MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

查找我的朋友 1.0.APK

APP名称:	查找我的朋友
包名:	car.wu.wei.oroc.chazhaowo
域名线索:	6条
URL线索:	10条
邮箱线索:	0条
分析日期:	2022年1月26日 18:46

文件信息

文件名: czwdpy.apk
文件大小: 2.87MB
MD5值: 83e7799ce6520ba5b295eb658ffd06f3
SHA1值: ecd3c21071f8106b2eba34423074b6eb8381684f
SHA256值: 0c8642f836667a115dad27b1cbe4955e67da3ef2d75d37944939b0c91a6b5c62

APP 信息

App名称: 查找我的朋友
包名: car.wu.wei.oroc.chazhaowo
主活动**Activity:** .OneActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
schemas.android.com	good	没有服务器地理信息.
d.91.com	good	**IP:** 125.77.24.228 所属国家: China 地区: Fujian 城市: Fuzhou 纬度: 26.061390 经度: 119.306107 查看地图: Google Map

域名	是否危险域名	服务器信息
124.173.143.211	good	IP: 124.173.143.211 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
mjoy.91.com	good	IP: 10.46.177.63 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
ws1.datouniao.com	good	IP: 42.121.19.154 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
ws2.datouniao.com	good	IP: 42.121.19.154 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://ws1.datouniao.com/android/AdsOffers?	com/datouniao/AdPublisher/AdsOffersWebView.java
http://ws2.datouniao.com/android/AdsOffers?	com/datouniao/AdPublisher/AdsOffersWebView.java
http://ws1.datouniao.com/ActivityFeedback?	com/datouniao/AdPublisher/k.java
http://ws2.datouniao.com/ActivityFeedback?	com/datouniao/AdPublisher/k.java
http://ws1.datouniao.com/SpendAmount?	com/datouniao/AdPublisher/r.java
http://ws2.datouniao.com/SpendAmount?	com/datouniao/AdPublisher/r.java
http://ws1.datouniao.com/GetAmount?	com/datouniao/AdPublisher/q.java
http://ws2.datouniao.com/GetAmount?	com/datouniao/AdPublisher/q.java
http://ws1.datouniao.com/AddAmount?	com/datouniao/AdPublisher/p.java
http://ws2.datouniao.com/AddAmount?	com/datouniao/AdPublisher/p.java
http://ws1.datouniao.com/AdPublisherConnect?	com/datouniao/AdPublisher/o.java
http://ws2.datouniao.com/AdPublisherConnect?	com/datouniao/AdPublisher/o.java
http://d.91.com/	com/nd/dianjin/k.java
http://d.91.com/	com/nd/dianjin/OfferBanner.java

URL信息	Url所在文件
http://schemas.android.com/apk/res/	com/nd/dianjin/OfferBanner.java
http://mjoy.91.com/index.php/server	com/nd/dianjin/webservice/BusinessProcess.java
http://124.173.143.211/index.php?m=content&c=index&f=show&catid=56&contentid=141	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.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_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.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
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.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

向手机申请的权限	是否危险	类型	详细情况
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
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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-04-06 14:26:51+00:00
Valid To: 2013-04-06 14:26:51+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x4f7efd2b
Hash Algorithm: sha1
md5: d33e0334a71f907a3f41e34629595d4e
sha1: db9fe66a7b4844c051f2e9247123ca2d485ef4f9
sha256: 810ab2aa95df452f9310302e3475e7f74314bd924d0ea6a1ef06e9b489f022bd
sha512: 2c5173bf3c9c7c48c560f563f71f7bc61bd7a2ef7e19c4282129b4c0c4d89716f8e28ba1745a82e2c9f205eb1c32a4fa3166c52f1a14555ec4a2f93c38b86ff3

加壳分析

<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.MODEL check
device ID check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
