MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

MSWJ

WJ 1.0.0.APK

APP名称:	WJ
包名:	com.pesongwj.mswj
域名线索:	12条
URL线索:	31条
邮箱线索:	1条
分析日期:	2022年2月3日 11:17

文件信息

文件名: wj511794.apk
文件大小: 7.25MB
MD5值: b33cc0264d3c10f179fbb32738bc98b5
SHA1值: 1dcb9df4b5e2668296a98d317047b90bbaeebf87
SHA256值: 0163eb9cf20a7f4a19150add4afd7f3c06415772579c48d11a332966f3ff31c5

APP 信息

App名称: WJ
包名: com.pesongwj.mswj
主活动**Activity:** com.fkuang.delivery.view.WellcomeActivity
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
api.coindog.com	good	**IP:** 39.107.228.170 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
mockapi.eolink.com	good	**IP:** 47.116.143.48 **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
xml.apache.org	good	**IP:** 151.101.2.132 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
39.98.245.21	good	**IP:** 39.98.245.21 **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
www.wl890.com	good	**IP:** 175.6.12.93 **所属国家:** China **地区:** Hunan **城市:** Changsha **纬度:** 28.200001 **经度:** 112.966667 **查看地图:** Google Map

域名	是否危险域名	服务器信息
github.com	good	**IP:** 20.205.243.166 **所属国家:** United States of America **地区:** Washington **城市:** Redmond **纬度:** 47.682899 **经度:** -122.120903 **查看地图:** Google Map
www.sishun56.com	good	**IP:** 118.31.35.124 **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
94.191.60.183	good	**IP:** 94.191.60.183 **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
1.116.85.39	good	**IP:** 1.116.85.39 **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
api.qhniua.com	good	**IP:** 128.1.131.106 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
47.95.213.35	good	**IP:** 47.95.213.35 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
mock-api.com	good	**IP:** 101.200.207.167 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://1.116.85.39:8080/new_war_exploded/bysj/getForgetPwd	com/fkuang/delivery/http/RetrofitApi.java

URL信息	Url所在文件
http://mock-api.com/GzqjjLgW.mock/user_shop	com/fkuang/delivery/http/RetrofitApi.java
http://1.116.85.39:8080/new_war_exploded/bysj/getLogin	com/fkuang/delivery/http/RetrofitApi.java
http://1.116.85.39:8080/new_war_exploded//bysj/getRegister	com/fkuang/delivery/http/RetrofitApi.java
http://47.95.213.35:81	com/fkuang/delivery/http/API.java
http://www.wl890.com/	com/fkuang/delivery/adapter/DynamicAdapter.java
http://www.wl890.com/	com/fkuang/delivery/adapter/GylAdapter.java
http://www.wl890.com/	com/fkuang/delivery/adapter/FactoryStorageAdapter.java
http://www.sishun56.com/	com/fkuang/delivery/adapter/CarSourceAdapter.java
http://www.wl890.com/	com/fkuang/delivery/view/MainFragment$initData$1.java
http://www.wl890.com/	com/fkuang/delivery/view/GyInfoActivity.java
http://www.sishun56.com/	com/fkuang/delivery/view/CarSourceInfoActivity.java
http://www.wl890.com/	com/fkuang/delivery/view/DeliveryInfoActivity.java
http://xml.apache.org/xslt}indent-amount	com/orhanobut/logger/LoggerPrinter.java
http://39.98.245.21:8080/	com/scrb/baselib/retrofit/RetrofitUtil.java
http://www.wl890.com/zgwuliu/html/news/moble/loadMoreNewsM.action	com/scrb/baselib/retrofit/ApiService.java

URL信息	Url所在文件
https://mockapi.eolink.com/Qz5pe7g2e125604afe5e3293ca09f171d52e220ccf7e84c/appconfig	com/scrb/baselib/retrofit/ApiService.java
http://www.sishun56.com/API/cheyuan.aspx?token=334A5FF816AFFC956AE9B2DE&isAsyn=1&pageSize=20	com/scrb/baselib/retrofit/ApiService.java
http://api.coindog.com/live/list	com/scrb/baselib/retrofit/ApiService.java
https://api.qhniua.com/checkVersion	com/scrb/baselib/retrofit/ApiService.java
http://api.coindog.com/topic/list	com/scrb/baselib/retrofit/ApiService.java
http://www.wl890.com/zgwuliu/html/verify/moble/findSearchUser2.action	com/scrb/baselib/retrofit/ApiService.java
http://www.wl890.com/zgwuliu/findSearchReceipt.action?type1=Z&userid=13381583683	com/scrb/baselib/retrofit/ApiService.java
http://www.wl890.com/html/warehouse/moble/findSearchWareHouse.action	com/scrb/baselib/retrofit/ApiService.java
http://1.116.85.39:8080/new_war_exploded/bysj/getLogin	com/scrb/baselib/retrofit/ApiService.java
http://1.116.85.39:8080/new_war_exploded/bysj/getCancellation	com/scrb/baselib/retrofit/ApiService.java
http://1.116.85.39:8080/new_war_exploded//bysj/getRegister	com/scrb/baselib/retrofit/ApiService.java
http://1.116.85.39:8080/new_war_exploded/bysj/getForgetPwd	com/scrb/baselib/retrofit/ApiService.java
http://94.191.60.183:3002/system/sendCode	com/scrb/baselib/retrofit/ApiService.java
http://1.116.85.39:8080/new_war_exploded/bysj/bannerList	com/scrb/baselib/retrofit/ApiService.java
http://39.98.245.21/upload	com/scrb/baselib/retrofit/ApiService.java

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	Android String Resource

✉ 邮箱线索

邮箱地址	所在文件
jtrvmp28495@chacuo.net	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.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_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.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.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。

✹ 签名证书

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=wj
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-01-14 06:29:33+00:00
Valid To: 2047-01-08 06:29:33+00:00
Issuer: CN=wj
Serial Number: 0x22f79f0
Hash Algorithm: sha256
md5: aa8f8a050cfd848d87a3dd6e78b702aa
```

sha1: 92fc063e5d8cb4aa9c863a981a060b60d5a099a6
sha256: 121415907cf77f044ef7b7f1e9a9a8a92514949d39f8f1cdac917e27a8fc3010
sha512: c7ff96c3ca64d922fe7fdad57f5c5863cde90b586418016e3bd1a19271da1f8b2b58534bc262cfcddcf30e2629356f80ec81c0e5296d03cfa6b4743f58097948
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 9f8e06ed0397cb59f247aac2c0559cf36821100385cba23cc0ba0cd8df2837ac

硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

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.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></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>

报告由 摸瓜平台 自动生成，并非包含所有检测结果，有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析