MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

伙伙 1.0.APK

APP名称:	伙伙
包名:	cn.cloudjoy.motor.vehicle
域名线索:	25条
URL线索:	16条
邮箱线索:	0条
分析日期:	2022年2月2日 20:12

文件信息

文件名: huohuo323699.apk
文件大小: 5.16MB
MD5值: 1f5a7297e3048cc05823b8279058b6f0
SHA1值: f47a4df67e3661b460a617789d4c7ea829bb3113
SHA256值: 64a67b49cb7061587f30aa8f4b1b297c7c83693933fd14de92488c4d9e1d0ea0

APP 信息

App名称: 伙伙
包名: cn.cloudjoy.motor.vehicle
主活动**Activity:** cn.cloudjoy.motor.vehicle.main.LoginAty
安卓版本名称: 1.0
安卓版本: 2021031601

域名线索

域名	是否危险域名	服务器信息
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
mobilegw-1-64.test.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
admin.zkqc-cq.com	good	IP: 116.63.166.112 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
mclient.alipay.com	good	IP: 203.209.250.6 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
open.weixin.qq.com	good	IP: 175.24.209.30 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
mcgw.alipay.com	good	IP: 203.209.250.6 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
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
mobilegw.stable.alipay.net	good	没有服务器地理信息.
schemas.android.com	good	没有服务器地理信息.
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
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
www.w3.org	good	IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge 纬度: 42.365078 经度: -71.104523 查看地图: Google Map

域名	是否危险域名	服务器信息
mobilegw.alipay.com	good	IP: 203.209.247.65 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
yxpay.cloudjoytech.com	good	IP: 117.78.22.52 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
long.open.weixin.qq.com	good	IP: 109.244.216.15 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
192.168.1.21	good	IP: 192.168.1.21 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map

域名	是否危险域名	服务器信息
m.alipay.com	good	IP: 203.209.245.120 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
192.168.1.16	good	IP: 192.168.1.16 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
192.168.1.18	good	IP: 192.168.1.18 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 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

域名	是否危险域名	服务器信息
render.alipay.com	good	IP: 150.138.144.196 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941 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
loggw-exsdk.alipay.com	good	IP: 110.75.130.110 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
www.smpte-ra.org	good	IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488 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:** 140.249.89.233 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
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

URL信息	Url所在文件
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/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.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java
http://www.w3.org/ns/ttml	com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
http://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java

URL信息	Url所在文件
https://yxpay.cloudjoytech.com:50135	cn/cloudjoy/motor/vehicle/app/Constants.java
http://192.168.1.16:8848	cn/cloudjoy/motor/vehicle/app/Constants.java
https://admin.zkqc-cq.com	cn/cloudjoy/motor/vehicle/app/Constants.java
http://192.168.1.18:8848	cn/cloudjoy/motor/vehicle/app/Constants.java
http://192.168.1.21:8848	cn/cloudjoy/motor/vehicle/app/Constants.java

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.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_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

向手机申请的权限	是否危险	类型	详细情况
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
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=JING KUN YUN XIANG
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-04-13 06:07:10+00:00
Valid To: 2118-03-20 06:07:10+00:00
Issuer: CN=JING KUN YUN XIANG
Serial Number: 0x3b724d3b
Hash Algorithm: sha256
md5: 6d66fc513202373b74c40de6b32aeeb3
sha1: 70ec9cb7284a3fc4701d5a0d110b90db6d5ec499
sha256: b8479dc17a1e1939990df00175657268c496238b887e682664b8bf997ca387a9
sha512: 2f1ef924b4bc7b70713e021836609c10cc734269e5ccb51c8afd9f9dd432447ece74effcea7cfe08abe79d0ef363852675607a36e3bab10a7ad44f0ed5fa7c37
PublicKey Algorithm: rsa

Bit Size: 2048
Fingerprint: b36473c676d4315ae3e66e08f80f6099962532c155fa2ff0c68e37b9f61bd4b2

Exodus威胁情报

名称	分类	URL链接
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

加壳分析

文件列表	分析结果
	壳列表 / 详细情况
	反虚拟机
	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

classes.dex 文件列表	分析结果	详细情况	
	编译器	r8	
