MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

车鉴定商家版 v1.2.4.APK

APP名称:	车鉴定商家版
包名:	com.taigesiit.dealer
域名线索:	36条
URL线索:	33条
邮箱线索:	0条
分析日期:	2022年1月28日 22:00

文件信息

文件名: cjdsjb342151.apk
文件大小: 6.29MB
MD5值: ec1b974808bb741d140b118ab3d58a02
SHA1值: b1b356c37700b659077bf8fd5b3d70d03c27171b
SHA256值: ad63e20f6554c23c351622ecfaf1f509f3baedc772f9879d878fe5d182cb634f

APP 信息

App名称: 车鉴定商家版
包名: com.taigesiit.dealer
主活动**Activity:** com.taigesiit.dealer.ui.guide.StartActivity
安卓版本名称: v1.2.4
安卓版本: 124

域名线索

域名	是否危险域名	服务器信息
paygate-yf.meituan.com	good	**IP:** 101.236.9.32 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
oss-cn-.aliyuncs.comor	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
log.umsns.com	good	IP: 59.82.29.163 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
oss-cn-hangzhou.aliyuncs.com	good	IP: 118.31.219.251 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
wappaygw.alipay.com	good	IP: 203.209.250.50 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
api.weixin.qq.com	good	IP: 109.244.145.152 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
mobilegw.alipaydev.com	good	IP: 110.75.132.131 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
hydra.alibaba.com	good	IP: 203.119.144.59 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
l.mob.com	good	IP: 203.107.55.19 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
alog.umengcloud.com	good	IP: 106.11.86.69 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
mobilegw.stable.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
devs.data.mob.com	good	IP: 203.107.55.19 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
mcgw.alipay.com	good	IP: 203.209.250.50 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
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
m.data.mob.com	good	IP: 203.107.55.19 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
up.sharesdk.cn	good	IP: 115.227.41.64 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998 查看地图: Google Map

域名	是否危险域名	服务器信息
h5.m.taobao.com	good	IP: 59.47.225.232 所属国家: China 地区: Liaoning 城市: Benxi 纬度: 41.288609 经度: 123.764999 查看地图: Google Map
mta.qq.com	good	IP: 111.161.14.94 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
mobilegw.alipay.com	good	IP: 203.209.245.129 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
uop.umeng.com	good	没有服务器地理信息.
up.sdk.mob.com	good	IP: 203.107.55.19 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

域名	是否危险域名	服务器信息
www.mob.com	good	IP: 116.62.130.46 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
alog.umeng.com	good	IP: 203.119.145.194 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
api.exc.mob.com	good	IP: 203.107.55.19 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
mclient.alipay.com	good	IP: 203.209.250.50 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

域名	是否危险域名	服务器信息
cmnsguider.yunos.com	good	IP: 203.119.169.44 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
c.data.mob.com	good	IP: 203.107.80.4 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
xmlpull.org	good	IP: 74.50.61.58 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map
image.cnamedomain.com	good	没有服务器地理信息.
api.share.mob.com	good	IP: 203.107.55.19 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

域名	是否危险域名	服务器信息
app-dealer.chejianding.com	good	IP: 115.28.115.123 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
mta.oa.com	good	IP: 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map
api.mch.weixin.qq.com	good	IP: 182.254.22.146 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
pingma.qq.com	good	IP: 119.45.78.184 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
m.alipay.com	good	IP: 203.209.245.74 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://c.data.mob.com/v2/cdata	com/mob/commons/b.java
http://m.data.mob.com/v3/cconf	com/mob/commons/a.java
http://api.exc.mob.com:80	com/mob/commons/logcollector/c.java
http://up.sdk.mob.com	com/mob/commons/filesys/FileUploader.java
http://devs.data.mob.com:80/dinfo	com/mob/commons/authorize/a.java
http://devs.data.mob.com:80/dsign	com/mob/commons/authorize/a.java
http://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java

