MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

药吉采 1.0.27.APK

APP名称:	药吉采
包名:	com.hzwl.yjc
域名线索:	15条
URL线索:	16条
邮箱线索:	0条
分析日期:	2022年1月25日 22:56

文件信息

文件名: yaojicai448931.apk
文件大小: 6.8MB
MD5值: cc72bb83245320f925f52392acfc1e74
SHA1值: 92bc25b2e1db2025861868f546accf4063e4d915
SHA256值: 16b4203065a767054b5e7f453d51f1c6281b0b60d85790fdb4a1189047f7448d

APP 信息

App名称: 药吉采
包名: com.hzwl.yjc
主活动**Activity:** com.hzwl.yjc.main.MainActivity
安卓版本名称: 1.0.27
安卓版本: 27

域名线索

域名	是否危险域名	服务器信息
api.yaojicai666.com	good	**IP:** 121.37.208.200 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
tsis.jpush.cn	good	**IP:** 121.36.81.251 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
bjuser.jpush.cn	good	**IP:** 122.9.9.94 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
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
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
www.abcdefgzxy.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
172.16.1.110	good	**IP:** 172.16.1.110 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
xml.org	good	**IP:** 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246 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
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

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
open.weixin.qq.com	good	**IP:** 109.244.144.48 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.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
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
182.92.20.189	good	**IP:** 182.92.20.189 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.yaojicai666.com	com/hzwl/yjc/BuildConfig.java
http://api.yaojicai666.com	com/hzwl/yjc/util/Constant.java
http://172.16.1.110:8350	com/hzwl/yjc/util/Constant.java
https://api.weixin.qq.com/sns/	com/hzwl/yjc/presenter/WxPresenter.java
http://www.w3.org/TR/SVG11/feature#	com/caverock/androidsvg/SVGParser.java
http://www.w3.org/2000/svg	com/caverock/androidsvg/SVGParser.java
http://www.w3.org/1999/xlink	com/caverock/androidsvg/SVGParser.java
http://xmlpull.org/v1/doc/features.html#process-docdecl	com/caverock/androidsvg/SVGParser.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/features/external-general-entities	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/features/external-parameter-entities	com/caverock/androidsvg/SVGParser.java
http://xml.org/sax/properties/lexical-handler	com/caverock/androidsvg/SVGParser.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java
https://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
www.abcdefgzxy.com	com/zxy/tiny/core/HttpUrlConnectionFetcher.java
http://182.92.20.189:9099/	cn/jiguang/o/c.java
https://tsis.jpush.cn	cn/jiguang/ad/i.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/aa/b.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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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.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。
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed

v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=xiong
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-05-02 07:59:47+00:00
Valid To: 2039-04-26 07:59:47+00:00
Issuer: CN=xiong
Serial Number: 0x4465c305
Hash Algorithm: sha256
md5: b1c1950b4e2e0ee14b2fd1b4475ec121
sha1: d0ff4a14cb264018d748803a16e4f6c800c70042
sha256: 989b527a1dc68ab59c7e19ab061e6a09e64d72a2c6c1e23d3cd38d5f9bb93ad8
sha512: 8ba42d2f24b3dd6b18bb83a6eefeeeaaa7ce85bb47f90f06f33d51ff5866de3a41bed023fc946aa3525ce148803939addcd35c1e03a00be6ba433fb72efc72ec
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d99b77aa0bbd740fe492e70f5438cbfc9984947a70e2ff037698a0819364c5c1

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

硬编码敏感信息

可能的敏感信息
"wx_auth_denied" : "已拒绝授权"

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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
SIM operator check
network operator name check
device ID check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
