MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

浩.进销存平台 1.0.APK

APP名称:	浩.进销存平台
包名:	hao.Sale
域名线索:	18条
URL线索:	46条
邮箱线索:	0条
分析日期:	2022年2月2日 20:08

文件信息

文件名: hjxcpt463691.apk
文件大小: 4.86MB
MD5值: 3aa056290fad777d19cfce11c210dd03
SHA1值: a5f01f2edf4a94192a6d4965fd59ac7f992f5a6b
SHA256值: 8609b50f0eec48c84d622484d473d2ac54f26b566616f7dd92102ee594edc8e4

APP 信息

App名称: 浩.进销存平台
包名: hao.Sale
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.0
安卓版本: 20210205

域名线索

域名	是否危险域名	服务器信息
da.mmarket.com	good	**IP:** 120.232.188.83 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
www.dcloud.io	good	**IP:** 124.95.157.146 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432777 查看地图: Google Map
iss.openspeech.cn	good	**IP:** 42.62.43.147 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
ask.dcloud.net.cn	good	**IP:** 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
imfv.openspeech.cn	good	**IP:** 42.62.116.34 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
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	good	**IP:** 47.93.95.208 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
stream.dcloud.net.cn	good	**IP:** 118.31.188.88 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
openapi.openspeech.cn	good	**IP:** 42.62.116.34 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.haosale.top	good	**IP:** 139.159.136.180 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
scs.openspeech.cn	good	**IP:** 220.248.230.134 所属国家: China 地区: Anhui 城市: Hefei 纬度: 31.863890 经度: 117.280830 查看地图: Google Map
service.dcloud.net.cn	good	**IP:** 47.97.36.120 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
dev.voicecloud.cn	good	**IP:** 59.107.24.11 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
hxqd.openspeech.cn	good	**IP:** 42.62.116.134 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
wke.openspeech.cn	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
stream.mobihtml5.com	good	没有服务器地理信息.
m3w.cn	good	IP: 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
data.openspeech.cn	good	IP: 220.248.230.134 所属国家: China 地区: Anhui 城市: Hefei 纬度: 31.863890 经度: 117.280830 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/b.java
http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/c.java
http://dev.voicecloud.cn/msc/help.html	com/iflytek/cloud/resource/a.java

URL信息	Url所在文件
http://scs.openspeech.cn/scs	com/iflytek/thirdparty/Z.java
http://data.openspeech.cn/index.php/clientrequest/clientcollect/isCollect	com/iflytek/thirdparty/Z.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog	com/iflytek/thirdparty/C0062b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog	com/iflytek/thirdparty/C0062b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog	com/iflytek/thirdparty/C0062b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog	com/iflytek/thirdparty/C0062b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:specposteventlog	com/iflytek/thirdparty/C0062b.java
http://openapi.openspeech.cn/webapi/wfr.do	com/iflytek/thirdparty/C0049ae.java
http://imfv.openspeech.cn/msp.do	com/iflytek/thirdparty/C0047ac.java
http://hxqd.openspeech.cn/launchconfig	com/iflytek/thirdparty/aF.java
http://wke.openspeech.cn/wakeup/	com/iflytek/thirdparty/C0079s.java
http://iss.openspeech.cn/v?	com/iflytek/speech/UtilityConfig.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java

URL信息	Url所在文件
http://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/ad/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/f/b/b.java
https://service.dcloud.net.cn/pdz	io/dcloud/f/b/d/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/b/d/a.java
http://ask.dcloud.net.cn/article/35627	io/dcloud/f/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/f/a/a.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://www.dcloud.io/streamapp/streamapp.apk	io/dcloud/common/util/ShortCutUtil.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/36199	io/dcloud/common/constant/DOMException.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java

URL信息	Url所在文件
http://www.haosale.top/privacypolicy/HaoSale.html	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.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.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.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.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.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。

向手机申请的权限	是否危险	类型	详细情况
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=BJ, L=HD, O=Test, OU=Test, CN=Tester
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-07-26 12:52:56+00:00
Valid To: 2119-07-02 12:52:56+00:00

Issuer: C=CN, ST=BJ, L=HD, O=Test, OU=Test, CN=Tester
Serial Number: 0x7dd12840
Hash Algorithm: sha256
md5: f9f6c81fdbab50147d6f2c4fcee60aa5
sha1: bbace22f973b1802e7d669a37a28efd23fa368e7
sha256: 24117de73612bcfeaf2a6a24bd044f2e33e52d41965f504d74177f4fe255eb26
sha512: 333aab8f49d2434b3c0a4cbba65e82f4056a9d17076b5b288846621868a6165482905ca5705fc2080570f31d969a22b9d023cd0b7ceb7984c5a6604a5de7b4e5
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b0efd86a24b6e59ce3afdbaadc6a22aff1217552a26ee9664f2124eb62fe23b7

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: hao.sale://,

加壳分析

文件列表	分析结果

<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.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check
subscriber ID check
possible VM check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
