MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

宝图盒子 1.1.0.APK

APP名称:	宝图盒子
包名:	com.bimgx.app
域名线索:	12条
URL线索:	49条
邮箱线索:	0条
分析日期:	2022年2月4日 11:13

文件信息

文件名: baotuhezi427765.apk
文件大小: 11.38MB
MD5值: 9b8ddcb2fb81c3c1f5820b4e9c8ce980
SHA1值: c3100491c3d7ddc5500655d2d9927e2c80a577b3
SHA256值: 9302727cc24a7a3b47396357c0b3eaf2bda48b19cf2673d9ddb42cccb730daff

APP 信息

App名称: 宝图盒子
包名: com.bimgx.app
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.1.0
安卓版本: 104

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.
lame.sf.net	good	**IP:** 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego 纬度: 32.799797 经度: -117.137047 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
ns.adobe.com	good	没有服务器地理信息.
crbug.com	good	IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 查看地图: Google Map
ask.dcloud.net.cn	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
stream.mobihtml5.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
long.open.weixin.qq.com	good	IP: 109.244.217.35 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: 222.85.26.230 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613 查看地图: Google Map
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
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
open.weixin.qq.com	good	**IP:** 175.24.219.72 **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
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.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/gg/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java

URL信息	Url所在文件
http://ask.dcloud.net.cn/article/283	io/dcloud/i/b.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://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/g/b/c.java
https://service.dcloud.net.cn/pdz	io/dcloud/g/b/h/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/g/b/h/a.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/36199	Android String Resource
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so

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。
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.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

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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。
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
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=CN, ST=sichuan, L=chengdu, O=bimgx, OU=bimgx, CN=bobby yang
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-10-27 08:45:43+00:00
Valid To: 2121-10-03 08:45:43+00:00
Issuer: C=CN, ST=sichuan, L=chengdu, O=bimgx, OU=bimgx, CN=bobby yang
Serial Number: 0x2900a0ad
Hash Algorithm: sha256
md5: d6f0d0d44e6743c43ce96cba4f8f7bdd
sha1: 6f9456e3c47184c0420bd73490aee06bdcd51e66
sha256: ecfdc00646492b569eb7e877799e194b7131823254f5c7a26bbd992a462a8213
sha512: 5c07d40e0146cf1961a5c81285c13ace7e5e15a2b6fe30d6b13034a64b22027d6af7f48a5ea56043510f4761f4c6b06b8c3d1cd423645f25e9596fab2f8ba5d3
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 76023afce718478b066360444a950de7b01eb321c0cc0bd6eabb3ed0d24dbf80

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_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_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"

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: wxdc559fd8e8411ee7://,

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