URL信息	Url所在文件
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
http://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/c.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&	com/alipay/sdk/data/a.java
https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple	com/alipay/test/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umengcloud.com/app_logs	com/umeng/analytics/a.java
https://uop.umeng.com	com/umeng/analytics/a.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/analytics/pro/an.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java

URL信息	Url所在文件
http://log.umsns.com/	com/umeng/analytics/social/d.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/d.java
http://mta.qq.com/	com/tencent/wxop/stat/e.java
http://mta.oa.com/	com/tencent/wxop/stat/e.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/c.java
http://hydra.alibaba.com/	com/ta/utdid2/aid/b.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/d.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/a.java
https://api.mch.weixin.qq.com/pay/unifiedorder	com/taigesiit/dealer/ui/recharge/RechargeNextActivty.java
https://app-dealer.chejianding.com/	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/api	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app/exam/aboutCjd.htm	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app/exam/aboutAgreement.htm	com/taigesiit/dealer/utils/Constants.java

URL信息	Url所在文件
https://app-dealer.chejianding.com/api/auth/authIndex	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app/violation/viewViolationInfo.htm?	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app/assessOrder/toolAssessOrderById.htm?	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app/account/getFAQPage.htm?	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app/checkOrder/checkInfo.htm?	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app/exam/reportExam.htm	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/api/report/viewReport?	com/taigesiit/dealer/utils/Constants.java
https://app-dealer.chejianding.com/app/exam/vinExam.htm	com/taigesiit/dealer/utils/Constants.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSClient.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/OSSClient.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
http://up.sharesdk.cn/upload/image	cn/sharesdk/framework/b/c.java
http://l.mob.com/url/ShareSdkMapping.do	cn/sharesdk/framework/b/c.java
http://api.share.mob.com:80	cn/sharesdk/framework/b/c.java
https://){1}	cn/sharesdk/framework/b/a.java

URL信息	Url所在文件
https://api.weixin.qq.com/sns/oauth2/access_token	cn/sharesdk/wechat/utils/g.java
https://api.weixin.qq.com/sns/oauth2/refresh_token	cn/sharesdk/wechat/utils/g.java
https://api.weixin.qq.com/sns/userinfo	cn/sharesdk/wechat/utils/g.java
http://www.mob.com	Android String Resource

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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

向手机申请的权限	是否危险	类型	详细情况
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.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.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_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.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
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
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.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

向手机申请的权限	是否危险	类型	详细情况
com.taigesiit.dealer.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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
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.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。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=bj, L=北京, O=中国, OU=北京泰格斯信息技术有限公司, CN=车鉴定
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-10-19 10:14:45+00:00
Valid To: 3014-02-19 10:14:45+00:00
Issuer: C=86, ST=bj, L=北京, O=中国, OU=北京泰格斯信息技术有限公司, CN=车鉴定
Serial Number: 0x5624c295
Hash Algorithm: sha1
md5: 9aedb8925c677bcc95125a9622aa2365
sha1: a638955528ff0825fbcf5baee1e9635b104743f5
sha256: d74b3c27cc902bc2ccd0c0857388a29c380837b2be30ddc90e94f9cb83bb5021
sha512: ff2c10c9dce7eae72f5994543a0b0cc88fcb7eb7c061ab71d691a31a3c73cf50afcb8c3af7be8dd0df3d88c6bbfdec8ffc7e4fef8aea7d1b84527d702444324e
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 4a0318053fdf7ae3a394e89dea36cfca5c6c54032d64c4b08eae83314c94b9bb

Exodus威胁情报

名称	分类	URL链接
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.mob.tools.MobUIShell	Schemes: tencent100371282://,
com.taigesiit.dealer.ui.MainActivity	Schemes: dealer://, Hosts: activity,

加壳分析

文件列表	分析结果

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check
device ID check
subscriber ID check
ro.product.device check
ro.kernel.qemu check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
