MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

展业呗 1.0.APK

APP名称:	展业呗
包名:	com.app.Hd6678cff41
域名线索:	33条
URL线索:	67条
邮箱线索:	1条
分析日期:	2022年2月3日 13:16

文件信息

文件名: zhanyebei.apk
文件大小: 5.73MB
MD5值: fc4453c2abec61a3e6f76bafd577bfcf
SHA1值: d0312a6df20e4010546fe0ac897b86e07921984d
SHA256值: baa89c78794e32ac5af979a9d9f10cf7283bf700f9c27f2780eecbff6aad817f

APP 信息

App名称: 展业呗
包名: com.app.Hd6678cff41
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.0
安卓版本: 100

域名线索

域名	是否危险域名	服务器信息
d.gt.igexin.com	good	**IP:** 124.160.124.197 **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
api-push.meizu.com	good	**IP:** 125.94.213.129 **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
wke.openspeech.cn	good	没有服务器地理信息.
metrics1.data.hicloud.com	good	**IP:** 118.194.33.17 **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
www.dcloud.io	good	**IP:** 222.85.26.233 **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
m3w.cn	good	**IP:** 125.37.206.223 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map

域名	是否危险域名	服务器信息
api-push.in.meizu.com	good	**IP:** 206.161.233.191 **所属国家:** United States of America **地区:** Virginia **城市:** Herndon **纬度:** 38.978210 **经度:** -77.386993 **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
schemas.android.com	good	没有服务器地理信息.
store.hispace.hicloud.com	good	**IP:** 49.4.44.164 **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
norma-external-collect.meizu.com	good	**IP:** 113.106.27.98 **所属国家:** China **地区:** Guangdong **城市:** Zhongshan **纬度:** 22.520580 **经度:** 113.382317 **查看地图:** Google Map

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
sdk.open.phone.igexin.com	good	**IP:** 124.160.127.216 **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
streamapp.sinaapp.com	good	**IP:** 127.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **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

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
stream.mobihtml5.com	good	没有服务器地理信息.
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
update.dcloud.net.cn	good	**IP:** 121.51.175.120 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **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

域名	是否危险域名	服务器信息
play.google.com	good	**IP:** 172.217.160.78 **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
api.xmpush.xiaomi.com	good	**IP:** 39.156.150.158 **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
uniad-report.dcloud.io	good	**IP:** 47.111.82.188 **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
ask.dcloud.net.cn	good	**IP:** 125.37.206.3 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map

域名	是否危险域名	服务器信息
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
s-gt.getui.com	good	**IP:** 183.131.7.107 **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
a.vmall.com	good	**IP:** 49.4.17.96 **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
c-hzgt2.getui.com	good	**IP:** 183.131.7.106 **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
hxqd.openspeech.cn	good	**IP:** 114.118.64.119 **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
metrics.data.hicloud.com	good	**IP:** 49.4.38.191 **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
dev.voicecloud.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
sdk.open.lbs.igexin.com	good	**IP:** 121.52.255.89 **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

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://wke.openspeech.cn/wakeup/	com/iflytek/thirdparty/C0076s.java
http://imfv.openspeech.cn/msp.do	com/iflytek/thirdparty/C0044ac.java
http://openapi.openspeech.cn/webapi/wfr.do	com/iflytek/thirdparty/C0046ae.java

URL信息	Url所在文件
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postactlog	com/iflytek/thirdparty/C0059b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:postsyslog	com/iflytek/thirdparty/C0059b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posterrlog	com/iflytek/thirdparty/C0059b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:posteventlog	com/iflytek/thirdparty/C0059b.java
http://da.mmarket.com/mmsdk/mmsdk?func=mmsdk:specposteventlog	com/iflytek/thirdparty/C0059b.java
http://hxqd.openspeech.cn/launchconfig	com/iflytek/thirdparty/aF.java
http://iss.openspeech.cn/v?	com/iflytek/speech/UtilityConfig.java
http://sdk.open.phone.igexin.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://c-hzgt2.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.lbs.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://d.gt.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://s-gt.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://bi.	com/igexin/push/config/p.java
http://config.	com/igexin/push/config/p.java
http://stat.	com/igexin/push/config/p.java

