.com	good	**IP:** 39.99.145.32 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map
eco.taobao.com	good	**IP:** 203.119.169.6 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
wap.cmpassport.com	good	**IP:** 120.197.235.27 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map

域名	是否危险域名	服务器信息
e.189.cn	good	**IP:** 42.123.76.65 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
store-at-dre.hispace.dbankcloud.com	good	**IP:** 80.158.5.6 **所属国家:** Germany **地区:** Schleswig-Holstein **城市:** Kiel **纬度:** 54.321331 **经度:** 10.134890 **查看地图:** Google Map
errlog.umeng.com	good	**IP:** 116.132.190.26 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
store.hispace.hicloud.com	good	**IP:** 49.4.18.123 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map

域名	是否危险域名	服务器信息
opencloud.wostore.cn	good	**IP:** 116.128.209.136 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061 查看地图: Google Map
uri.amap.com	good	**IP:** 203.119.211.253 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
errlogos.umeng.com	good	**IP:** 47.246.110.18 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692 查看地图: Google Map
play.google.com	good	**IP:** 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 查看地图: Google Map

域名	是否危险域名	服务器信息
api.map.baidu.com	good	**IP:** 111.206.209.166 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
pic.sdqc56.com	good	**IP:** 36.102.212.85 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://api.map.baidu.com/direction?origin=latlng:%s,%s	Android String Resource
https://pic.sdqc56.com	Android String Resource
https://api.sdqc56.com	Android String Resource
https://api2.sdqc56.com	Android String Resource
https://pic5.sdqc56.com	Android String Resource

URL信息	Url所在文件
https://uri.amap.com/navigation?from=%s,%s,%s&to=%s,%s,%s&via=,midwaypoint&mode=car&policy=1&src=andr.sdqc.driver&coordinate=gaode&callnative=1	Android String Resource
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource
https://wap.cmpassport.com/resources/html/contract.html	lib/armeabi-v7a/libauth_number_product-2.12.0.1-log-online-standard-release_alijtca_plus.so
https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true	lib/armeabi-v7a/libauth_number_product-2.12.0.1-log-online-standard-release_alijtca_plus.so
https://e.189.cn/sdk/agreement/detail.do?isWap=true&hidetop=true&appKey=8138111118	lib/armeabi-v7a/libauth_number_product-2.12.0.1-log-online-standard-release_alijtca_plus.so
https://eco.taobao.com/router/rest	lib/armeabi-v7a/libauth_number_product-2.12.0.1-log-online-standard-release_alijtca_plus.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so

URL信息	Url所在文件
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.ACCESS_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.ACCESS_WIFI_STATE	正常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息

向手机申请的权限	是否危险	类型	详细情况
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕

向手机申请的权限	是否危险	类型	详细情况
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.RAISED_THREAD_PRIORITY	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
oppo.permission.OPPO_COMPONENT_SAFE	未知	Unknown permission	Unknown permission from android reference
com.vivo.abe.permission.action.openhpactivity	未知	Unknown permission	Unknown permission from android reference
com.huawei.systemmanager.permission.ACCESS_INTERFACE	未知	Unknown permission	Unknown permission from android reference
android.permission.GRANT_RUNTIME_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息

向手机申请的权限	是否危险	类型	详细情况
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
getui.permission.GetuiService.com.sdqc56.driver	未知	Unknown permission	Unknown permission from android reference
com.sdqc56.driver.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.sdqc56.driver.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: L=山东济宁, O=全程物流, OU=全程物流, CN=全程物流
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-12-16 05:51:20+00:00
Valid To: 2044-12-09 05:51:20+00:00
Issuer: L=山东济宁, O=全程物流, OU=全程物流, CN=全程物流
Serial Number: 0x32b3de82
Hash Algorithm: sha256
md5: 26da7a4ad7652ff1dcbfddd6d3478a2c
sha1: 14e248988dd2fd81dcc65971b9e723ae928b7864
sha256: 3ab78090bc5c18b833472d7fb4687e144a5aa4b2eba9299886419c1cdcfe265b
sha512: ee8e673bbe8e5983da6b04e80c272d96e7bed58438617bb454738c812dbd03a25cc89d497fe16bde5fcee4962b82b367b365754c3b3ad3132fee2980483fcf0a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a67298a4b402551a6ca9ab93658856e05184091f71b749a5733864fa9a202075

硬编码敏感信息

可能的敏感信息
"bank_card_auth_tips" : "1、因银行要求，提款之前需先验证银行卡是否真实才可使用； 2、本次验证为银行行为，仅验证真实性，对银行卡无任何操作权限； 3、客服不会向您索要获取的验证码，请妥善保管"
"driving_user_name" : "驾驶证姓名"
"get_auth_code" : "获取验证码"
"key_agent_name" : "收 款 人"
"key_agent_percent" : "收款比例"

可能的敏感信息
"key_agent_price" : "收款金额"
"key_agent_reason" : "收款理由"
"key_agent_unit_price" : "收款单价"
"key_charge_unit" : "计量单位"
"key_count_type" : "结算方式"
"key_dispatch" : "调　　度"
"key_goods_loaded" : "装 货 量"
"key_goods_name" : "货物名称"
"key_goods_price" : "货　　值"
"key_item_load_address" : "装 货 方"
"key_item_unload_address" : "卸 货 方"
"key_load_address" : "装货地址"
"key_path_loss" : "允许路耗"
"key_price_per_ton" : "运费单价"
"key_recept_carnum" : "接单车辆"
"key_source_order_id" : "货源单号"

可能的敏感信息
"key_unload_address" : "卸货地址"
"key_waybill_id" : "运单编号"
"oauth" : "本机号码一键登录"
"user_name" : "姓名"
"warring_authcode_length" : "请输入有效验证码"
"warring_password" : "密码格式不符，请重新设置"

加壳分析

文件列表	分析结果
APK包	壳列表 | 详细情况 打包 | Jiagu
classes.dex	壳列表 | 详细情况 编译器 | dexlib 2.x

文件列表	分析结果
lib/armeabi-v7a/libauth_number_product-2.12.0.1-log-online-standard-release_alijtca_plus.so	壳列表 | 详细情况 反虚拟机 | possible VM check

---