MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

贝宝加 1.3.APK

APP名称:	贝宝加
包名:	w2a.W2Abeibao.hqhyqc.com
域名线索:	16条
URL线索:	46条
邮箱线索:	0条
分析日期:	2022年1月25日 21:38

文件信息

文件名: beibaojia.apk
文件大小: 5.27MB
MD5值: fee8e9286838f267365043427db72be6
SHA1值: 9fbea6b70e97e5d08b4451926e89c2d4c8e74746
SHA256值: 23d22fc41fa13dbf20a7b33a0b9f3d5e243ba3136de0d4be6e0edfc53549b830

APP 信息

App名称: 贝宝加
包名: w2a.W2Abeibao.hqhyqc.com
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.3
安卓版本: 4

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.
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

域名	是否危险域名	服务器信息
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:** 42.62.116.35 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
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
ask.dcloud.net.cn	good	**IP:** 124.165.213.234 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.560280 查看地图: Google Map

域名	是否危险域名	服务器信息
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
stream.mobihtml5.com	good	没有服务器地理信息.
wke.openspeech.cn	good	没有服务器地理信息.
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
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
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
imfv.openspeech.cn	good	**IP:** 42.62.116.18 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
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
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

域名	是否危险域名	服务器信息
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

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
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://imfv.openspeech.cn/msp.do	com/iflytek/thirdparty/C0056ac.java
http://wke.openspeech.cn/wakeup/	com/iflytek/thirdparty/C0088s.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog	com/iflytek/thirdparty/C0071b.java

URL信息	Url所在文件
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog	com/iflytek/thirdparty/C0071b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog	com/iflytek/thirdparty/C0071b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog	com/iflytek/thirdparty/C0071b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:specposteventlog	com/iflytek/thirdparty/C0071b.java
http://openapi.openspeech.cn/webapi/wfr.do	com/iflytek/thirdparty/C0058ae.java
http://hxqd.openspeech.cn/launchconfig	com/iflytek/thirdparty/aF.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
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/283	io/dcloud/h/b.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/c.java

URL信息	Url所在文件
https://service.dcloud.net.cn/pdz	io/dcloud/f/b/f/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/b/f/a.java
https://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://ask.dcloud.net.cn/article/282	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
https://ask.dcloud.net.cn/article/36199	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

向手机申请的权限	是否危险	类型	详细情况
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.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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

向手机申请的权限	是否危险	类型	详细情况
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。
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

向手机申请的权限	是否危险	类型	详细情况
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
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。
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
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.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=beibaojks, ST=beibaojks, L=beibaojks, O=beibaojks, OU=beibaojks, CN=beibaojks
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-22 06:35:41+00:00

Valid To: 2046-06-16 06:35:41+00:00
Issuer: C=beibaojks, ST=beibaojks, L=beibaojks, O=beibaojks, OU=beibaojks, CN=beibaojks
Serial Number: 0x4e2e8ed6
Hash Algorithm: sha256
md5: 60ce269799d5e4b0230d7ffc0c28096c
sha1: 010bacb18a48fef6a5b2a1d1db7a97771b342704
sha256: 2598e64cae09e06f17f7d5a23293180f1ba0182e4359e4b8be7b0a202b026a2a
sha512: 3933bedcf941501d7d9454e802afe7f3fc61b60317a7e2801bd4580961cf538b8d8c1c8b4b0d7f1cdc4d17d903b0e1eb37c21d1f83333b8aba8e559e162b86d1
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b8cab148c1205b171306c412e7cd5ed88f56da589943a019555549f1b6415129

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_feature_confusion_exception_no_key_input" : "no public key input"
"dcloud_feature_confusion_exception_no_private_key_input" : "no private key input"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"

可能的敏感信息
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_feature_confusion_exception_no_key_input" : "公钥数据为空"
"dcloud_feature_confusion_exception_no_private_key_input" : "私钥数据为空"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"

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>