URL信息	Url所在文件
http://log.	com/igexin/push/config/p.java
http://lbs.	com/igexin/push/config/p.java
https://api-push.meizu.com	com/meizu/cloud/pushsdk/b/c/e.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/a.java
http://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/a/a/b.java
http://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/a/a/a.java
https://api-push.meizu.com/garcia/api/server/getPublicKey	com/meizu/cloud/pushsdk/handler/a/a.java
https://)	com/huawei/a/k/f/c.java
https://)	com/huawei/a/l/c.java
https://metrics.data.hicloud.com:6447	com/huawei/a/f/f/j.java
https://store.hispace.hicloud.com/hwmarket/api/tlsApis	com/huawei/updatesdk/sdk/service/c/a/c.java
https://play.google.com/store	com/huawei/hms/update/c/a.java
https://a.vmall.com/app/	com/huawei/hms/update/e/l.java
https://metrics1.data.hicloud.com:6447	com/huawei/hms/api/HuaweiApiClient.java

URL信息	Url所在文件
https://play.google.com/store/apps/details?id=	com/huawei/hms/support/api/push/a/a/a.java
https://a.vmall.com/	com/huawei/hms/support/api/push/a/a/a.java
https://api.xmpush.xiaomi.com/upload/xmsf_log?file=	com/xiaomi/mipush/sdk/u.java
https://api.xmpush.xiaomi.com/upload/app_log?file=	com/xiaomi/mipush/sdk/u.java
https://api.xmpush.xiaomi.com/upload/crash_log?file=	com/xiaomi/mipush/sdk/w.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://m3w.cn/sd/reg	io/dcloud/appstream/b.java
http://m3w.cn/s/	io/dcloud/appstream/share/a.java
http://ask.dcloud.net.cn/article/283	io/dcloud/feature/b.java
http://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://service.dcloud.net.cn/advert/splash	io/dcloud/feature/ad/dcloud/ADHandler.java
https://service.dcloud.net.cn/collect/plusapp/cad	io/dcloud/feature/ad/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java

URL信息	Url所在文件
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://www.dcloud.io/streamapp/streamapp.apk	io/dcloud/common/util/ShortCutUtil.java
http://stream.dcloud.net.cn/resource/sitemap/v2?appid=	io/dcloud/common/a/d.java
https://service.dcloud.net.cn/collect/plusapp/startup	io/dcloud/common/a/d.java
http://ask.dcloud.net.cn/article/35627	io/dcloud/common/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/common/a/a.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/common/core/a.java
https://service.dcloud.net.cn/collect/plusapp/action	io/dcloud/common/core/b/a.java
https://service.dcloud.net.cn/pdz	io/dcloud/common/core/b/a.java
https://uniad-report.dcloud.io/video/report?p=a&t=r	io/dcloud/common/core/b/a.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
http://update.dcloud.net.cn/apps/	io/dcloud/common/constant/IntentConst.java
http://streamapp.sinaapp.com	io/dcloud/streamdownload/utils/CommitPointData.java

邮箱线索

邮箱地址	所在文件
xxxx@xxxx.com	com/huawei/hms/support/api/push/a/d/a.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
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

向手机申请的权限	是否危险	类型	详细情况
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
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
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
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备

向手机申请的权限	是否危险	类型	详细情况
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
getui.permission.GetuiService.com.app.Hd6678cff41	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
com.app.Hd6678cff41.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.app.Hd6678cff41.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.app.Hd6678cff41.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.app.Hd6678cff41.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	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
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。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=SH, L=SH, O=juzhibao, OU=juzhibao, CN=juzhibao
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-21 16:02:14+00:00
Valid To: 2030-09-19 16:02:14+00:00
Issuer: C=CN, ST=SH, L=SH, O=juzhibao, OU=juzhibao, CN=juzhibao
Serial Number: 0x49f336de
Hash Algorithm: sha256
md5: c53cba2c28613aca0574c47124b51797
sha1: 8b9e99ba03555fd638a631661f385b9068aaef47
sha256: 3c40e73f6ff237bf1567b1b636b2697c3220b39e1f0de7f6163f34cf630b511b
sha512: 0ff68f706c8fa8b01c79db7842891bb66db3bde21d30d47f0045377128c8f0f86a4c5f6feea5894d14d8e92317a5597a30b2cd9c6dacb6ef238233f3142adab2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6e48094bd142ea4ad2bc5da77e7f13fd7941546ab15fed85d46bd49cc6c9f94d

Exodus威胁情报

名称	分类	URL链接
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h5c9d71b5://,
io.dcloud.appstream.StreamAppMainActivity	Schemes: streamapp://, streamappmain://,

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机：Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check SIM operator check network operator name check device ID check subscriber ID check possible VM check 编译器：r8 without marker (suspicious)