MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

云惠搜 1.22.APK

APP名称:	云惠搜
包名:	com.android.yunhuisou
域名线索:	2条
URL线索:	5条
邮箱线索:	0条
分析日期:	2022年1月25日 23:06

文件信息

文件名: yunhuisou.apk
文件大小: 3.37MB
MD5值: a1db1834c67542397af55d2380155d0f
SHA1值: 45d2d2b10fdd02f17a90e411d16ce383a0350b7d
SHA256值: 957a812319ef7a14f935db91a6867748e40fae120b8eb62b95e20fb1a605cd7b

APP 信息

App名称: 云惠搜
包名: com.android.yunhuisou
主活动**Activity:** com.android.yunhuisou.StartActivity
安卓版本名称: 1.22
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
docs.growingio.com	good	**IP:** 117.50.63.183 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

域名	是否危险域名	服务器信息
api.growingio.com	good	**IP:** 117.50.9.189 **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

URL线索

URL信息	Url所在文件
http://api.growingio.com	com/growingio/android/sdk/TrackConfiguration.java
https://docs.growingio.com/docs/developer-manual/sdkintegrated/android-sdk/android-sdk-api/customize-api	com/growingio/android/sdk/track/ErrorLog.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=mx, ST=mx, L=shishi, O=shishi, OU=yiyi, CN=yiyi
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-08-24 09:17:47+00:00
Valid To: 2046-08-18 09:17:47+00:00
Issuer: C=mx, ST=mx, L=shishi, O=shishi, OU=yiyi, CN=yiyi
Serial Number: 0x30499dbf
Hash Algorithm: sha256
md5: faca5346aacce4ffe1f0fd37761cc3c6
sha1: cf61ea0c97c707b3e57d260a9780e8796e94a8e3
sha256: a9876a3f6337c70b6b3410bc8cdd1875e6dac1b0c14a937843119e280f9ccb6c
sha512: 2b25c1f0b4f83a4a21f0d0b4dd76b651b7b04eb620e4dbcbdb275d63ca361a684d4d7bbbfd8c3b721c044e9c26b3da8c9f7f1ddaf6d2c880916edc22b7614d62
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 055f96f24763f0cef3b28fc8a0353b572ee9d0030e3712e17c911b58d1de2581

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 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
