MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

航空气象服务 2.0.APK

APP名称:	航空气象服务
包名:	w2a.W2Ath.kongqin.com
域名线索:	8条
URL线索:	36条
邮箱线索:	0条
分析日期:	2022年1月26日 18:58

文件信息

文件名: hkqxfw.apk
文件大小: 4.48MB
MD5值: 95aca66a128694151e479a0ad6a29f0d
SHA1值: 4e2a55ad1a24301348b593302faaafb5a484c619
SHA256值: 4ad6db3f070bb33a9f8e0bbe92c0f24aa5ea405eb5441bf0c598b7f952710957

APP 信息

App名称: 航空气象服务
包名: w2a.W2Ath.kongqin.com
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 2.0
安卓版本: 14

域名线索

域名	是否危险域名	服务器信息
service.dcloud.net.cn	good	**IP:** 120.26.1.80 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
schemas.android.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
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
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.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
stream.dcloud.net.cn	good	**IP:** 118.31.103.188 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
th.kongqin.com	good	**IP:** 122.112.156.86 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061 查看地图: Google Map

URL线索

URL信息	Url所在文件
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/e/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/b/e/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
https://th.kongqin.com/#/privacy	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.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.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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度

向手机申请的权限	是否危险	类型	详细情况
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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
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
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: False
Found 1 unique certificates
Subject: C=china, ST=sichuan, L=guanghan, O=kongqin, OU=kongqin, CN=kongqin
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-04-13 04:04:49+00:00

Valid To: 2120-03-20 04:04:49+00:00
Issuer: C=china, ST=sichuan, L=guanghan, O=kongqin, OU=kongqin, CN=kongqin
Serial Number: 0x33a06295
Hash Algorithm: sha256
md5: 92b44263edad51b67de5dfc8b4e370c5
sha1: 1ff7575d583fa371a0cc41de8adff9bbbb284aa2
sha256: e4ec33cccf19837f363c955e43b456812767097408c91d81f6fd5da5d6273a01
sha512: 1a2796f881e8813ebd0b5902ce16ab5c74ba7c53c583db30cee83359da7607ffa3b7094f1ae7b585a4e17d1cc2ca3a052ad18c002f5c9b54def13f2197ea9747
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 1001087f3f02cbf3d622a7ddd5995ebe269867485dc17d974ae869831b9d1400

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.PRODUCT check
Build.HARDWARE check
possible Build.SERIAL check
SIM operator check
possible VM check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
